S. HRG. 112–851

WHAT FACIAL RECOGNITION TECHNOLOGY MEANS FOR PRIVACY AND CIVIL LIBERTIES

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY
TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

SECOND SESSION

JULY 18, 2012

Serial No. J–112–87

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE
86–599 PDF WASHINGTON : 2012

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
AL FRANKEN, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut

CHUCK GRASSLEY, Iowa
ORRIN G. HATCH, Utah
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TOM COBURN, Oklahoma

Bruce A. Cohen, *Chief Counsel and Staff Director*
Kolan Davis, *Republican Chief Counsel and Staff Director*

Subcommittee on Privacy, Technology and the Law

AL FRANKEN, Minnesota, *Chairman*

CHUCK SCHUMER, New York
SHELDON WHITEHOUSE, Rhode Island
RICHARD BLUMENTHAL, Connecticut

TOM COBURN, Oklahoma
ORRIN G. HATCH, Utah
LINDSEY GRAHAM, South Carolina

Alvaro Bedoya, *Democratic Chief Counsel*
Elizabeth Hays, *Republican General Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

WITNESSES

QUESTIONS

QUESTIONS AND ANSWERS

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

ADDITIONAL SUBMISSIONS FOR THE RECORD

WHAT FACIAL RECOGNITION TECHNOLOGY MEANS FOR PRIVACY AND CIVIL LIBERTIES

WEDNESDAY, JULY 18, 2012

U.S. SENATE,
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:36 p.m., in Room SD–226, Dirksen Senate Office Building, Hon. Al Franken, Chairman of the Subcommittee, presiding.

Present: Senators Franken, Whitehouse, and Blumenthal.

Also present. Senator Sessions.

OPENING STATEMENT OF HON. AL FRANKEN, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Chairman FRANKEN. This hearing will be called to order. Welcome to the fourth hearing of the Subcommittee on Privacy, Technology, and the Law. Today's hearing will examine the use of facial recognition technology by the Government and the private sector and what that means for privacy and civil liberties.

I want to be clear: There is nothing inherently right or wrong with facial recognition technology. Just like any other new and powerful technology, it is a tool that can be used for great good. But if we do not stop and carefully consider the way we use this technology, it could also be abused in ways that could threaten basic aspects of our privacy and civil liberties. I called this hearing so we can just start this conversation.

I believe that we have a fundamental right to control our private information, and biometric information is already among the most sensitive of our private information, mainly because it is both unique and permanent. You can change your password. You can get a new credit card. But you cannot change your fingerprint, and you cannot change your face—unless, I guess, you go to a great deal of trouble.

Indeed, the dimensions of our faces are unique to each of us—just like our fingerprints. And just like fingerprint analysis, facial recognition technology allows others to identify you with what is called a "faceprint"—a unique file describing your face.

But facial recognition creates acute privacy concerns that fingerprints do not. Once someone has your fingerprint, they can dust your house or your surroundings to figure out what you have touched.

Once someone has your faceprint, they can get your name, they can find your social networking account, and they can find and track you in the street, in the stores that you visit, the Government buildings you enter, and the photos your friends post online. Your face is a conduit to an incredible amount of information about you, and facial recognition technology can allow others to access all of that information from a distance, without your knowledge, and in about as much time as it takes to snap a photo.

People think of facial recognition as something out of a science fiction novel. In reality, facial recognition technology is in broad use today. If you have a driver's license, if you have a passport, if you are a member of a social network, chances are good that you are part of a facial recognition data base.

There are countless uses of this technology, and many of them are innovative and quite useful. The State Department uses facial recognition technology to identify and stop passport fraud—preventing people from getting multiple passports under different names. Using facial recognition technology, Sheriff Larry Amerson of Calhoun County, Alabama, who is with us here today, can make sure that a prisoner being released from the Calhoun County jail is actually the same prisoner that is supposed to be released. That is useful. Similarly, some of the latest smartphones can be unlocked by the owner by just looking at the phone and blinking.

But there are uses of this technology that should give us pause.

In 2010, Facebook, the largest social network, began signing up all of its then 800 million users in a program called Tag Suggestions. Tag Suggestions made it easier to tag close friends in photos, and that is a good thing.

But the feature did this by creating a unique faceprint for every one of those friends. And in doing so, Facebook may have created the world's largest privately held data base of faceprints—without the explicit consent of its users. To date, Tag Suggestions is an opt-out program. Unless you have taken the time to turn it off, it may have already been used to generate your faceprint.

Separately, last year, the FBI rolled out a Facial Recognition Pilot program in Maryland, Michigan, and Hawaii that will soon expand to three more States. This pilot lets officers in the field take a photo of someone and compare it to a Federal data base of criminal mug shots. The pilot can also help ID a suspect in a photo from an actual crime. Already, several other States are setting up their own facial recognition systems independently of the FBI. These efforts will catch criminals. In fact, they already have.

Now, many of you may be thinking that that is an excellent thing, and I agree. But unless law enforcement facial recognition programs are deployed in a very careful manner, I fear that these gains could eventually come at a high cost to our civil liberties.

I fear that the FBI pilot could be abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution, stifling their First Amendment rights. Curiously enough, a lot of the presentations on this technology by the Department of Justice show it being used on people attending political events or other public gatherings.

I also fear that without further protections, facial recognition technology could be used on unsuspecting civilians innocent of any crime, invading their privacy and exposing them to potential false identifications.

Since 2010, the National Institute of Justice, which is a part of DOJ, has spent $1.4 million to develop facial recognition-enhanced binoculars that can be used to identify people at a distance and in crowds. It seems easy to envision facial recognition technology being used on innocent civilians when all an officer has to do is look at them through his binoculars or her binoculars.

But facial recognition technology has reached a point where it is not limited to law enforcement and multi-billion-dollar companies. It can also be used by private citizens. Last year, Professor Alessandro Acquisti of Carnegie Mellon University, who is testifying today, used a consumer-grade digital camera and off-the-shelf facial recognition software to identify one out of three students walking across a campus.

I called this hearing to raise awareness about the fact that facial recognition already exists right here, today, and we need to think about what that means for our society. I also called this hearing to call attention to the fact that our Federal privacy laws are almost totally unprepared to deal with this technology.

Unlike what we have in place for wiretaps and other surveillance devices, there is no law regulating law enforcement use of facial recognition technology. And current Fourth Amendment case law generally says that we have no reasonable expectation of privacy in what we voluntarily expose to the public; yet we can hardly leave our houses in the morning without exposing our faces to the public. So law enforcement does not need a warrant to use this technology on someone. It might not even need to have a reasonable suspicion that the subject has been involved in a crime.

The situation for the private sector is similar. Federal law provides some protection against true bad actors that promise one thing yet do another. But that is pretty much as far as the law goes. If a store wants to take a photo of your face when you walk in and generate a faceprint—without your permission—they can do that. They might even be able to sell it to third parties.

Thankfully, we have a little time to do better. While this technology will in a matter of time be at a place where it can be used quickly and reliably to identify a stranger, it is not there quite just yet. And so I have called the FBI and Facebook here today to challenge them to use their position as leaders in their fields to set an example for others before this technology is used pervasively.

The FBI already has some privacy safeguards in place. But I still think that they could do more to prevent this technology from being used to identify and target people engaging in political protests or other free speech. I think the FBI could do more to make sure that officers use this technology only when they have good reason to think that someone is involved in a crime. I also think that if the FBI did these things, law enforcement agencies around the country would follow.

For their part, Facebook allows people to use Tag Suggestions only on their close friends. But I think Facebook could still do more to explain to its users how it uses facial recognition and to give them better choices about whether or not to participate in Tag Suggestions. I think that Facebook could make clear to its users just how much data it has and how it will and will not use its large and growing data base of faceprints. And I think that if Facebook did these things, they would establish a best practice against which other social networks would be measured.

My understanding is that for the past few months, Facebook Tag Suggestions has been temporarily disabled to allow for some technical maintenance. It seems to me that Facebook has the perfect opportunity to make changes to its facial recognition program when it brings Tag Suggestions back online.

I am also calling the Federal Trade Commission to testify because they are in the process of actually writing best practices for the use of this technology in industry. I urge the Commission to use this as an opportunity to guarantee consumers the information and choices they need to make informed decisions about their privacy.

In the end, though, I also think that Congress may need to act, and it would not be the first time it did. In the era of J. Edgar Hoover, wiretaps were used freely with little regard to privacy. Under some Supreme Court precedents of that era, as long as the wiretapping device did not actually penetrate the person's home or property, it was deemed constitutionally sound—even without a warrant. And so in 1968, Congress passed the Wiretap Act. Thanks to that law, wiretaps are still used to stop violent and serious crimes. But police need a warrant before they get a wiretap. And you cannot wiretap someone just because they are a few days late on their taxes. Wiretaps can be used only for certain categories of serious crimes.

I think that we need to ask ourselves whether Congress is in a similar position today as it was 50 or 60 years ago before the passage of the Wiretap Act. I hope the witnesses today will help us consider this and all of the different questions raised by this technology.

I was going to turn it over to my friend and Ranking Member, Senator Coburn, but I do not think he would have a lot to say at this moment.

[Laughter.]

Chairman FRANKEN. I am sure he will have some great questions.

What I would like to do is introduce our first panel of witnesses. But before I do, I would like to give my esteemed colleague, Senator Sessions, the opportunity to make an introduction of the sheriff, who is going to be on the second panel from your own State.

STATEMENT OF HON. JEFF SESSIONS, A U.S. SENATOR FROM THE STATE OF ALABAMA

Senator SESSIONS. That would be wonderful. Thank you, Mr. Chairman. Those are remarks that we need to think about as we go forward with new technologies, and it takes some effort to get to the bottom of it.

I am honored to take a few moments to introduce my friend, Sheriff Larry Amerson, who has served for 18 years as sheriff in Calhoun County, Alabama, and Anniston. He is a graduate of Jacksonville State University, one of my superb universities, with a B.A. in law enforcement, finally becoming sheriff. He served for 14 years as deputy sheriff in Calhoun County. He currently serves as the 71st president of the National Sheriffs' Association and is also the chairman of the National Sheriffs' Institute Education and Training Committee and vice chair of the Court Security Committee. He is a certified jail manager and past member of the FBI Criminal Justice Information System's Southern Working Group, and that Criminal Justice Information System is a lot of what we will be talking about today, how that system works.

Sheriff, it is great to see you. Thank you for coming, and I am pleased to have this opportunity to introduce you.

Mr. Chairman, could I just say a couple of things?

Chairman FRANKEN. Absolutely.

Senator SESSIONS. I would like to come back if you would allow me, but I might not be able to.

Chairman FRANKEN. I understand.

Senator SESSIONS. We need to look at facial recognition and see how it works and where it can be beneficial consistent with our constitutional rights and privileges that we value in our country. But it is a matter that I have dealt with for a long time, and there are a lot of people who would like to see a major enhancement of the facial identification system used at airports for security and that sort of thing. And there are some fundamental weaknesses at this point with that as a practical matter.

The fingerprint has been in use for 50 years, I guess. Virtually every criminal in America has had his fingerprint placed in records that can be ascertained by even a local police officer at his police car. He can have people put their hands on a machine, and it will read that to see if the ID he presented may be false and he may be somebody else, maybe a fugitive from justice. So the fingerprint system is really, really proven. And you have the criminal histories that are available to law officers when they produce that.

So if we start with the facial recognition—and maybe it is time to start with some of that. But if we start with it, we do not have many people in it. There are not that many people who have been identified who have had their visage imprinted and can be drawn. And terrorists around the world, presumably we do not have their facial things, where we may have been collecting their fingerprints for years.

Secretary Ridge, when he was Homeland Security Secretary, tried to figure a way to deal with the situation at the airports. A lot of people wanted to use facial recognition, Mr. Chairman, because they thought it would be quicker, people would just go right on through the system. But, you know, I would ask a simple question: If there is no bank of visages, what good is it? And why couldn't you use a fingerprint situation where you put your fingerprint in, the computer reads it, even if you check through and you go down and wait to get on the plane, if a minute, five minutes, three minutes later, it comes back this is a terrorist, you can go down and get the man.

When he left, I would say I was kind of pleased. I had not talked to him for some time about it. He said, "Well, I have one bit of advice for my successor: Emphasize the fingerprint." So I felt like he had concluded that is a suggestion.

So I do not know how far you can go with utilizing the face system effectively. I was a Federal prosecutor for 15 years. Knowing how the system works today, I know it would take many years to get it to compete with the fingerprint system for basic law enforcement work. But, Mr. Chairman, there could be certain things, like in a jail. You suggested that. There are other things that could work right now.

So thank you for giving me the opportunity to share those thoughts. You have got a great panel of witnesses. I salute you for investing the time and effort to wrestle with these important issues.

Chairman FRANKEN. Well, thank you for your very well-made comments, and these are questions that we are starting to deal with in today's hearing, so thank you.

Senator SESSIONS. If I come back, I would like to ask some of those. If not, I will try to submit it for the record, if you do not mind.

Chairman FRANKEN. Absolutely.

Senator SESSIONS. Thank you.

Chairman FRANKEN. Maybe we should call it, after listening to you, "visage recognition technology."

[Laughter.]

Chairman FRANKEN. Just to confuse people, I would like to do that.

Chairman FRANKEN. Now I would like to introduce our first panel of witnesses.

Jerome Pender is the Deputy Assistant Director of the Operations Branch at the FBI's Criminal Justice Information Division. He manages information technology for many of the FBI's biometric systems and helps oversee the deployment of a pilot facial recognition program as part of the FBI's Next Generation Identification Initiative. Prior to joining the FBI, Mr. Pender served as the executive director of Information Technology for UBS Warburg. He holds a master's degree in computer science from Johns Hopkins and is a graduate of the United States Air Force Academy. Thank you for being here.

Maneesha Mithal is the Associate Director of the Federal Trade Commission's Division of Privacy and Identity Protection. She oversees work on commercial privacy, data security, and credit reporting, and works to ensure companies comply with the FTC Act's unfair or deceptive practices provision. Before joining the FTC, Ms. Mithal was an attorney at the Washington office of Covington & Burling. She earned her undergraduate and law degrees from Georgetown University.

Thank you again, both of you, for being here today. I really hope that your presence here will mark the start of a productive dialogue about this technology going forward. Your complete written testimony will be made a part of the record. You each have about 5 minutes for opening remarks that you would like to make.

Mr. Pender, would you like to begin?

STATEMENT OF JEROME M. PENDER, DEPUTY ASSISTANT DIRECTOR, CRIMINAL JUSTICE INFORMATION SERVICES DIVISION, FEDERAL BUREAU OF INVESTIGATION, U.S. DEPARTMENT OF JUSTICE, CLARKSBURG, WEST VIRGINIA

Mr. PENDER. Certainly. Thank you. Mr. Chairman, I would like to thank the Subcommittee for the opportunity to discuss the FBI's

Next Generation Identification Program, NGI. The FBI is committed to ensuring appropriate privacy protections are in place as we deploy NGI technologies, including facial recognition, and that the capabilities are implemented and operated with transparency and full disclosure.

The FBI began collecting criminal history on a national level in 1924. From 1924 until 1999, fingerprints and associated criminal history information, including mug shot photographs, were received in the U.S. mail and processed manually. In 1999, with the launching of the Integrated Automated Fingerprint Identification System, fingerprints were searched, processed, and stored using automation.

The NGI Program, which is on scope, on schedule, and on cost, and 60 percent deployed, is enabling the FBI to meet its criminal justice mission. It will use facial recognition to automate for the first time the processing of mug shots.

NGI is being deployed in seven separate increments. Increment four includes the facial recognition system. It was deployed as a pilot in February 2012 and is scheduled for full operational capability in the summer of 2014. The objective of the pilot is to conduct image-based facial recognition searches of the FBI's national repository and provide investigative candidate lists to agencies submitting queries.

The goals of the pilot are to test the facial recognition processes, resolve policy and processing issues, solidify privacy protection procedures, and address user concerns.

The pilot provides a search of the national repository of photos consisting of criminal mug shots, which were taken at the time of a criminal booking. Only criminal mug shot photos are used to populate the national repository. Query photos and photos obtained from social networking sites, surveillance cameras, and similar sources are not used to populate the national repository. It contains approximately 12.8 million photos.

The Facial Recognition Pilot permits authorized law enforcement agencies to submit queries for a facial recognition search of the national repository. It can be queried by authorized criminal justice agencies for criminal justice purposes.

Access is subject to all rules regarding access to FBI CJIS systems information and subject to dissemination rules for authorized criminal justice agencies. The investigative response provided to a submitting agency will include the number of candidates requested, in ranked order, along with a caveat noting that the response should only be used as an investigative lead.

In accordance with Section 208 of the E-Government Act of 2002, facial recognition was initially addressed by the FBI's June 9, 2008, Interstate Photo System Privacy Impact Assessment, or PIA. In coordination with the FBI's Office of the General Counsel, the 2008 PIA is currently in the process of being renewed by way of Privacy Threshold Analysis, with an emphasis on facial recognition. An updated PIA is planned and will address all evolutionary changes since the preparation of the 2008 PIA.

Each participating pilot State or agency is required to execute a Memorandum of Understanding, MOU, that details the purpose, authority, scope, disclosure, and use of information, and the security rules and procedures associated with piloting. Pilot participants are advised that all information is treated as "law enforcement sensitive" and protected from unauthorized disclosure.

Information derived from the pilot search requests and resulting responses are to be used only as an investigative lead. Results are not to be considered as positive identifications.

In February 2012, the State of Michigan successfully completed an end-to-end Facial Recognition Pilot transaction and is currently submitting facial recognition searches to CJIS. MOUs have also been executed with Hawaii and Maryland; South Carolina, Ohio, and New Mexico are engaged in the MOU review process for Facial Recognition Pilot participation.

In summary, the FBI's Next Generation Identification Program is on scope, on schedule, on cost, and 60 percent deployed. The Facial Recognition Pilot which began operation in February 2012 searches criminal mug shots and provides investigative leads. The Facial Recognition Pilot is evaluating and solidifying policies, procedures, and privacy protections. Full operational capability for facial recognition is scheduled for the summer of 2014.

Thank you.

[The prepared statement of Mr. Pender appears as a submission for the record.]

Chairman FRANKEN. Thank you, Mr. Pender.

Ms. Mithal.

STATEMENT OF MANEESHA MITHAL, ASSOCIATE DIRECTOR, DIVISION OF PRIVACY AND IDENTITY PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, D.C.

Ms. MITHAL. Thank you, Chairman Franken. I am Maneesha Mithal with the Federal Trade Commission. I appreciate the opportunity to present the Commission's testimony on the commercial uses of facial recognition technology, the potential benefits, and privacy implications.

Imagine a world where you are walking down the street and a stranger takes a picture of you with their smartphone. The stranger is then able to pull up not only your name but where you live, how much you paid for your house, and who your close friends are.

Imagine another scenario where you walk into a store and a digital sign scans your face, links you with a loyalty card, and greets you with a message: "Jane Doe, I see you have bought Slimfast before. Here is a coupon for $1 off your next purchase."

These scenarios are not far from becoming a reality. Some consumers might think they are innovative and they want to participate in them. Others may find them invasive. Today facial recognition is being used commercially for a variety of purposes, many of them beneficial to consumers. For example, as you mentioned, companies are using the technology to allow consumers to unlock their smartphones using their faces rather than their passwords, to allow consumers to upload their faces to a website to try on make up hair styles and eyeglasses, and to help consumers manage and organize photos.

In December 2011, the Commission hosted a workshop to examine these current and future uses of facial recognition, as well as the privacy implications they raise. In my statement today, I would like to discuss four themes that emerged from the workshop and conclude by setting forth our next steps in this area.

First, many workshop participants highlighted the recent growth in the commercial use of facial recognition technologies. Until recently, because of high costs and limited accuracy, companies did not widely use these technologies. However, several recent developments have brought steady improvements. For example, better quality digital cameras and lenses create higher-quality images from which biometric data can be more easily extracted. Recent technological advances have been accompanied by a rapid growth in the availability of online photos. For example, approximately 2.5 billion photos are uploaded to Facebook each month. As a result, companies do not need to purchase proprietary sets of identified images, thereby lowering costs and making facial recognition technologies commercially viable for a broad range of entities.

Second, we learned about current applications of facial recognition technologies. In one application, the technology can simply be used for pure facial detection—that is, to determine that a photo has a face in it. Current uses include refining search engine results to include only those results that contain a face, locating faces in images in order to blur them, or ensuring that the frame for a video chat feed actually includes a face.

In another application, the technology allows companies to assess characteristics of facial images. For instance, companies can identify moods or emotions from facial expressions to determine a player's engagement with a video game or a viewer's excitement during a movie.

Companies can also determine demographic characteristics of a face such as age and gender to deliver targeted ads in real time in retail spaces.

The use of facial recognition technology that potentially raises the most privacy concerns is the use to identify anonymous individuals in images. One of the most prevalent current uses of this application is to enable semiautomated photo tagging or photo organization on social networks and in photo management applications.

Third, in addition to these current uses, panelists discussed the ways in which facial recognition could be implemented in the future. For example, will it become feasible to use facial recognition to identify previously anonymous individuals in public places or in previously unidentified photos online? In a 2011 study, which we will be hearing about, Carnegie Mellon researchers were able to identify individuals in previously unidentified photos from a dating site by using facial recognition technology to match them to their Facebook profile photos.

Finally, panelists discussed the privacy concerns associated with facial recognition. For example, a mobile app that could, in real-time, identify previously anonymous individuals on the street or in a bar and correlate a name with a person's physical address could raise serious physical safety concerns.

Following the workshop, Commission staff has been developing a report that builds on the principles that the Commission outlined in its March 2012 privacy report. Those principles are: privacy by design, simplified choice, and improved transparency. The report discusses the application of these principles to the realm of facial recognition, and we should be issuing a report in the coming months.

Thank you for the opportunity to provide the Commission's views, and we look forward to working with Congress on this important issue.

[The prepared statement of Ms. Mithal appears as a submission for the record.]

Chairman FRANKEN. Thank you, Ms. Mithal.

Mr. Pender, the FBI allows searches of its facial recognition data base. They are done only for criminal justice purposes, and that is a good thing. But the term "criminal justice purpose" is kind of broad, so I am concerned that this system allows law enforcement to identify and target people marching in a rally or protesting in front of a courthouse because in all three States where the pilot is operating, it is technically a crime to block a sidewalk or obstruct the entrance to a building.

Mr. Pender, has the FBI issued a rule prohibiting or discouraging jurisdictions from using facial recognition technology in a way that could stifle free speech? And if not, will the FBI consider doing this?

Mr. PENDER. Certainly as we are deploying the NGI system, we are extremely concerned to make sure that we have appropriate protections in it to ensure there is not any invasion of privacy or those sorts of things.

The definition of "criminal justice purpose" is defined in 28 CFR Section 20.3(b), and it has nine particular activities that are part of the administration of criminal justice. In the scenario that you mentioned about the protesters and potentially blocking the sidewalk, I think you are implying that an officer is taking a photo of someone for blocking the sidewalk on the pretext of putting them into some type of data base. So I can say a few things about that.

First of all, the only photos that will go into the data base are the criminal mug shot photos, so the probe photos that are being searched through the system do not ever go into the data base.

Then as regards to whether or not the particular person blocking the sidewalk could even be searched, the officer would have to clearly articulate which of those administration of criminal justice functions that they are trying to perform, and the way you have let out the scenario there, you are implying that they are not really interested in blocking the sidewalk. They are using it as a pretext for something else, and that would not be a valid use of the system under the current rules.

Again, we take this very seriously, so that is certainly the reason that we are deploying the system slowly in a pilot phase to work out any details, make sure that there is appropriate training and guidance in place, and so that is an important part of our process.

One of the things that the MOUs that we sign with the agencies that are going to access the system require is an audit process, so the local agencies are required to audit the use of the system on an annual basis to detect any type of misuse. And then, in addition to that, within our FBI CJIS Division we have an audit unit that goes out and does triennial audits of the same agencies, and that is done as a little bit of a safety net, a double-check on the audits, as well as to be sure that the audit processes are in place and being done effectively.

In those audits, if any misuse is detected, there is a full range of options that is defined in the sanctions process, and that could range from administrative letters, that sort of thing, to removal of access from the system, either on an individual or an agency basis, if the controls are not effective, up to and including criminal prosecution for misuse.

Chairman FRANKEN. OK. How do you define "misuse"? First of all, have any audits been produced yet?

Mr. PENDER. The audit process that I am talking about is with regards to access to criminal history in general. It has been longstanding for the last many decades. The photos are part of that criminal history data base, so all of those same standards apply.

At this point, we have not done any audits specific to the use of facial recognition. That is what we are in the process of developing through the pilot.

Chairman FRANKEN. OK. So is there anything that explicitly in your pilot discourages the use of this technology at a rally or a political event?

Mr. PENDER. I cannot think of something that says you should not use this at a political event. I think it is defined in the terms of the positive where it is allowed to be used, and that would be outside of what is permitted. But certainly we are—that is the purpose of doing the slow deployment, is to identify if there are particular gray areas that need to be trained——

Chairman FRANKEN. Part of the reason I bring this up is that the FBI's own presentations of this technology—I do not know if we have a blow-up of this, but it shows it being used to identify people at a political rally. That is what the FBI did. So that is—you know, I mean, this is done by the Obama administration. It is at an Obama rally. One of them is. And one is at a Hillary rally, and, you know, they have made up.

[Laughter.]

Chairman FRANKEN. She is a great Secretary of State. But they might be sending the wrong message, don't you think?

Mr. PENDER. I am not familiar with that particular presentation. I am not familiar with the photos, but certainly if there are photos of a political rally, what we are—the NGI system that we are deploying and what we are doing, we absolutely have no intention of going out. It absolutely will be limited to the mug shot photos and the criminal history data base.

Chairman FRANKEN. OK. In a similar vein, will the FBI consider telling States in its facial recognition program that they should use the technology to identify someone only if they have a probable cause that they have been involved in a criminal activity?

Mr. PENDER. The mug shot photos are part of the criminal history data base, and so this is an issue that we have been working with for many years on when is it appropriate to distribute information out of the criminal history data base. And so in April 2001, there were some questions about that, and we sent out what we call a contributor letter that clarifies when it is appropriate to use the system or not. And the language in that particular letter says that the officer must clearly articulate one of the administration of criminal justice purposes that they are administering, and if they are basing it on the detection or apprehension function, they have to have an articulable suspicion or a reasonable basis for the search.

So, again, that was in the context of criminal history, but mug shots are part of that. And certainly as we are deploying the system——

Chairman FRANKEN. Well, I understand that the mug shots are the data base from which they are looking. I am wondering who they choose to search, I mean, who they choose to take a picture of, say, to see if they match the data base. That is what I am asking.

Mr. PENDER. Right. The probe photos are photos that they are searching against the data base. They have to be able to have that articulable suspicion or reasonable basis for performing the search. And certainly, again, that is the reason for going slowly. We have a series of working groups that we are working with, our State and local partners from the Advisory Policy Board, as Senator Sessions was talking about, that were working on it and making sure that the policies are clear, that we have appropriate training programs in place as well. Prior to accessing our NCIC system, for example, an individual is required to have training and a certification test that is repeated every two years to maintain the current certification. And we require annual training on security practices as well.

So if there are appropriate enhancements that we need to make specific to facial recognition, we are very open to doing that.

Chairman FRANKEN. OK. Thank you.

Ms. Mithal, my understanding is that the Commission is in the process of proposing best practices for the commercial use of facial recognition. I want to urge you to make a very simple rule one of your best practices; that is, if a company wants to create a unique faceprint for someone to identify them, they need to get their permission first. Will the Commission do that?

Ms. MITHAL. Thank you. As I mentioned, the Commission is considering best practices, and I am certainly sure that that is one of the issues that they are considering, and I will take it back to them that you have requested us to consider this.

The other thing I would note is that in our March 2012 privacy report, we talked about the importance of providing consumers with meaningful choice when their information is collected. At a minimum, what we think that means is that a disclosure has to be provided very clearly outside the privacy policy so that consumers can make informed decisions about their data.

Chairman FRANKEN. That does not sound like a yes. I do not think this is a heavy lift, frankly. While Federal law says nothing about this, two States—Illinois and Texas—both require a company to get a customer's consent before they create a biometric for them. So, at least in theory, this is already the standard that national companies have to meet, and without objection, I would like to enter these laws into the record.

[The information appears as a submission for the record.]

Chairman FRANKEN. Could you pass this on to the Commission? I will give it to you.

Ms. MITHAL. We will take a look, and I will pass it on, yes. Thank you.

Chairman FRANKEN. Thank you. Thank you very much.

Ms. Mithal, when a social network or an app company is creating a faceprint to identify someone in a photo, what is the Commission's position on the kind of notice they need to provide their users? Is the best practice to tell their users, you know, "We are going to create a unique faceprint for you"? Or is it something less than that?

Ms. MITHAL. Sir, again, this is exactly the type of issue the Commission is currently considering, and I cannot get in front of my Commission on this. They are really considering these issues. But if you look at what the Commission has said publicly in terms of our privacy report, we have called for transparency. And what that means is clear, simple, concise notices, not in legalese.

Chairman FRANKEN. OK. Clear, simple, and precise.

Ms. MITHAL. Concise.

Chairman FRANKEN. Concise. Oh, I am sorry.

Ms. MITHAL. Precise would be good, too.

Chairman FRANKEN. Thank you for that validation.

[Laughter.]

Chairman FRANKEN. OK. Well, I want to thank you both for your testimony and call the second panel. Thank you, Ms. Mithal and Mr. Pender.

Ms. MITHAL. Thank you.

Mr. PENDER. Thank you.

Chairman FRANKEN. We have now our second panel, and let me introduce them while they take their seats.

We have Mr. Brian Martin, who is director of Biometric Research for MorphoTrust USA, a leading biometrics company that supplies facial recognition technology to the Federal Government and many State governments. Mr. Martin has over 15 years of experience in the biometrics and has helped develop numerous biometric technologies involving iris, fingerprint, and facial recognition. He earned his Ph.D. in physics from the University of Pittsburgh. I called Mr. Martin to be our star technical witness who can begin our second panel by explaining how the technology actually works.

Alessandro Acquisti is an associate professor of information technology and public policy at Carnegie Mellon University where his research focuses on the economics of privacy. Professor Acquisti is at the helm of not just one but several pioneering studies evaluating the privacy implications of facial recognition technology. He has received numerous awards for his research and expertise on privacy issues. Professor Acquisti earned a master's and Ph.D. in information systems from UC-Berkeley and received a master's in economics from Trinity College, Dublin, and from the London School of Economics.

Sheriff Larry Amerson, whom Senator Sessions introduced earlier, is the president of the National Sheriffs' Association and is also serving in his 18th year as sheriff of Calhoun County, Alabama, and that is in Anniston as the county seat?

Mr. AMERSON. Yes, sir.

Chairman FRANKEN. As part of his mission to modernize police operations, Sheriff Amerson is overseeing the implementation of iris and facial recognition in Calhoun County jails and in the field. Sheriff Amerson has had a long, successful career in law enforcement. Sheriff Amerson earned his bachelor's degree in law enforcement from Jacksonville State University.

Nita Farahany is an associate professor of law at the Duke University School of Law and is a leading scholar on the ethical, legal, and social implications of emerging technologies. She was appointed in 2010 by President Obama to serve on the Presidential Commission on the Study of Bioethical Issues. Professor Farahany has written on the application of the Fourth Amendment to emerging technology. She received her bachelor's degree from Dartmouth College and a J.D. and Ph.D. in philosophy from Duke University.

Rob Sherman is the manager of privacy and public policy at Facebook. He manages policy matters involving privacy, security, and online trust. Prior to joining Facebook, Mr. Sherman was an attorney at Covington & Burling, where he focused his practice on issues relating to privacy and online security. Mr. Sherman received his law degree from the University of Michigan and his undergraduate degree from the University of Maryland.

Jennifer Lynch is a staff attorney at the Electronic Frontier Foundation, where she focuses on Government transparency and privacy issues. Ms. Lynch has written and spoken on biometrics collection, including the Government's use of facial recognition technology. Before joining EFF, she served as a clinical teaching fellow with the Samuelson Law, Technology, and Public Policy Clinic at the UC-Berkeley School of Law and clerked for Judge A. Howard Matz in the Central District of California. She received both her undergraduate and law degrees from UC-Berkeley.

Thank you all for joining us, and your complete written testimonies will be made part of the record. You each have approximately five minutes for any opening remarks that you would like to make. Mr. Martin, please start us off.

STATEMENT OF BRIAN MARTIN, PH.D., DIRECTOR OF BIOMETRIC RESEARCH, MORPHOTRUST USA, JERSEY CITY, NEW JERSEY

Mr. MARTIN. Thank you. Good afternoon, Chairman Franken. Thank you for asking MorphoTrust to testify on the capabilities of face recognition.

As the director of Biometric Research for MorphoTrust, my team is responsible for the biometric technologies used by the U.S. Department of State, the Department of Defense, the FBI, and numerous motor vehicle/driver's license systems. I am here today to testify on the state-of-the-art of face recognition.

First, I would like to briefly explain how face recognition works. Now, face recognition is not new. The idea has been around for almost half a century. But only in the late 1990s did these ideas become commercialized. The different approaches are varied. They can be 2–D, a regular image; they can be 3–D from a special 3–D scanner. Face recognition can look at the shape of the face, or it can even look at microscopic features like your pores and wrinkles on your skin.

In all cases, though, modern face recognition approaches are vastly more complicated than commonly perceived, where people say, oh, they are just measuring, you know, the distance between the eyes and the nose or something.

While there are several different approaches to face recognition, there are some general steps to face recognition. The first is what is called face detection, and this is exactly what your camera is doing when it tries to focus on the face. It is just trying to see if there is a face in the image.

Another step is called feature registration and extraction, and this is maybe the more interesting case because this is where the individualized features of the face are extracted from an image and stored into a binary format which you have called a "faceprint" or "facial template."

Now, these faceprints are vendor-specific, meaning they are not very useful outside of the face recognition system. They contain no more information than what was in the original image. They do not contain meta data or identity data about the person. They are just a different representation of what was already in the image. And they cannot be reverse engineered, so you cannot regenerate the image from the faceprint.

After you have two or more faceprints, then you can perform facial matching, and facial matching, in the state of the art, can be as fast as tens of millions of matches per second on a modern computer. Typically, the faster you match, the less accurate the match is. This accuracy has been benchmarked by the U.S. Government since the early 1990s, and in a recent report from the National Institute of Standards and Technology in 2010, they said that the best face recognition algorithms are over 100 times better than they were a decade ago. So this means essentially from their report that an algorithm can determine if two faces belong to the same person 99.7 percent of the time, while only making a mistake about one in 1,000 times. In fact, face recognition is as good is as good as a human if the human is not a trained expert.

Now, these accuracy numbers are for a staged or controlled setting. When you have variable lighting, when the person is not looking directly at the camera, or when it is a low-resolution image, then the accuracy does decrease, and that is an active area of research.

Furthermore, when I quoted this 99 percent number, this is for verification when you are trying to determine if you are who you say you are, say, for instance, unlock your phone. Much more demanding is the application of identification where you are trying to determine an unknown identity from a gallery of individuals. So this would be where you are trying to generate an investigative lead from a mug shot data base.

Identification is more complicated because it is essentially like performing many verifications. So if you had to perform a million verifications, then you are going to have a higher false positive rate because you have more chances to make a mistake. And that is why with identification applications, there is almost always a human in the loop, and this is even the case when you have a photo-tagging feature and you have to sit there and you actually have to tell that algorithm, "Did you make a mistake or not?" "Yes, this is who the photo-tagging algorithm thinks it is."

So to summarize, and maybe speculate on the future a little bit, I do not think that the accuracy of face recognition for good-quality images will continue to improve at the rate that it has in the last 10 years. However, for the uncontrolled cases, where you are not looking at the camera, I do think that over the next couple decades, there will be a substantial improvement in accuracy to help these forensic type of face cases.

Thank you for the opportunity to address the Subcommittee. I look forward to answering any of your questions.

[The prepared statement of Mr. Martin appears as a submission for the record.]

Chairman FRANKEN. Thank you, Mr. Martin.

Mr. Acquisti.

STATEMENT OF ALESSANDRO ACQUISTI, ASSOCIATE PROFESSOR, HEINZ COLLEGE AND CYLAB, CARNEGIE MELLON UNIVERSITY, PITTSBURGH, PENNSYLVANIA

Mr. ACQUISTI. Thank you, Chairman Franken. It is an honor to appear before you today. I will discuss four findings from research on privacy and face recognition.

The first finding is that while early computer algorithms vastly underperform humans in detecting and recognizing faces, modern ones have progressed to a point that they can outperform humans in certain tasks and can be found in consumer applications. Later on, billboards predicted the age of pedestrians, cameras estimated generation of crowds in a bar, online social networks identified people and tagged their names in photos.

The second finding is that the convergence of face recognition, online social networks, and data mining will make it possible to identify people online and offline and infer sensitive information about them, starting from anonymous faces, and using only public data.

In one experiment we completed last year, we took anonymous photos from a popular dating site where people used pseudonyms to protect their privacy, compared them using face recognition to public but identified photos from Facebook, and identified about 10 percent of the anonymous members of the dating site.

In another experiment, we identified about one-third of the participants, students on a college campus, simply taking photos of them on a webcam and comparing these photos in real time to images from Facebook.

In a final experiment, we predicted the interests and Social Security numbers for some of the participants of the second experiment, combining face recognition with the algorithms we had developed in 2009 to predict SSNs from public data. We also developed a phone application which completes the process I just described on the mobile device in real time showing on the device screen the predicted sensitive information of the target subject overlaid on their face, and this is a screen shot of the application there.

Social Security numbers are just an example of many sensitive data it is possible to infer, starting from an anonymous face and using public data. The results we obtained are not yet scalable to the entire American population due to computational costs, false positives, availability of facial images. But each of these hurdles is being overcome by software and hardware improvements. In fact, some entities already have access to more powerful computational tools and larger and more accurate repositories of data than we do.

In particular, online social networks are accumulating the largest known data bases of facial images, often tagged or linked to identified profiles, providing a public connection between a person's facial biometrics and their real names.

The third finding is that the process through which face recognition can undermine our notions of privacy and anonymity has already started, and its consequences will be nuanced and complex. Your phone, we will remind you of the name of someone at a party. However, it will also tell a stalker in a bar where you live. The hotel will greet you as you arrive in the lobby. However, also such person may infer your credit score the moment you enter the dealership and also predict in real time based on your online posts a psychological profile for you, and, therefore, nudge you to accept the steepest price for a car. An agency will be able to find missing children in an online data base; however, another agency could chill free speech by identifying via remote, high-definition cameras all the thousands of participants in a peaceful protest.

The fourth finding is that, depending on which goals Congress intends to achieve in this area, different approaches may be considered: price of technologies, more commercial applications, legislation. However, if privacy and civil liberties are the concern here, it is not a given, not guaranteed that industry self-regulatory approaches will suffice. I say this for two reasons. One reason is that facial biometric data is particularly valuable. It provides a permanent, ubiquitous, and invisible means for identification and tracking online and offline.

First to control the base facial biometrics will be able to provide valuable identity recognition services to others. Hence, competition for control over the data will be fierce and will likely come at the cost of individuals' privacy.

The second reason is that recent history in the markets for personal data suggest that firms will engage in progressively more invasive applications of face recognition over time. Current users of face recognition are limited not just by computational costs but by fear of consumer backlash. These initial applications that we see, however, could be considered as "bridgeheads." In a way, they are designed to habituate us into accepting progressively more expansive services. Consider the frequency in which companies such as Facebook have engaged in changes to settings and defaults associated with users' privacy so as to nudge users into disclosing and sharing more. Why? Because information is power. In the 21st century, the wealth of data accumulated about individuals and the staggering progress of behavioral research in using the data to influence individual behavior make it so that control over personal information implies power over the person. As control is tilting from data subjects to data holders, it is the balance of power within different entities which is at stake.

Thank you.

[The prepared statement of Mr. Acquisti appears as a submission for the record.]

Chairman FRANKEN. Thank you, Mr. Acquisti.

Sheriff Amerson, please.

STATEMENT OF LARRY AMERSON, SHERIFF, CALHOUN COUNTY, ALABAMA, ANNISTON, ALABAMA, ON BEHALF OF THE NATIONAL SHERIFFS' ASSOCIATION

Mr. AMERSON. Mr. Chairman, thank you for inviting me today to testify today on behalf of the National Sheriffs' Association. Chartered in 1940, the National Sheriffs' Association is a professional association dedicated to serving the Office of Sheriff and its affiliates throughout law enforcement with education, training, and information resources. NSA represents thousands of sheriffs, their deputies, and other law enforcement professionals, and concerned citizens nationwide.

I applaud the Subcommittee for holding this important hearing on the implications of facial recognition for privacy and civil liberties. These are critical concerns that rightfully need to be debated and the rights of innocent citizens protected from unwarranted interference in their privacy and everyday lives.

On the other hand, new technologies, especially facial recognition, already implemented in law enforcement, national defense, and the fight against terrorism, are a critical tool in protecting the rights of citizens, in ensuring the accurate identification of suspects, prisoners, and potential terrorists while it is protecting the safety of our citizens and law enforcement officers.

There is a critical balance between protecting the rights of law-abiding citizens and providing law enforcement agencies with the most advanced tools to combat crime, properly identify suspects, catalogue those incarcerated in prisons and jails, and defending America from acts of terrorism.

Most importantly, advances in facial recognition technology over the last 10 years will result in the end of the total reliance on fingerprinting, where it can take hours and even days to identify a suspect, fugitive, or person being booked into a jail, to the immediate identification of those known to have criminal records or who are wanted by law enforcement. It will surprise many in the room today to know that there is no national data base of those incarcerated in America's jails at any one time. The use of facial recognition to provide instant identification of those incarcerated or under arrest will eliminate many problems while protecting innocent civilians and law enforcement officers.

For instance, utilizing facial recognition in law enforcement would:

- Interconnect law enforcement and intel organizations to instantly share vital information with accurate identification results;
- Establish a national data base of those incarcerated, past and present, wanted fugitives, felons, and persons of interest among all law enforcement agencies;
- Allow officers to quickly determine who they are encountering and provide notification if a suspect is wanted or a convicted felon;
- A simple, cost-effective, software-based solution delivered in Windows-based computers with inexpensive, non- proprietary, off-the-shelf cameras will provide a huge cost savings;

- Demonstrate new capabilities in alias detection, fugitive apprehension, and the speed of suspect recognition;
- Ensure correct identification of prisoners being released and reduce costs associated with administrative procedures;
- Establish a complete national data base of incarcerated persons for the first time in U.S. history; no longer could wanted criminals escape detection and arrest due to inefficient processes.

While fingerprints take hours and days for analysis, some advanced facial recognition in use today by U.S. law enforcement is as accurate as fingerprints, but results are obtained in seconds, not hours, in identifying criminals and perpetrators attempting to use false identities and aliases.

It is also important to point out that facial recognition comes in two general forms, two-dimensional and three-dimensional. Only All-aspect 3–D Facial systems can protect the privacy of participants who agree to be enrolled, except for in law enforcement or Homeland Security applications. All-aspect 3–D cannot search on 2–D facial photographs and cannot be invasive of privacy by design. All-aspect 3–D facial recognition systems remove skin color and facial hair and, therefore, have no profiling capability.

Currently, the National Sheriffs' Association, the Bureau of Prisons, and the United States Marshals Service are all in support of utilizing this new three-dimensional, holographic imaging technology to eliminate errors in identification; detecting false identities; and immediately identifying dangerous suspects, fugitives, or terrorists rather than learning who they are after they are released on traffic offenses or let go without suspicion because immediate identification is not possible.

Accidental releases, sometimes of dangerous felons, could also be eliminated. This technology has been in use for over eight years in Georgia detention facilities with data bases of approximately five million inmates without a single erroneous release.

And just last year, a dangerous murderer was released from the District of Columbia jail by switching a wrist band with another inmate. This cannot happen with facial recognition.

In closing, the proper utilization of facial recognition for intelligence or law enforcement uses can protect civil liberties, save millions of dollars, and instantly identify fugitives, felons, and dangerous suspects while saving lives.

Thank you, Mr. Chairman. I will be glad to answer any questions you may have.

[The prepared statement of Mr. Amerson appears as a submission for the record.]

Chairman FRANKEN. Thank you, Sheriff.

Ms. Farahany.

STATEMENT OF NITA A. FARAHANY, PROFESSOR OF LAW, DUKE LAW SCHOOL, AND PROFESSOR OF GENOME SCIENCES& POLICY, INSTITUTE FOR GENOME SCIENCES & POLICY, DUKE UNIVERSITY, DURHAM, NORTH CAROLINA

Ms. FARAHANY. Thank you. Chairman Franken and distinguished Members of the Subcommittee, thank you for the opportunity to express my views about facial recognition technology and its implications for privacy and civil liberties.

My fellow witnesses today have canvassed the science behind facial recognition technology and the myriad of privacy concerns about its use. Rather than repeat what has already been said, I will focus my comments on why I believe that law enforcement use of these technologies is not, in itself, a Fourth Amendment search, let alone an unreasonable one. Although the Supreme Court has not yet addressed this issue, as Senator Franken acknowledged earlier, the doctrine in analogous cases supports this view.

A novel feature of facial recognition technology is that the first step of the investigative process—scanning a face of interest—can be done from a distance and without the awareness of the individual being scanned. No physical contact, proximity, or detention of an individual is necessary for law enforcement to obtain a faceprint.

A faceprint is a form of identifying information that is the bread and butter of law enforcement: information about the physical likeness and other descriptive features of a suspect, which is routine practice for investigators to collect. Except in extraordinary circumstances, individuals have received only minimal constitutional protection against law enforcement collection of their personally identifying information.

The Fourth Amendment guarantees the right of the people to be secure in their person, houses, papers, and effects against unreasonable searches and seizures. A Fourth Amendment search only occurs when the Government intrudes upon a legally cognizable interest of an individual. This technology may be used in different ways which may require different Fourth Amendment analyses. It may be used from afar without a subject's awareness or during a brief investigative stop based on reasonable suspicion. Under either approach, I believe that the facial scanning itself is neither a search nor an unreasonable one.

If the police use facial recognition from afar without an individual's awareness, then no Fourth Amendment search has occurred. Neither his person nor his effects has been disturbed, and he lacks any legal source to support a reasonable expectation of hiding his facial features from Government view. He has chosen to present his face to the world, and he must expect that the world, including the police, may be watching.

Cameras and machines may now be doing the scanning, but for constitutional purposes, this is no different from a police officer scanning faces in public places. This has never been thought to be a Fourth Amendment search. But even if the use of this technology did constitute a search, it would likely be a constitutionally reasonable one, consistent with the Fourth Amendment.

Since the Court primarily uses property rights to inform Fourth Amendment privacy interests, it measures the reasonableness of a search based on the physical intrusiveness of the search rather than the personal indignity that one may have endured by having their personal information revealed. Mere observation without any physical intrusion is not tantamount to a search, and certainly not to an unreasonable one.

The police might instead choose to use facial scanning technology during a brief investigative stop, which requires a slightly different constitutional analysis. Beginning with *Terry* v. *Ohio*, the Court has held that if a police officer has a reasonable suspicion that somebody has committed, is committing, or is about to commit a crime, the police may detain the individual without a warrant. A facial recognition scan to achieve the same is not constitutionally distinguishable. Such stops are Fourth Amendment searches, and a person is seized while they are detained. But using facial scanning during the stop is unlikely to change the Fourth Amendment reasonableness. The individual privacy interest that the Court recognizes during stop-and-frisk detentions is the personal security of that individual and the interest against interference with his free movement, not the secrecy of his personal identity. In other words, the Court has not included secrecy of personally identifying information as a relevant privacy concern to determine the reasonableness of a stop.

The second step of the process, which is probing a data base for an identity match, is now a commonplace practice by law enforcement in other contexts. They regularly check local and national data bases to find the identity of individuals by using their license plates, Social Security numbers, fingerprints, or DNA, and all of this is nothing more than an automated version of what police have done for centuries: compare information acquired in the world with information held at police headquarters looking for a match.

Ultimately, the privacy concern advanced in most debates regarding facial recognition technology is whether an individual has a right to secrecy of their personal information. The Court has never recognized a Fourth Amendment privacy interest in the mere secrecy of identifying information. This is likely because intrusions upon possession and privacy are the core individual interests protected by the Fourth Amendment. And so from the beginning, the Court has turned to property law to inform Fourth Amendment interests.

Indeed, when the Court first encountered the modern investigative technique of wiretapping, which, like facial recognition, enables investigators to obtain evidence without physical interference, the Court found no search had occurred.

Now, to be sure, the Court has subsequently extended the Fourth Amendment beyond property. The Court has held that the Fourth Amendment applies to tangible and intangible interests such as private conversations. But even with this expanded view of individual interests, an individual who is facially scanned in public cannot reasonably claim that the police have searched or seized something that he has sought to seclude from public view. Instead, he must argue that he has a reasonable expectation of privacy in his personal identity associated with his facial features. Under current doctrine, courts would properly reject such a claim.

Most recently, in the *United States* v. *Jones*, the Court revisited this analysis. But what remains after *Jones* is an incomplete picture of which individual interest beyond real property interest, if any, the Fourth Amendment protects. The *Jones* majority emphasized that trespassed upon property and the *Katz* expectation-of-privacy framework co-exist under Fourth Amendment jurisprudence. But under either analysis, without trespass upon real property or upon information that a person has sought to hide, there is no legitimate source of law upon which a reasonable expectation of privacy could be founded.

Again, I thank you for the opportunity to appear before you today, and I look forward to your questions.

[The prepared statement of Ms. Farahany appears as a submission for the record.]

Chairman FRANKEN. Thank you, Doctor.

Mr. Sherman.

STATEMENT OF ROB SHERMAN, MANAGER OF PRIVACY AND PUBLIC POLICY, FACEBOOK, WASHINGTON, D.C.

Mr. SHERMAN. Chairman Franken, Members of the Subcommittee, my name is Robert Sherman. I am the manager of privacy and public policy at Facebook.

Facebook is committed to building innovative tools that enhance people's online experiences while giving them control over their personal information. We appreciate the opportunity to share our views on what the use of facial recognition technology means for our users.

Today I will describe how we use facial recognition technology as a part of our photo-sharing product, the important controls that we offer, and how Facebook safeguards the data that we use.

At the outset, I want to provide some background on why we offer photo-sharing features on Facebook. We learned early on how important photo sharing was to our users when we realized that people were frequently changing their profile photos to show friends recent snapshots. In response, we built tools that allowed people to upload and share photos, and we continue to build on those tools today.

One component of our photo sharing on Facebook is tagging, which is the 21st century version of handwriting captions on the backs of photos to label important events like birthdays or reunions and the people who participated. Tags promote transparency and control on Facebook because Facebook lets a person know when she is tagged. This allows the person included in the photo to interact with the user who uploaded it or to take action if she does not like the photo, for example, removing the tag or requesting that the photo be deleted.

Our Tag Suggestion tool uses facial recognition technology to automate the process of identifying and, if the user chooses, tagging her friends in the photo she uploads. Tag Suggestions work by identified similarities among photos in which a person has been tagged. We use this information to create a template that allows us to offer recommendations about whom a user should tag when she uploads a photo. The user can then accept or reject that recommendation.

Use of our photo-sharing tools continues to grow. In fact, as you noted, Mr. Chairman, a few months ago we took our Tag Suggestion feature down to improve its efficiency, and we plan to restore it soon.

Individual control is the hallmark of Facebook's Tag Suggestion feature. It includes four important protections.

First, we are transparent about the use of the technology. Across our site, we describe Tag Suggestions and the controls that we offer. This included providing information in our data use policy, on our Help Center, on our Privacy Settings page, and on our Facebook blog.

Secondly, Tag Suggestions only use data people have voluntarily provided to Facebook and derives information from that data to automate the process of future tagging. We do not collect any new information as a part of this process.

Third, Facebook's technology only uses a person's friends and does not enable people to identify random strangers.

Fourth, through an easy-to-use privacy setting, Facebook enables people to prevent the user of their images and tag suggestions. If a user makes that selection, Facebook will not include her name when suggesting tags for uploaded photos. And we will delete the template in which we stored the user's facial recognition data if one was previously created.

In addition to these controls, we protect facial recognition data from unauthorized disclosure to third parties, including to law enforcement. Two aspects of our technology significantly limit its use to third parties. First, our templates are encrypted, and they work only with our proprietary software, so they would be useless to a third party. Second, our software is designed to search only a limited set of potential matches, namely, an individual user's friends, and is not used to identify strangers.

Last, we share our users' private information with law enforcement only in very limited circumstances and consistent with our terms of service and applicable law. A dedicated team of professionals scrutinizes each request for legal sufficiency and compliance with Facebook's internal requirements. We are one of the handful of major Internet companies that promotes transparency in this process by publishing our law enforcement guidelines on our website.

I hope that my testimony has helped the Members of this Subcommittee understand how Facebook uses facial recognition technology and, more importantly, the privacy and security protections that define our implementation. We look forward to continuing our discussion with Members of Congress about the important issues raised in today's hearing.

Thank you again for the opportunity to testify, and I look forward to answering any questions that you have.

[The prepared statement of Mr. Sherman appears as a submission for the record.]

Chairman FRANKEN. Well, thank you, Mr. Sherman.

Ms. Lynch.

STATEMENT OF JENNIFER LYNCH, STAFF ATTORNEY, ELECTRONIC FRONTIER FOUNDATION, SAN FRANCISCO, CALIFORNIA

Ms. LYNCH. Mr. Chairman, thank you very much for the invitation to testify on the important topic of facial recognition today. My name is Jennifer Lynch, and I am an attorney with the Electronic Frontier Foundation in San Francisco. We are a nonprofit, and for over 20 years, we have been focused on protecting privacy and defending civil liberties in new technology.

Today, and in my written testimony, I would like to address the implications of government and private sector use of facial recognition on privacy and civil liberties and on the laws that do or do not apply.

The collection of biometrics, including facial recognition, may seem like science fiction or something out of a movie like "Minority Report," but it is already a well-established part of our lives in the United States. The FBI and the DHS have the largest biometrics data bases in the world, with over 100 million records each, and DHS alone collects 300,000 fingerprints every day. Both of these and other agencies in the Federal Government are working quickly to add extensive facial recognition capabilities to these data bases.

The scope of Government-driven biometrics data collection is well matched by private sector collection. Facebook, for example, uses facial recognition by default to scan all images uploaded to its site, and its 900 million members upload 300,000 photos every day. Face.com, which is the company that developed Facebook's facial recognition system and was recently acquired by Facebook, stated in March that it had indexed 31 billion face images. Other companies, from Google and Apple to smartphone app developers, also provide facial recognition services to their customers, and biometrics are used by private companies to track employee time, to prevent unauthorized access to computers or facilities or even the gym. And private companies, like Morpho, represented on the panel here today, and other companies, are building out large facial recognition systems for governments and agencies around the world.

For example, Morpho has developed a facial recognition technology at 41 of the 50 DMVs in the United States and for the FBI. And companies like this often retain access to the data that is collected.

So facial recognition is here to stay, and yet at the same time many Americans do not even realize that they are already in a facial recognition data base.

Facial recognition technology, like other biometrics programs that collect, store, share, and combine sensitive and unique data poses critical threats to privacy and to civil liberties. Biometrics in general are immutable, readily accessible, individuating, and can be highly prejudicial. And facial recognition takes the risks inherent in other biometrics to a new level. Americans cannot take precautions to prevent the collection of their image. We walk around in public. Our image is always exposed to the public. Facial recognition allows for covert, remote, and mass capture and identification of images, and the photos that may end up in a data base include not just a person's face but also what she is wearing, what she might be carrying, and who she is associated with. This creates threats to free expression and to freedom of association that are not evident in other biometrics.

Americans should also be concerned about the extensive sharing of biometric data that is already occurring at the government- and private-sector level. Data accumulation and sharing can be good for identifying people, for verifying identities, and for solving crimes. But it can also create social stigma when people end up in criminal data bases and their image is searched constantly. And it can perpetuate racial and ethnic profiling and inaccuracies throughout the system. It can also allow for Government tracking and surveillance on a level that has not before been possible.

Americans cannot participate in society today without exposing their faces to public view. And, similarly, connecting with friends, family, and the broader world through social media has quickly become a daily—and many would say necessary—experience for Americans of all ages. Though face recognition implicates important First and Fourth Amendment values, it is unclear whether the Constitution would protect against the challenges it presents. Without legal protections in place, it could be relatively easy for the government or private companies to amass a data base of images on all Americans. This presents opportunities for Congress to develop legislation to protect Americans. The Constitution creates a baseline, but Congress can and has legislated significant additional privacy protections. As I discuss in more detail in my written testimony, Congress could use statutes like the *Wiretap Act* or the *Video Privacy Protection Act* as models for this legislation.

Given that facial recognition and the accompanying privacy concerns are not going away, it is imperative that Congress and the rest of the United States act now to limit unnecessary biometrics collection, to instill proper protections on data collection, transfer, and search, to ensure accountability, to mandate independent oversight, to require appropriate legal process before government collection, and define clear rules for data sharing at all levels. All of these are necessary to preserve the democratic and constitutional values that are bedrock to American society.

Thank you once again for the invitation to testify today. I look forward to your questions.

[The prepared statement of Ms. Lynch appears as a submission for the record.]

Chairman FRANKEN. Thank you all for your testimony.

Just for the sake of the record, I want to clarify that Facebook users upload 300 million photos to the site a day, not 300,000. I will add a document to the record to that effect. I would not want to underestimate the power of Facebook.

[The information appears as a submission for the record.]

Chairman FRANKEN. Professor Acquisti, one of the things I think is so special about your work is that it really shows us how a face can be a real conduit between your online world and your offline world in a way that other biometrics are not. Can you tell us why facial recognition technology is so sensitive and how it compares to taking someone's fingerprint and analyzing that?

Mr. ACQUISTI. Senator, I believe facial biometrics are a more powerful and sensitive biometrics than fingerprints. Not only they are permanent, starting with childhood your face changes, but computers are learning to be able to predict these changes, and your face can be changed, as you mentioned earlier, only at very great cost. Also, this biometric can be captured remotely. In fact, we have a gigapixels camera, very remotely shot can be sufficient to make a good, effective faceprint of someone's face. Remote capturing means that this is happening without the person's consent or even knowledge.

Also, the technology to capture facial images and do matching is becoming ubiquitous. Your phone probably can do it, my phone, iPad, and so forth.

Also, unlike fingerprints, which are not usually publicly available online, facial data is, as our experiment showed and studies by others have shown, plenty available online.

And, finally, as you mentioned, a face is truly the conduit between your different personas, who you are on the street, in real life, and who you are online, who you are online may be on a dating site, and who you are on a social network. And the face, therefore, allows these different sides of your life that you wanted to keep, perhaps, compartmentalized to be connected. Plus there is also the issue of the sensitive inferences one can make starting from a face, which is perhaps another story, but it is related to this topic as well.

Chairman FRANKEN. Thank you.

Mr. Sherman, you have heard from almost everyone else at this hearing that facial recognition technology is extremely powerful and extremely sensitive. Why doesn't Facebook turn its facial recognition feature off by default and give its users the choice to turn it on?

Mr. SHERMAN. Well, Senator, I think you are right to say that, like all of the other information that we store about our users, it is important that we take appropriate steps to protect information. We take that responsibility very seriously. And in terms of implementing choice throughout our site, and we do that in a lot of ways, we use a number of different mechanisms to do it.

As you point out, with regard to the tag suggestion feature specifically, it is turned on by default, and we give people the opportunity to go in and disable it if they do not want to use it.

The reason for that in part is we think that is the appropriate choice because Facebook itself is an opt-in experience. People choose to be on Facebook because they want to share with each other. Beyond that, tag suggestions are only used in the context of an opt-in friend relationship on Facebook, which means that you would not be suggested to somebody as a potential tag for a photo unless both parties to the relationship had already decided to communicate with one another on Facebook, had already seen each other's photos. So we are actually not exposing any additional information to anybody as a part of this process.

And so given those things and the fact that we do a lot to be transparent and to let people know about the feature, we think that it is the right choice to let people who are uncomfortable with it decide to opt out.

Chairman FRANKEN. I understand what you are saying. We are just going to have to disagree on this a little bit. I just think that this information is so sensitive that it is the kind of thing that users should have to consciously opt themselves into. I will note that Facebook's competitor Google leaves their facial recognition feature off by default on its social network and then lets users opt into it. But I am worried about how Facebook handles the choices that it does give its users about this technology.

Mr. Sherman, on page six of your written testimony, you write that, "Through an easy-to-use privacy setting, people can choose whether we will use our facial recognition technology to suggest that their friends tag them in photos."

This is the screen that Facebook users get when they go to their privacy settings to find out about tag suggestions. Nowhere on this screen or on the screen that you get when you click "Learn More" do you see the words "facial recognition" or anything that describes facial recognition. Those words are elsewhere in your Help Center, but right now you have to go through six different screens to get there. I am not sure that is easy to use.

How can users make an informed decision about facial recognition in their privacy settings if you do not actually tell them in their privacy settings that you are using facial recognition?

Mr. SHERMAN. Well, the screen shot that you have displayed does not use the words "facial recognition." I believe that the "Learn More" link at the bottom leads to the page in our Help Center. We have a series of frequently asked questions that we provide to users that explains in detail how——

Chairman FRANKEN. This is the page that it links to.

[Laughter.]

Chairman FRANKEN. And nowhere does it talk about a facial recognition page, right?

Mr. SHERMAN. I have not done that, so I do not know that——

Chairman FRANKEN. You have not done that?

Mr. SHERMAN. I have done that. I did not create the visual, so I do not know that, but I can tell you that——

Chairman FRANKEN. What haven't you done?

Mr. SHERMAN. I am sorry. I just have not seen the visual. I think the page that you are looking at is one of the pages in our Help Center that provides information about how tagging works on Facebook. The Help Center content that you are talking about, which I think is available from that page, does describe facial recognition, uses the words "facial recognition" specifically, and provides some detail about the way in which the templates that we use, the files that include the facial recognition data are stored.

Chairman FRANKEN. It is my understanding, am I right, that that is six clicks away?

Mr. SHERMAN. I am not sure about the number. I do not think that is right, but I am not sure.

Chairman FRANKEN. OK. You are head of this at Facebook?

Mr. SHERMAN. I am one of many people who work on privacy at Facebook.

Chairman FRANKEN. What is your title?

Mr. SHERMAN. I am the manager of privacy and public policy.

Chairman FRANKEN. Thank you, Mr. Sherman.

Mr. SHERMAN. Thank you.

Chairman FRANKEN. Ms. Lynch, you are a privacy and civil liberties lawyer. It is your job to interpret the law in a way that protects privacy and civil liberties. Can you summarize for us in a few sentences what concrete legal protections there are with respect to the use of facial recognition technology by the government and by the private sector?

Ms. LYNCH. Well, I think at the Federal level it is pretty clear that there are no specific laws that regulate facial recognition or that regulate the collection of images to be put into a facial recognition data base, whether from the government or the private sector.

That said, the Constitution creates a baseline. I think we have seen in the *U.S.* v. *Jones* case that was decided in January that the Supreme Court and several other courts are concerned about collection of information on us when we are in public. And, also, the FTC, of course, has some ability to regulate companies that are engaged in deceptive or unfair trade practices. And then there are two State laws, which you mentioned earlier, in Illinois and Texas, that would govern the collection of biometrics on citizens within those States.

Chairman FRANKEN. Thank you.

Right now, I know Senator Blumenthal has been here for a while. Since I am chairing this, I am going to be here. I want to be conscious of your time, so why don't I turn the questioning over to you, Senator?

Senator BLUMENTHAL. Thank you, Mr. Chairman.

Mr. Sherman, let me first thank Facebook for being so cooperative in the Password Protection Act that I proposed, with the support of a number of other Members of the Judiciary Committee, that prohibits employers from compelling passwords and other such information that provides access to private personal accounts to being divulged in the course of employment, whether it is applications for employment or prospective employment or existing employment.

Why does Facebook not require or not permit the kind of opt-in procedure that Senator Franken mentioned?

Mr. SHERMAN. Well, we do not provide—we have implemented tag suggestions in a way that does not require people to opt in for a number of reasons, including the fact that, as I mentioned, Facebook is an opt-in service and the fact that we provide tag suggestions only in the context of existing friendships.

I think we also work very hard to be transparent with people about how the feature works. We provide information about the tool on a lot of different places on the site. And we also think that there are benefits both in terms of social engagement and also in terms of privacy associated with photo tagging. And we think that making it easier for people to tag people on Facebook, again, people that they already know and already are in relationships with, promotes those benefits. It gives people the ability to know that they are in photos that have been posted on Facebook and to exercise control over them if they want to do so.

Senator BLUMENTHAL. Does Facebook share facial recognition data with any third parties?

Mr. SHERMAN. We do not.

Senator BLUMENTHAL. Is there anything in your guidelines or company practices that precludes it?

Mr. SHERMAN. As I mentioned, we publish on our website our law enforcement guidelines, which I think may be the circumstance that you are talking about, and with regard to that information, first, we—as far as I know, we have never received a request from law enforcement from the information that you are talking about. I think that reflects the fact that the templates that we have would not be useful outside of our service. They just cannot be used by law enforcement. I think there are other technologies that law enforcement might use. And I think beyond that there is a very rigorous standard that we describe in our policies under which we would provide any non-public personal information to law enforcement.

Senator BLUMENTHAL. And what about going beyond law enforcement? Is there anything in your guidelines or practices that precludes sharing with non-law enforcement?

Mr. SHERMAN. I do not know whether we have said specifically with regard to facial recognition information, but we have a data use policy which we publish on our website which provides significant detail about the restrictions, and the general standard is that we do not disclose personal information to third parties without our users' consent.

Senator BLUMENTHAL. Does Facebook allow third-party apps to collect facial recognition data from users?

Mr. SHERMAN. Just to make sure I understand your question, Senator, the facial recognition data that is in our data bases, the templates?

Senator BLUMENTHAL. Correct.

Mr. SHERMAN. No, we do not provide those to any apps.

Senator BLUMENTHAL. And just assume that someone signs up for Facebook—you mentioned that it is, obviously, voluntary—and he or she does not want to have facial data stored, collected, used by Facebook. What are the options available to that person?

Mr. SHERMAN. So if a person signs up for Facebook and does not want facial recognition data to be collected or used about that person, the person can go to their Privacy Center, click on Tagging, and then the option to turn off the tag suggestion feature is there. If they do that, two things will happen: one, we will not suggest them to any of their friends when their friends upload photos; and, two, if a facial recognition template was created, it will be deleted. In the circumstance that I think you are describing, we probably would not have a facial recognition template in the first instance.

If a user wanted to allow the use of the feature but to exercise other kinds of control, we offer that as well. For example, the user can be notified when he or she is tagged, can remove the tag from the photo. If he or she does that, then that removes that from the template that we use to power our tag suggestions feature.

And, finally, the user can choose to exercise control before any photo in which he or she is tagged shows up on her timeline.

Senator BLUMENTHAL. Now that Facebook is considering allowing children under 13 to sign up for Facebook accounts, which obviously implicates a number of privacy concerns of a different nature and magnitude, does Facebook have any new policies or plans to develop new policies and what will those policies be regarding facial recognition technology on pictures of children who use Facebook?

Mr. SHERMAN. Well, Senator, as you know, our current policy is that children under 13 are not allowed on Facebook, and we have a number of technical and procedural measures that we put in place to try to prevent children under 13 from gaining access to our service in violation of that policy.

There have been some studies that have come out recently that have suggested that children, despite our efforts, are gaining access to Facebook, and in many cases with the assistance of their parents. And so one of the things that has been suggested is that we provide tools for parents to manage their children's access of Facebook if they do get on.

We are in the process of thinking about those. Those are really important issues, and protecting children and all of our uses is a high priority at Facebook. And we are thinking through the right way to manage those questions. So we have not made any final decision about what we would do, if anything, about changing our under-13 policy.

What I can tell you is we do implement the tag suggestion feature in a slightly different way for children who are over—for teenagers, excuse me, who are over 13 but under 17. In those cases, the tag suggestion feature is off by default, and the teenagers can turn it on if they want to do so, but it is not on by default.

Senator BLUMENTHAL. Wouldn't it make sense to simply preclude those images for children under 13 to be in any way collected or stored?

Mr. SHERMAN. Well, I mean, I think certainly there are difficult questions, and the one that you raise is one of a large number of questions that we would have to confront if we decided to allow children under 13. It is something certainly that we would consider actively, but until we make a decision about changing our policy, I think it is premature to say exactly how we would implement it.

Senator BLUMENTHAL. Well, I am going to ask that Facebook commit to not collecting or storing those facial recognition data for anyone under 13 if you decide to go ahead. I think it is a matter of public policy and public safety that Facebook adopt that kind of policy if you decide to go ahead.

Mr. SHERMAN. OK, thank you. We absolutely appreciate the feedback, and if we go in that direction, that is something we will certainly consider.

Senator BLUMENTHAL. Thank you.

Thank you, Mr. Chairman.

Chairman FRANKEN. Thank you, Senator Blumenthal.

I just want to also correct the record that MorphoTrust has 32 driver's license contracts that include facial recognition, not 40.

Professor Acquisti, a month or two ago, a company called Face.com released an iPhone app that allowed you to point your iPhone at someone and have a little box pop up above that person's face on your screen that told you their name. The app was only supposed to work on your friends, but soon after the release of this app, a well-respected security researcher who has testified before this Subcommittee, Ashkan Soltani, revealed that the app could easily be hacked in a way that would appear to allow it to identify strangers.

Facebook has since purchased Face.com and shut down this app. But were you familiar with this app and the vulnerability that it created or had? What did it tell you about the state of privacy when it comes to facial recognition technology? Is this something we should be thinking about?

Mr. ACQUISTI. Senator, yes, I have been following the news and the research about Klik, this app. I will make a few points.

One is that this app shows that the studies we presented last year are not just theoretical experiments. They happen in reality. The reality of face mobile, real-time face recognition is coming much faster than what some people may have believed.

A second point is that the vulnerability Ashkan Soltani found shows that there are inherent risks in this technology in that they cluster and aggregate very sensitive information which becomes a desirable target for hackers and third parties. Soltani was able, through the vulnerability he discovered, to get access to non-public photos of individuals as well as to private data of other users, which means that conceivably he could have used these additional photos for face recognition not just of his own friends but friends of friends and many other people in the network.

Which leads me to the third point. Currently, the limitations in this app come mostly from two directions. One is computational cost. In experiments we did, we were working on data bases of hundreds of thousands of images; therefore, we could do a match in real time. If we had tried to do it against 300 million Americans or, in fact, 90 billion photos, it would take hours and hours and hours. However, this limit is transient; it is not systemic in the sense that cloud computing clusters are getting faster and faster. Therefore, we cannot guarantee that what is not possible to do now, extrapolating our results to nationwide to the entire population, will not be possible five years out.

The second limitation is, like I mentioned in my testimony, there is a sort of a self-restraint in the providers of the services which can be found in statements such as, “Don’t worry. This only works with your friends. Only your friends will be able to tag you.” Well, this is now. There is no guarantee that a few years from now it will be friends of friends or some years later it will be anyone in the network. In fact, the history of social media and online social networks in general shows that there is this progressive nudging of users toward more and more disclosure. So this is to me one of the concerns we have in this area.

Chairman FRANKEN. Well, then, I will turn to Mr. Martin. I am going to try to get everybody in here. We are really talking about how fast this technology is improving, and that is sort of what I was just asking Mr. Acquisti. What are we approaching? What kind of world are we approaching in terms of how quickly and reliably this technology can identify unknown individuals walking down a city street? I know we are not quite there yet, but tell me how fast this technology is improving and how far we are from that world.

Mr. MARTIN. There is not a black-and-white answer to this. So certainly, today, if you have a small data base of individuals, a few thousand or even tens of thousands, and you had a controlled situation where somebody was walking through a metal detector but still they did not know the camera was on them, then you could reliably do identification on that small data base, say if you had a watchlist of criminals or terrorists or something.

In the case where you now expand the data base to the size of multiple millions and you are just shooting a camera outside the window down the street, you cannot reliably do that for a large data base. What you could do is, for instance, have some humans that look at the results, and if you only were looking for a few people, not millions of people, then you could shoot something out the window and probably try to find a suspect. But certainly the technology is not there to do that on a large scale with 300 million people or a billion people. And even if you have more processors and it is faster, I do not think you are going to be there in the next several years.

Chairman FRANKEN. What about the scenario of going into—a guy goes into a bar, takes a picture of a woman, wants to stalk her, can find out where she lives?

Mr. MARTIN. Some of the arguments here was that that is a concern that you can do something like that, and I think the only way it would be viable today is that you would need some additional information. Like you would have to know that she is a friend of somebody on Facebook and you are a friend with that person and you have access to see who their friends are. Then potentially you could look at images off of the Internet and link up that extra metadata that is on her profile with that picture and find out that information.

But even just from the science side of it, taking a picture in the bar where it is dark and the person is not looking at your camera unless you ask them for a good picture, it is technically very hard even to do the face recognition matching, despite the other part that you need to have all this linking information to get it to work. So it is not easy.

Chairman FRANKEN. Sometimes you would say, "Hey"——

Mr. MARTIN. "Can I get a picture of you?" Right.

Chairman FRANKEN. A flash, and there it is.

Mr. MARTIN. Right. So if you did that, though, then the question is: What is the data base that you are going to search against?

Chairman FRANKEN. I just want to ask this with Mr. Acquisti and Mr. Sherman. Mr. Acquisti said that the social networks—the privacy policy has sort of loosened in a way. What did you mean by that in terms of—let us just get a little dialogue maybe between the two of you just on this. Has Facebook done that? Have they loosened their privacy policies? You are nodding, Ms. Farahany, so—I just go to whoever is nodding. That is my role as Chairman.

[Laughter.]

Chairman FRANKEN. If you want to get called on, nod.

Ms. FARAHANY. I am happy to nod and be called on. I think Facebook and other social media sites are changing our expectations of privacy. So I think part of the reason why the Fourth Amendment analysis is useful here is that it is tied to what does society expect to be able to keep private. And in today's world, we are moving toward much greater transparency. As I have been listening to the conversation, it does not seem like it is facial recognition itself that anybody is afraid of. It is linking it to other information that people are frightened by. And I think that is right, which is, there is nothing inherently frightening about having your face seen. We have it seen in public all the time. We do not try to hide it from view. It is the aggregation of data that frightens people.

And so what is it, if anything, we should be doing about aggregation of data? Well, Congress has already taken a number of initiatives to keep some types of personal information private, like your health information, financial transactions, your genetic information for certain types of uses through the *Genetic Information Nondiscrimination Act*. But we do not stop the flow of information. We say there are certain applications of the information which are limited or impermissible. And I think there is nothing about for me personally—and this may be because, you know, I am a user of Facebook and somebody who is comfortable with greater transparency. There is nothing frightening to me about somebody having a photograph taken of me or even going into every store or every place on the street and having a photograph taken of me. It is the ability to make a complete dossier about me and know a lot of other information.

And so if there is something about the use and application that we are frightened about, I think that is an appropriate place for Congress to focus very targeted interest, but it may not be facial recognition technology it should be focusing on then. It is the act of data aggregation itself and who can aggregate data, for what purpose, and to whom they can package and sell it.

Chairman FRANKEN. OK. Now, you are nodding, so that means you are going to be called on.

Mr. ACQUISTI. I was nodding, Senator. In my written testimony, I made a short list of examples where Facebook indeed changed something—settings, defaults—to unilaterally create more disclosure or more sharing. The examples include Facebook News in 2006, Tagging in 2009; changes in privacy settings in early 2010; changing of the cache time limits in 2010—that refers to how long third-party developers can keep your data; the introduction of Facebook Places in 2010, which allows others to tag you when you go in a certain location; the switch to the “Timeline” in early 2012, initially voluntary, then compulsory; more recent the switching of users to using Facebook emails rather than other parties’ emails. So there is an extensive list of examples showing this trend.

Chairman FRANKEN. How do you respond to that?

Mr. SHERMAN. Well, I think the examples that Professor Acquisti is offering are examples of ways in which we have changed our service, and I think you would want Facebook to innovate, you would want Facebook to continue to offer new and better products to our users, and that is something that we try to do every day. Anytime we make any change to our service, including the changes that Professor Acquisti referred to, we have a robust privacy process that includes professionals from all across our organization who review those changes to make sure that they are consistent with the commitments that we have made to our users and that they will help us maintain the trust of our users, because, after all, if people do not trust us, then they will not use our service, and that is something we very much want people to do. And I think if we did make a change of any sort—and I think in the instances that he has described—we let our users know about that and give them the ability to make choices about them.

Chairman FRANKEN. OK. And did it involve information retrospectively? In other words, did it involve loosening the privacy on information they had already put in there that they did not know would—I am saying this out of ignorance here. I am just asking.

Mr. SHERMAN. There may be instances where we would change a default, so for new people who come onto the site, things might work in a slightly different way, and we would be very clear with them about how that works. But we have committed to the FTC that when we have information that we already have that is covered by a privacy setting, we will not disclose it in a way that materially exceeds the privacy setting after that has been done.

Chairman FRANKEN. OK. Thank you.

I want to go to Ms. Lynch in kind of a final question, but I have not talked to the sheriff yet, and I want to thank you for being with us. I know that right now Calhoun County is about to roll out a facial recognition system for the field. If your deputy pulls someone over and that person refuses to identify him- or herself, this system will allow you to see if they are a wanted criminal or someone with an arrest record.

Now, I know that the data base of photos you are using for this field system is still going to be a data base of mug shots from arrests.

Mr. AMERSON. Right.

Chairman FRANKEN. It is not going to be the data base from the Department of Motor Vehicles. Can you tell us why you decided to stick with the criminal data base and not use a bigger data base like the DMV's?

Mr. AMERSON. I think the key is for us to focus on the people that are of interest to us. Ordinary, honest people going about their daily business are not of interest to us. Our interests are people who are committing crimes, people who are wanted for questioning about crimes. It would have to be a very certain degree of information allowed—available for us to do that. But, again, the key to us is locating wanted criminals so that we can locate and arrest them and take them off the street.

Chairman FRANKEN. Thank you.

Ms. Lynch, if Congress were to pass a law governing law enforcement use of facial recognition technology, what are the two or three protections you think need to be included?

Ms. LYNCH. Well, I think first we have to look at how law enforcement is getting the data. So law enforcement is currently getting data in general in two different ways. One is directly, so let us say they are bringing a suspected criminal into a police department and fingerprint them, or they are collecting an image on the street. And then the second way that law enforcement gets data is from a private company or a third party—bank records or data from Facebook, submitting a warrant to Facebook. And I think in both of those situations, we would like to see a warrant based on probable cause to get access to the data.

Facial recognition data and faceprints and photographs are pretty sensitive data, and everyone though we do share our faces with the public and we share our images with third parties, there has been a lot of significant research done to show that people still have an expectation of privacy in this information. Even though we are sharing it with our friends and our family and our networks, we are not necessarily expecting that that data should be shared with the Government. And I think based on that, we do have a reasonable expectation of privacy in the data that would warrant a warrant standard. So that is the first thing.

I think the second thing that I would like to see is that there would be some data minimization requirements put in place. This could be minimization of how much data the gvernment collects, so instead of getting 10 pictures of a person or crowd photos of a person—that include a person, it is limited to mug shots like the sheriff said. So that is one way of minimizing the data collection. Another is if the government is collecting crowd photo data for an individual investigation, that that crowd photo be deleted once the investigation is concluded, or that other faces in the crowd be scrubbed so that they are not identifiable. So that is the second.

And then I think the third thing that I would like to see is that data that is gathered for one purpose is not combined with data gathered for another. So, for example, right now the FBI has two separate parts to its fingerprint data base. It has the records collected for civil purposes, like employment. If you are Federal employee, if you are a lawyer in California, if you are applying for a job to work with children, your fingerprints are collected and put in the FBI's civil fingerprint data base. And that is kept separate from the criminal data base where all of the fingerprints of anybody arrested in the United States go. And, currently, although those are kept separate, the FBI is planning to incorporate a master name system that would allow searching of both data bases at the same time, and I think this raises a lot of implications for privacy and civil liberties that we have not discussed. And even though we are talking about fingerprints here, when the FBI includes facial recognition into its data base—and it is supposed to do that by 2014—they will be searching facial recognition-ready photographs as well.

Chairman FRANKEN. Thank you.

I have a note here that Professor Farahany has a plane to catch. Is that correct?

Ms. FARAHANY. My flight is at seven.

Chairman FRANKEN. I am sorry?

Ms. FARAHANY. I said my flight is at seven.

Chairman FRANKEN. Let us see. It is rush hour. Is it National or Dulles? Dulles.

[Laughter.]

Chairman FRANKEN. Are you checking any bags?

[Laughter.]

Chairman FRANKEN. OK. Well, I will ask my last question, and then you can get out of here.

Mr. Sherman, once you generate a faceprint for somebody, even though you might not do it now, you can use it down the road in countless ways. You could. I would like for you to tell us on the record how Facebook will and will not use its faceprints going forward. We did have the matter of some changes in policy. For example, can you assure us that Facebook will share or sell users' faceprints along with the software needed to use them to third parties—will not do that? Can you assure us that they will not do that?

Mr. SHERMAN. Well, Senator Franken, I think it is difficult to know in the future what Facebook will look like five or 10 years down the road, and so it is hard to respond to that hypothetical. What I can tell you is that we have a robust process, as I have described, to vet any changes that we would make along those lines. We also have relationships with the Federal Trade Commission, the Irish Data Protection Commissioner which regulates our Irish affiliate, and consumer groups like the Electronic Frontier Foundation. We talk with them regularly about changes that we are making or are planning to make. I think if we would make a change that would be concerning, those are certainly groups that would express concern, and we obviously would be transparent with any change with our users.

Chairman FRANKEN. Well, I think that is a fair answer. Your company has every right not to lock itself into future business decisions and to keep your options open. But perhaps that is why Congress should be looking at this and considering whether we need to put in place protections so that users' faceprints are never shared or sold without their explicit permission, for example.

Well, I want to thank you all for joining us. Ms. Farahany, you—you are all permitted to bolt.

[Laughter.]

Chairman FRANKEN. But I want to thank you and, again, your complete written testimonies will be made part of the record.

In closing, I want to thank Ranking Member Coburn, and I want to thank each of the witnesses who appeared with us today. I will add a statement from EPIC to the record.

[The statement appears as a submission for the record.]

Chairman FRANKEN. We are adjourned. Thank you. Thank you all.

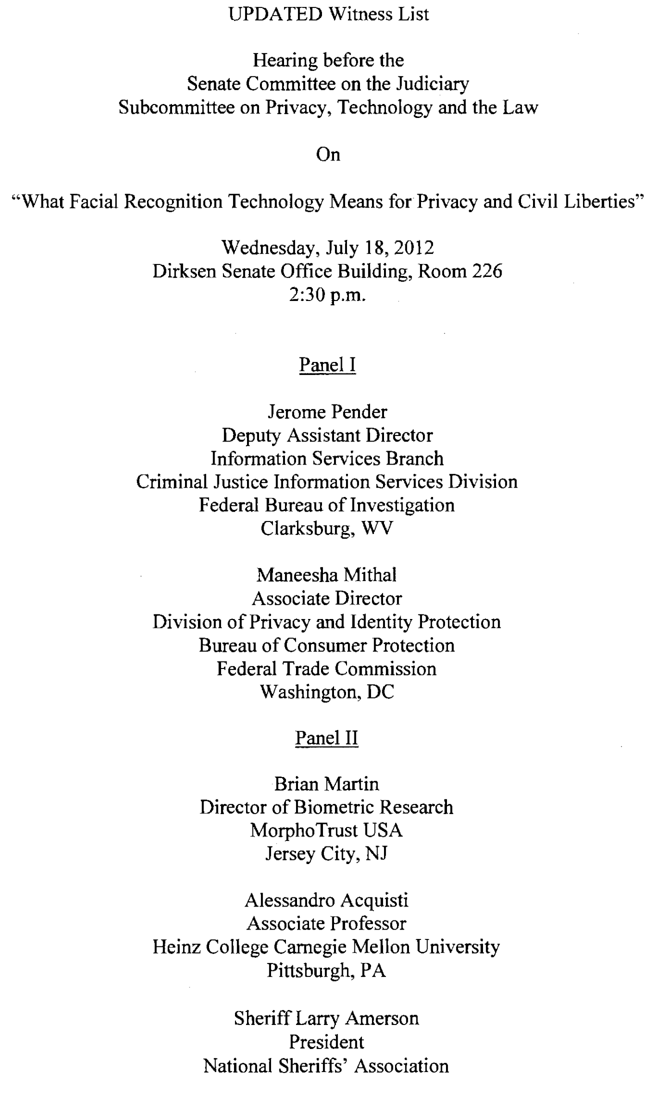
[Whereupon, at 4:35 p.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

APPENDIX

Additional Material Submitted for the Record

Witness List



UPDATED Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

On

"What Facial Recognition Technology Means for Privacy and Civil Liberties"

Wednesday, July 18, 2012
Dirksen Senate Office Building, Room 226
2:30 p.m.

Panel I

Jerome Pender
Deputy Assistant Director
Information Services Branch
Criminal Justice Information Services Division
Federal Bureau of Investigation
Clarksburg, WV

Maneesha Mithal
Associate Director
Division of Privacy and Identity Protection
Bureau of Consumer Protection
Federal Trade Commission
Washington, DC

Panel II

Brian Martin
Director of Biometric Research
MorphoTrust USA
Jersey City, NJ

Alessandro Acquisti
Associate Professor
Heinz College Carnegie Mellon University
Pittsburgh, PA

Sheriff Larry Amerson
President
National Sheriffs' Association

Anniston, AL

Nita A. Farahany
Professor of Law and Professor of Genome Sciences & Policy
Duke University
Durham, NC

Rob Sherman
Manager of Privacy and Public Policy
Facebook
Washington, DC

Jennifer Lynch
Staff Attorney
Electronic Frontier Foundation
San Francisco, CA

PREPARED STATEMENTS OF WITNESSES

Department of Justice

STATEMENT

OF

JEROME M. PENDER
DEPUTY ASSISTANT DIRECTOR
CRIMINAL JUSTICE INFORMATION SERVICES DIVISION
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW
COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

AT A HEARING ENTITLED

"WHAT FACIAL RECOGNITION TECHNOLOGY MEANS FOR
PRIVACY AND CIVIL LIBERTIES"

PRESENTED

JULY 18, 2012

Jerome M. Pender
Deputy Assistant Director
Criminal Justice Information Services Division
Federal Bureau of Investigation
U.S. Department of Justice

Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate

"What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

History of the Criminal Justice Information Services Division

The Criminal Justice Information Services (CJIS) Division, the largest division in the FBI, was established in February 1992 to serve as the focal point and central repository for criminal justice information services. Collection of fingerprints by the FBI had begun 70 years earlier with the creation of the FBI's Identification Division in 1924. Prior to 1924, states maintained individual repositories of fingerprints and shared information at the state level. It was not until 1924, with the creation of the FBI's Identification Division, that fingerprints were shared on a national level. From 1924 until 1999, fingerprints and associated criminal history information, including mug shot photographs, were received in the U.S. mail and processed manually. In 1999, with the launching of the Integrated Automated Fingerprint Identification System (IAFIS), fingerprints and associated criminal history information were searched, processed, and stored.

Next Generation Identification

The FBI initiated the Next Generation Identification (NGI) Program in response to advances in technology, FBI customer requirements, growing demand for IAFIS services, and growing obsolescence of the IAFIS Information Technology infrastructure. The NGI Program, which is on scope, on schedule, on cost, and 60 percent deployed, is enabling the FBI to meet its criminal justice mission and continue to build its reputation as the global leader in biometrics. The NGI Program is dramatically improving the major features of the current IAFIS, including system flexibility, storage capacity, accuracy and timeliness of responses, and interoperability with other systems. The NGI Program is addressing the increase in identification requests, in the form of biometric submissions, and the rapidly expanding database of biometric information and new biometric identifiers concomitant with evolving tribal, local, state, federal, international, and intelligence requirements. NGI improvements and new capabilities are being introduced across a multi-year time frame through a phased, incremental approach, resulting in a flexible framework of core capabilities that will serve as a platform for multimodal functionality.

General Authority for Next Generation Identification Initiatives

28 U.S.C. § 534 authorizes the FBI to acquire, collect, classify, and preserve identification, criminal identification, crime, and other records. 28 U.S.C. § 534 further enables the exchange of the aforementioned records and information with, and for the official use of, authorized officials of Federal, State, local, and tribal criminal and noncriminal justice departments and agencies. In addition, 42 U.S.C. § 3771 authorizes the Director of the FBI to develop new or improved approaches, techniques, systems, equipment, and devices to improve and strengthen criminal justice.

Status of Next Generation Identification Incremental Deployment

NGI is being deployed in 7 separate increments to balance operational needs and technical feasibility. Increment 0 (Advanced Technology Workstations (ATWs)) was completed in March 2010. Increment 1 (the Initial Operating Capability) was completed in February 2011. Increment 1 provided more accurate fingerprint searches, increasing the true match rate to 99.6 percent, and improving support for processing flat and less than 10 fingerprints. Increment 2 (Repository for Individuals of Special Concern (RISC) and Initial Infrastructure) was completed in August 2011. RISC provides mobile fingerprint identification operations on a national level, in time-critical situations, to assist with the identification of: wanted persons; known or appropriately suspected terrorists; sex offenders; and persons of special interest.

NGI currently has 3 Increments in progress (Increments 3, 4, and 5). Increment 3 (Palm Print Searching & Latent Print Searching) is scheduled to deploy in the spring of 2013. Increment 3 will establish the National Palm Print System, provide enhanced latent fingerprint matching, and provide cascaded searches of incoming transactions against unsolved latent and palm prints. Increment 4 (Rap Back, Facial, and Scars, Marks, and Tattoo (SMT) Search Capabilities and Migration of Remaining IAFIS Functionality to NGI) is targeted to deploy in the Summer of 2014. Increment 4 will provide a National Rap Back Service for notification of the criminal activity of enrolled individuals and access to a national repository for Facial and SMT searches for investigative purposes. Increment 5 (the Iris Pilot) is scheduled for late Summer or Fall of 2013 and will implement a new iris recognition capability. Increment 6 (Technology Refreshment of the NGI system) is slated for 2014.

Next Generation Identification Success

In addition to increased fingerprint accuracy of 99.6 percent, deployment of Increment 1 (AFIT) has allowed operations to reduce the dependency on a supplemental name check, resulting in a 90 percent (weekly) decrease in the number of manual fingerprint reviews required by CJIS Division service providers.

Since deployment of Increment 2 (RISC), 9 states, representing over 500 agencies, have begun participation in the national service; 10 additional states are in the process of implementing RISC. Over 500 transactions are processed daily with a response time of less than 7 seconds and an average weekly hit rate of 6-10 percent.

Facial Recognition

Next Generation Identification Facial Recognition

NGI Increment 4 includes a new facial recognition system. It was deployed as a pilot in February 2012 and is scheduled for full operational capability in the Summer of 2014. The objective of the NGI Facial Recognition Pilot is to conduct image-based facial recognition searches of the FBI's national repository and provide investigative candidate lists to agencies submitting queries. The goals of the Facial Recognition Pilot are to test the facial recognition processes, resolve policy and processing issues, solidify privacy protection procedures, and address user concerns.

The Facial Recognition Pilot provides a search of the national repository of photos consisting of criminal mug shots, which were taken at the time of a criminal booking. Only criminal mug shot photos are used to populate the national repository. Query photos and photos obtained from social networking sites, surveillance cameras, and similar sources are not used to populate the national repository. The national repository is updated as transactions, including enrollments and deletions, are submitted by law enforcement users. The national repository contains approximately 12.8 million searchable frontal photos.

The Facial Recognition Pilot permits authorized law enforcement agencies to submit queries for a facial recognition search of the national repository of mug shots. The national repository can be queried by authorized criminal justice agencies for criminal justice purposes. Access to the national repository is subject to all rules regarding access to FBI CJIS systems information and subject to dissemination rules for authorized criminal justice agencies. Query requests are processed "lights out" (without human intervention), and the results are returned to the submitting agency as an investigative lead in the form of a ranked candidate list.

The investigative response provided to a submitting agency will include the number of candidates requested, in ranked order. The FBI Number/Universal Control Number of each candidate will also be returned, along with a caveat noting that the response should only be used as an investigative lead. Upon receipt of an investigative response from the FBI, the submitting agency will be responsible for conducting a full investigation of potential matching candidates.

Facial Recognition Privacy Documentation

In accordance with Section 208 of the E-Government Act of 2002, facial recognition was initially addressed by the FBI's June 9, 2008 Interstate Photo System Privacy Impact Assessment (PIA). In coordination with the FBI's Office of the General Counsel, the 2008 Interstate Photo System PIA is currently in the process of being renewed by way of Privacy Threshold Analysis (PTA), with an emphasis on Facial Recognition. An updated PIA is planned and will address all evolutionary changes since the preparation of the 2008 IPS PIA.

Participating States and Agencies

Initial pilot participants are states or agencies that already have established facial recognition systems. Following completion of the pilot and implementation of the full facial recognition operating capability, additional federal, state, local, and tribal partners and agencies, with or without established facial recognition systems, will be eligible for participation.

Appropriate Use of Next Generation Identification Facial Recognition Technology

Searches of the national repository of mug shots are subject to all rules regarding access to FBI CJIS systems information (28 U.S.C. § 534, the FBI security framework, and the CJIS Security Policy) and subject to dissemination rules for authorized criminal justice agencies. Queries submitted for search against the national repository must be from authorized criminal justice agencies for criminal justice purposes.

Each participating pilot state or agency is required to execute a Memorandum of Understanding (MOU) that details the purpose, authority, scope, disclosure and use of information, and the security rules and procedures associated with piloting. Pilot participants are advised that all information is treated as "law enforcement sensitive" and protected from unauthorized disclosure.

Pilot participants are informed that Information derived from pilot search requests and resulting responses is to be used only as an investigative lead. Results are not to be considered as positive identifications.

Current Facial Recognition Pilot Participants

In February 2012, the State of Michigan successfully completed an end-to-end Facial Recognition Pilot transaction and is currently submitting facial recognition searches to CJIS. MOUs have also been executed with Hawaii and Maryland; and South Carolina, Ohio, and New Mexico are engaged in the MOU review process for Facial Recognition Pilot participation. Kansas, Arizona, Tennessee, Nebraska, and Missouri are also interested in Facial Recognition Pilot participation.

Summary

The FBI's Next Generation Identification Program is on scope, on schedule, on cost, and sixty percent deployed. The Facial Recognition Pilot which began operation in February 2012 searches criminal mug shots and provides investigative leads. The Facial Recognition Pilot is evaluating and solidifying policies, procedures, and privacy protections. Full operational capability for facial recognition is scheduled for the summer of 2014.

TESTIMONY OF

THE FEDERAL TRADE COMMISSION

ON

"WHAT FACIAL RECOGNITION TECHNOLOGY

MEANS FOR PRIVACY AND CIVIL LIBERTIES"

PRESENTED BY

MANEESHA MITHAL

ASSOCIATE DIRECTOR, DIVISION OF PRIVACY AND IDENTITY PROTECTION

SENATE COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW

July 18, 2012

I. Introduction

Chairman Franken, Ranking Member Coburn, and members of the Subcommittee, I am Maneesha Mithal, Associate Director of the Division of Privacy and Identity Protection at the Federal Trade Commission ("FTC" or "Commission"). I appreciate the opportunity to present the Commission's testimony on facial recognition technologies.[1]

Facial recognition technologies currently operate across a spectrum, ranging from pure facial detection, which simply means detecting a face in an image, to biometric analysis of facial images, in which unique mathematical data are derived from a face in order to match it to another face.[2] In the latter example, if one of the faces is identified – *i.e.* the name of the individual is known – then in addition to being able to demonstrate a match between two faces, the technology can be used to identify previously anonymous faces. In between these two points are a range of possibilities that include determining the demographic characteristics of a face, such as age range and gender, and recognizing emotions from facial expressions.

Having overcome the high costs and poor accuracy that once stunted their growth, facial recognition technologies are quickly moving out of the realm of science fiction and into the commercial marketplace.[3] Today facial recognition technologies can be found in a wide array of

[1] This written statement represents the views of the Federal Trade Commission. My oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or of any Commissioner. Commissioner J. Thomas Rosch dissents to certain portions of the testimony. His views are explained in the attached separate statement.

[2] *See* Dr. Joseph J. Atick, International Biometrics & Identification Association, *Face Recognition in the Era of Cloud and Social Media: Is it Time to Hit the Panic Button?* (Dec. 2011), at 2, *available at* http://www.ibia.org/resources/.

[3] Throughout this testimony, the term "facial recognition" is used broadly to refer to technologies that are used to extract data from facial images. *See* Sony, Face Recognition Technology, http://www.sony.net/SonyInfo/technology/technology/theme/sface_01.html.

contexts, including digital signs, mobile applications, and social networks. While consumers may enjoy the benefits associated with advancements to these technologies – such as easier organization of online photos – there are also concerns that the technologies may increase the risks to consumer privacy. Recognizing that the commercial use of these technologies will likely continue to grow, the FTC has sought to understand how these technologies are being used, how they could be used, and how they will shape consumers' commercial experiences.

To examine these issues, the FTC hosted a workshop in December 2011 – "Face Facts: A Forum on Facial Recognition Technology" ("Face Facts workshop").[4] Researchers, academics, industry representatives, and consumer and privacy professionals all took part in a series of wide-ranging discussions. Major topics included the recent advances, current uses, and possible future uses of facial recognition technologies, as well as the privacy and security concerns those issues raise. Following the workshop, Commission staff requested public comments regarding a number of topics and questions.[5] Commenters were asked to provide input on, among other issues: the privacy and security concerns surrounding the commercial use of these technologies, best practices for providing consumers with notice and choice about the use of these technologies, and best practices for deploying these technologies in a way that protects consumer privacy. The FTC received eighty public comments from private citizens, industry representatives, trade groups, consumer and privacy advocates, think tanks, and members of

[4] FTC Workshop, *Face Facts: A Forum on Facial Recognition Technology* (Dec. 8, 2011), http://www.ftc.gov/bcp/workshops/facefacts/.

[5] *See* Press Release, FTC, FTC Seeks Public Comments on Facial Recognition Technology (Dec. 23, 2011), *available at* http://www.ftc.gov/opa/2011/12/facefacts.shtm.

Congress, reflecting a wide variety of viewpoints on these issues.[6] We are still reviewing these comments, and staff plans to use the information we have learned to date to release a report later this year setting forth recommended best practices for using facial recognition technologies in a manner that respects consumer privacy while still allowing consumers to receive the benefits these technologies may provide, such as convenience and more personalized service. The report would not serve as a template for law enforcement actions or regulations under laws currently enforced by the FTC.

The FTC is also considering how the three core principles articulated in the Commission's March 2012 report on consumer privacy ("Privacy Report") – privacy by design, simplified consumer choice, and transparency – can be applied to the use of facial recognition technologies.[7] These principles call upon companies handling consumer data to implement privacy by design by building in privacy protections at every stage in the development of their products and services, provide consumers with simplified choices about the collection and use of their information, and increase transparency by providing clearer, shorter and more standardized privacy notices.

This testimony addresses solely commercial uses and does not address the use of facial recognition technologies for security purposes or by law enforcement or government actors. It describes the current facial recognition landscape, including: (1) recent advances in facial

[6] *See* FTC, # 402; FTC Seeks Public Comments on Facial Recognition Technology; Project Number P115406, http://www.ftc.gov/os/comments/facialrecognitiontechnology/index.shtm.

[7] FTC, *Protecting Consumer Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers,* (Mar. 2012), *available at* http://www.ftc.gov/os/2012/03/120326privacyreport.pdf.

recognition technologies, (2) current commercial uses of facial recognition technologies, and (3) possible future commercial uses of facial recognition technologies. The testimony concludes by setting forth some privacy considerations the Commission is examining as staff prepares its facial recognition report and weighs next steps in this area.[8]

II. Current Facial Recognition Landscape

A. Recent advances in facial recognition technologies

Until recently, because of high costs and limited accuracy, facial recognition technologies were not widely used on a commercial basis. However, recent years have brought steady improvements in these technologies. Several developments have contributed to the increased accuracy in facial recognition systems. For example, better quality digital cameras and lenses create higher quality images, from which biometric data can be more easily extracted. In addition, the goal of some facial recognition technologies is to match an image of an unknown face to an identified "reference photo," where the name of the individual is known. Until recently, it was difficult to match two images if the photos were taken from different angles. With current technologies, companies can generate 3D face images to help reconcile pose variations in different images.

These recent technological advances have been accompanied by rapid growth in the availability of identified photos online. Previously, most of the images available online were of celebrities, but today there are many sources of identified images of private citizens online. One

[8] This hearing, and therefore this testimony, focuses specifically on facial recognition technology. However, the Commission is aware that there have also been recent advances in other forms of biometric technologies, such as voice recognition, which may raise similar privacy concerns. Accordingly, the Commission is working to better understand the privacy implications of all forms of biometric technology that commercial entities are using.

explanation for this is the rise in popularity of social networking sites. For example, approximately 2.5 billion photos are uploaded to Facebook each month.[9] This multitude of identified images online can eliminate the need to purchase proprietary sets of identified images, thereby lowering costs and making facial recognition technologies commercially viable for a broader spectrum of commercial entities.[10]

B. Current commercial uses of facial recognition technologies

As noted, facial recognition technologies currently operate across a spectrum ranging from the ability to determine that a photo has a face in it ("pure facial detection") to the ability to identify demographic characteristics of a face, to the ability to match different images of the same face and possibly identify an unknown face. In many cases, the privacy risks associated with commercial uses of facial recognition increase along with the sophistication of the technology at use. For example, the privacy risks associated with companies using facial recognition to identify an unknown face are generally much greater than the risks raised by a company using pure facial detection to locate a face in an image.

Current uses of pure facial detection include, among others, refining search engine results to include only those results that contain a face, locating faces in images in order to blur or de-identify them, or ensuring that the frame for a video chat feed actually includes a face. Pure facial detection is also used in virtual eyeglass fitting systems and virtual makeover tools that

[9] *See* Chris Putnam, *Faster Simpler Photo Uploads*, THE FACEBOOK BLOG (Feb. 5, 2010), http://blog.facebook.com/blog.php?post=206178097130.

[10] *See* Center for Democracy & Technology, *Seeing is ID'ing: Facial Recognition & Privacy*, Center for Democracy & Technology (Jan. 22, 2012) at 3, *available at* https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-Center_for_Democracy_and_Technology-January_2012.pdf.

allow consumers to "try on" a pair of glasses or a new hairstyle online. In these systems, after the consumer has uploaded a photo of herself to the website, that photo is scanned, basic facial features are picked out and – using the detected facial features as reference points – the eyewear or hairstyle is superimposed on the consumer's face.

More sophisticated technologies that do not merely distinguish a face from surrounding objects, but also assess various characteristics of that face, can be used commercially in a variety of ways. For instance, companies can use technologies that identify moods or emotions from facial expressions to determine a player's engagement with a video game or a viewer's excitement during a movie.

Companies are also using technologies that determine demographic characteristics to deliver targeted advertisements in real-time in retail spaces.[11] These companies place cameras – which assess the age range and gender of the consumer standing in front of the screen – into digital signs or kiosks. They then display an advertisement based on that consumer's assessed demographic characteristics. For example, a 30 year-old male might be shown an advertisement for shaving cream, while a 50 year-old female may be shown an advertisement for perfume. As currently implemented, companies do not appear to be storing images processed by digital signs for future use.

Digital signage is an area where industry trade groups have proactively issued guidance and "best practices" for their members. For example, Point of Purchase Advertising International's Digital Signage Group ("POPAI") has developed a code of conduct containing

[11] Shan Li and David Sarno, *Advertisers start using facial recognition to tailor pitches*, LA TIMES, Aug. 21, 2011, *available at* http://articles.latimes.com/2011/aug/21/business/la-fi-facial-recognition-20110821.

recommendations for marketers to follow in order to maintain ethical data collection practices in retail settings.[12] Similarly, the Digital Signage Federation worked with the Center for Democracy and Technology to craft a voluntary set of privacy guidelines for their members, which include advertisers and digital sign operators.[13] Both of these self-regulatory codes address the use of facial recognition technologies in digital signs.

One company has leveraged this ability to determine age range and gender in order to obtain aggregated demographic data about the clientele of bars and nightclubs via cameras placed at the entrance to these venues. This company only stores the aggregated demographic data, and not images of the venues' customers. Both the operators of the venue and third parties – such as liquor distributors – can use this data to understand the demographics of a particular venue's customers at certain times, and possibly tailor their specials or promotions accordingly. This company also makes the aggregate information it collects available through a mobile app that consumers can use to make decisions about which venues to patronize.[14]

Facial recognition technologies that are used to actually identify individuals, rather than simply to detect a face or demographic characteristics, work by deriving unique biometric data from facial images. This biometric data is the unique mathematical characteristics that are extracted from the image in order to capture the individual identity (e.g., distance between eyes,

[12] POPAI, Digital Signage Group, *Best Practices: Recommended Code of Conduct for Consumer Tracking Research* (Feb 2010) *available at* http://www.popai.com/docs/DS/2010dscc.pdf.

[13] *See* Digital Signage Federation, *Digital Signage Privacy Standards* (Feb. 2011) *available at* http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002-2011%20%283%29.pdf.

[14] *See* SceneTap, http://www.scenetap.com/.

ears, size of features, etc.). Those unique mathematical characteristics can then be compared to the characteristics extracted from other facial images to determine if there is a match.[15]

This type of technology has been implemented in a variety of manners. For example, a mobile phone user can authenticate herself by using her face, rather than a password, to unlock her phone. One of the most prevalent current uses of this technology is to enable semi-automated photo tagging or photo organization on social networks and in photo management applications. On social networks these features typically work by scanning new photos a user uploads against existing "tagged" photos. The social network then identifies the user's "friends"[16] in the new photos so the user can tag them. As currently implemented, these features on social networks suggest "tags" only of people that the user already knows, either through a "friend" relationship or other contacts that suggest the two individuals know each other.

C. Possible future commercial uses of facial recognition technologies

Future uses of facial recognition technologies may provide new and exciting products and services that consumers want. They may also provide privacy and security benefits. For example, as noted above facial recognition technology can be used to authenticate users on mobile devices. In the future, we can foresee broader use of these technologies for authentication purposes which can enhance privacy and security for consumers.

At the same time, there may be privacy and security concerns. For example, will it become feasible to use facial recognition to identify previously anonymous individuals in public

[15] *See* Dr. Joseph J. Atick, International Biometrics & Identification Association, *Face Recognition in the Era of Cloud and Social Media: Is it Time to Hit the Panic Button?* (Dec. 2011), at 2, *available at* http://www.ibia.org/resources/.

[16] We use the term "friend" to refer to an individual user that another user has a mutual connection with on the social network.

places, such as streets or retail stores, or in previously unidentified photos online? While it does not seem that it is currently possible for commercial entities to accomplish this on a wide scale, recent studies suggest that in the near future, it may be possible. For example in a 2011 study, Carnegie Mellon researchers were able to identify individuals in previously unidentified photos from a dating site, by using facial recognition technology to match them to their Facebook profile photos.[17]

Some have surmised that advances in facial recognition technologies may end the ability of individuals to remain anonymous in public. If these predictions come to fruition, companies could employ facial recognition technologies in a number of ways that raise significant privacy concerns. For example, companies could match images from digital signs with other information to identify customers by name and target highly-personalized ads to them based on past purchases, or other personal information available about them online. Further, a mobile app that could, in real-time, identify previously anonymous individuals on the street or in a bar could cause serious privacy and physical safety concerns, although such an app might have benefits for some consumers.

III. Questions and Next Steps

In its March 2012 Privacy Report the Commission articulated three core principles for companies to consider in protecting consumer privacy:

(1) **Privacy by Design**: The Commission called on companies to build in privacy at every

[17] *See Face Recognition Study - FAQ*, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/. This study used a limited geographic area, and therefore a limited number of photos and subjects; thus, the results cannot necessarily be duplicated on larger scale. *See Face Facts Workshop, Remarks of Prof. Alessandro Acquisti, Carnegie Mellon University*, at 130-131 and 138-139.

stage of product development. Such protections include providing reasonable security for consumer data, collecting only the data that is consistent with the context of a particular transaction or the consumer's relationship with the business, retaining data only as long as necessary to fulfill the purpose for which it was collected, safely disposing of data no longer being used, and implementing reasonable procedures to promote data accuracy. The Commission also called on companies to implement and enforce procedurally sound privacy practices throughout their organizations, including, for instance, assigning personnel to oversee privacy issues, training employees on privacy issues, and conducting privacy reviews when developing new products and services.

(2) **Simplified Consumer Choice**: The Commission noted that, for practices that are not consistent with the context of a transaction or a consumer's relationship with a business, companies should provide consumers with choices at a relevant time and context. In addition, companies should obtain affirmative consent before (1) collecting sensitive data or (2) using consumer data in a materially different manner than claimed when the data was collected.

(3) **Transparency**: The Commission called on companies to increase the transparency of their data practices so that interested parties can compare data practices and choices across companies. The Commission also suggested that companies – particularly those that do not interact with consumers directly, such as data brokers – provide consumers with reasonable access to the data that the companies maintain about them.

The Commission intends to release a report this year laying out recommended best practices for the use of facial recognition technologies that build on comments by workshop panelists, written submissions, and these three core principles. In developing the report, the Commission is considering the following questions.

First, the Commission is considering ways in which companies using facial recognition technologies can implement "privacy by design." For example, how can companies establish and maintain sound retention and disposal practices for the consumer images and biometric data that they collect? For instance, should digital signs using demographic detection ever store consumers' images? Are there certain sensitive areas where companies should not place digital signs? Are there ways that the use of facial recognition technologies may increase consumer information privacy and security?

Second, the Commission is examining how companies that use these technologies can provide consumers with simplified choices about the collection and use of their data. How should companies using facial recognition technology provide choices? Under what circumstances should companies seek consumers' affirmative express consent before engaging in facial recognition?

Finally, the Commission is considering how companies using facial recognition technologies can increase the transparency of their data practices. For example, are consumers aware that digital signs using demographic detection are being used in retail environments? How can they be made aware? Similarly, how many consumers know that social networks have begun implementing facial recognition for photo "tagging"? How and when should these social networks disclose their practices to consumers? The Commission is currently evaluating these and other questions as it develops a final report on the use of facial recognition technologies in commercial environments.

IV. Conclusion

Thank you for the opportunity to provide the Commission's views on the topic of facial recognition. We look forward to continuing to work with Congress and this Subcommittee on this important issue.

Statement of

Brian Martin, Ph.D.
Director of Biometric Research
MorphoTrust USA

Before

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law

"What Facial Recognition Technology Means for Privacy and Civil Liberties"

July 18, 2012

Good afternoon Chairman Franken, Senator Coburn, and other distinguished members of the Subcommittee. Thank you for asking MorphoTrust USA to discuss the capabilities of facial recognition technology today.

My name is Dr. Brian Martin and as the Director of Biometric Research for MorphoTrust USA, my primary responsibility is the research and development of our company's biometric search engine. After earning a Ph.D. in Physics from the University of Pittsburgh, my career in biometrics began at a startup company called Visionics, which pioneered software-based face recognition technologies. Over the last 15 years, my teams have played an integral part in the research and development of world class algorithms and search engines for face, iris, and fingerprint matching. These technologies are used by the U.S. Departments of Defense and State, the FBI, over 30 face recognition-enabled drivers' license systems, and by several large international biometric systems including the world's largest in India. With a decade and a half of real world experience in developing biometric systems, I will address the following in my testimony:

- An explanation of how facial recognition algorithms work;
- A statement on the accuracy and limitations of current state-of-the-art face recognition technologies;
- An overview of the different categories of face recognition applications; and
- Some comments on face recognition technology/design as it relates to privacy.

MorphoTrust USA's History and Role in Identity Solutions

MorphoTrust USA was formed when L-1 Identity Solutions was acquired in July 2011 by Safran, a global technology powerhouse in aerospace, defense, and security. Headquartered in Billerica, Massachusetts, MorphoTrust has over 1,100 employees across the country, including a biometrics facility in Bloomington, Minnesota.

MorphoTrust USA is the leading domestic provider of U.S. driver licenses, passports and passport cards. We provide solutions for border management, public safety, law enforcement, retail, travel and applicant vetting. We develop the technology for and deliver some of the largest, most complex biometric systems in the world, which are used for searching large databases to prevent identity fraud, provide criminal investigative leads, and fight terrorism. Our accomplishments range from introducing the first face recognition powered de-duplication of driver's license databases to providing the first commercial face detection technology to digital camera manufacturers. Under previous names, Visionics, Identix, Viisage, and L1 Identity Solutions, we have been at the forefront in the adoption of face recognition systems used by states and the federal government for over a decade.

How Face Recognition Works

Automated face recognition algorithms were first studied in the late 1980's and became popular in the mid 1990's. Over the last 20 years, the technology has matured to the point where it can be used as a tool to help prevent identity fraud, to provide leads in criminal investigations, and fight terrorism. The technology is based on pattern recognition techniques used in the field of computer vision. Though there are several different approaches to face recognition, each with its own merits, most modern commercial grade algorithms follow these general steps:

1. Detection: First, patterns in an image are extracted and compared to, or tested against, a model of a face. When these patterns are determined to closely resemble the face model, the assumption is that a face is present in the image. This is called face detection, and in itself, can be a challenging research problem due to the large variability in what a face could look like in an image. Changes in the pose of the face, the expression on the face and the lighting (shadows) on the face make what is seemingly trivial for the human brain to accomplish an active area of research for computer vision scientists. Furthermore, algorithms have to discriminate between items that look similar to faces, but are not human faccs (think of how one sees the man in the moon).
2. Registration: The next step following face detection is called 'feature registration'. The algorithms focus on the area of the image where a face was detected and attempt to determine the locations of a common set of facial features that will be used as key points when extracting the binary template or faceprint. The most commonly used registration points are the center of the eyes, but algorithms can use others, such as the tip of the nose, the corners of the mouth, etc. Once the algorithm determines the location of these points of interest, the features of the face are said to be registered or localized. If the

algorithm cannot find suitable features in this stage, feature registration will fail, causing the face to 'fail to enroll' in the system. Note that a human can aid in these first two steps, and in fact, face detection and feature registration were performed manually in early face recognition algorithms.

3. Feature Extraction: Once the features are registered, various forms of image processing can be performed to normalize the image, reduce noise in the image, reduce lighting and expression variations, and even normalize the pose of the face. This image processing helps to remove variations in the face that the matching algorithms cannot easily deal with. For instance, algorithms may not be able to match the same face in two different images if they are simply at a different scale (e.g., one is more zoomed in than the other). This stage would normalize the face in the image to ensure that it is the same size as the other faces it may be matched against. After this image processing is complete, features are extracted from the face into a binary representation appropriate for classification and/or matching. This is often referred to as a facial template or a faceprint. The feature extraction step is usually quite complex and can vary drastically from algorithm to algorithm. That is, the faceprint from one approach is rarely if ever compatible with a different approach or implementation.
4. Classification: An optional step is face classification. With the faceprint in hand, algorithms can be trained to classify the face into any number of categories that can be used to aid face matching or can just be informational. Some examples would be to use a classifying algorithm to estimate the gender or age of the face or even estimate if the extracted features of the face are of sufficient quality to support an accurate match of the face.
5. Matching: Finally, after the features of a face have been generated for two presentations of a face, an algorithm can be applied to match the two faceprints against each other to produce a single score value that represents the amount of similarity between the two faces. Depending on the features used and the efficiency of the representation of the features, the complexity of the match can be extremely high and CPU intensive taking on the order of a second per match or the complexity can be very low allowing 10's of millions of matches per second on a modern server computer. An example of a simple matching algorithm would be one that simply counts how many times the 1's and 0's are different between two binary faceprints. When the count of differing bits is low, the two faces are given a higher similarity (match) score compared to a case when the counts of differing bits are high.

Though the general recipe for face recognition is similar for many approaches, the details can vary dramatically. For example, the facial features used for matching could be texture-based, such as the pattern of a hairline or eyebrow, or the features could be shape-based, where the curvature of facial features is used for matching. 3D features can be estimated from the information in an image or can be directly measured from the image capture system. Features used for matching can be global, such as the shape of the head; they can be local, such as the shape of the eye, or they can be nearly microscopic such as the pores and wrinkles in the skin. In all cases, the approaches are vastly more complicated than the commonly perceived notion that face recognition systems simply look at geometrical distance measures between local features of the face such as the eyes, nose, and mouth.

Despite the complexity, the technology is currently at a state where these face recognition algorithms can be deployed in anything from cell phones to large multi-server search engines capable of searching over 100,000,000 faces in just a few seconds with operational accuracy.

Accuracy of Facial Recognition Technology

For almost two decades, the U.S. Government has benchmarked the accuracy of automated face recognition systems. The National Institute of Standards and Technology (NIST) is currently viewed as the worldwide leader in independent benchmarking of state-of-the-art biometric technology. In NIST's 2010 face recognition report (NIST Interagency Report 7709 - Report on the Evaluation of 2D Still-Image Face Recognition Algorithms), it was shown that the best face recognition algorithms have improved by two orders of magnitude (over 100 times better) over the last decade. That is, the best algorithms can correctly determine if two faces belong to the same person 99.7% of the time while at the same time only making a mistake by falsely matching a face to the wrong person 0.1% of the time. In 1997, the algorithms could determine only if faces belonged to the same person about 50% of the time at this 0.1% false matching rate. Current state-of-the-art algorithms can in fact match faces as accurately as humans who are not trained to be experts in face matching.

This high accuracy is realized when the faces are captured in a controlled or staged environment with cooperative subjects. When the face is not looking directly at the camera, when there are strong shadows on the face, and when the image resolution is low (as one would expect from convenience store surveillance video) the accuracy of facial recognition can approach that from the late 1990's, making these scenarios an active area of current face recognition research. It is likely that recognition of faces captured in uncontrolled environments will dramatically improve over the next couple of decades, and as camera technology improves, it may allow face matching at accuracies close to what we see now in ideal conditions. Nevertheless, even when accuracy is relatively low, face recognition still proves to be a valuable tool for investigative searches. For instance, if face recognition can provide an investigative lead to a crime only 50% of the time, it is still helping to solve crimes whereas in the past it would have been unlikely to find any leads on suspects.

Face Recognition Applications

In my earlier remarks, I addressed the concept of accuracy, but to be fair, there are different measures of accuracy for different types of applications. There are generally two main types of applications: verification and identification. The first, verification, is where the face recognition system is used to verify that you are who you say you are. This applies to the scenario of using a biometric to open a door or using your face to unlock your phone. The accuracy numbers mentioned above reflect precisely this type of application. Arguably more demanding (and more useful) is the application of identification where face recognition is used to determine an unknown identity from a gallery of known identities. This would include applications where a photo from a crime scene could be compared to a database of known offenders to generate investigative leads or where faces in the database are compared to the database itself to detect people committing identity fraud by enrolling twice under different identities.

With identification, the requirements on an algorithm are very demanding since in order to perform a single identification, the recognition system must, in an oversimplified description, perform multiple verifications – one for each member in the gallery. Identification from a database of one million faces is, in effect, the same as performing one million verifications, and consequently the algorithms should be one million times more accurate to ensure similar false positive match rates compared to the verification application. Though most modern identification systems cannot be simplified to performing several verification attempts, the point is that as the database of identities grows to the size of millions of records, the ability to perform accuracy matching becomes that much harder, and requires that much more matching power. With today's computers and state-of-the-art face recognition technology, tens of millions of records can be accurately matched per second on a single computer enabling very large scale identification applications while only taking up a relatively small hardware footprint.

Unlike verification where the system runs with very little human intervention, most large face identification systems require an expert human operator to be 'in the loop' since the chance of getting a false match in identification is directly related to the size of the gallery of faces. These expert operators either help narrow down and direct the facial search to a smaller target set of individuals or they are used to validate the potential match candidates from a facial search. This would be the case where a criminal investigator could narrow the search to suspects who live in a specific neighborhood where a crime was committed and because the pool of candidates is smaller, there is a better chance of finding a correct face matching result. Similarly, the investigator would review the recommended list of candidates from the face recognition technology after the search is complete to validate or correct the face algorithms decisions. This is just what one is doing when they correct the automatic face labels generated by photo organization software that uses face recognition.

An offshoot application of facial recognition is simply the ability to classify or characterize faces. In this application, there is no actual matching of faceprints to known or unknown identities. Instead, the features of the face are analyzed to estimate any number of aspects of the captured face. These could include gender, age, expression, at what direction the subject is looking, etc... with the most obvious use being to collect demographic information about the subjects in front of a camera. Since this can be performed in real-time with a video camera, advertisers can use this information to tailor the advertisements based on the faces looking at them by dynamically changing the content of digital billboards.

Face Recognition System Design and Privacy

MorphoTrust USA face recognition search engines are designed to store and search faceprints anonymously. That is, the faceprint is identified only by a system-specific number, which the customer of the system must link to the person's identity. This makes a faceprint match, by itself, relatively useless unless the attached identity information is available. Customers that implement face recognition systems take the responsibility for the security of their identity data, since it is this customer-owned identity database that connects various metadata to the individual, such as account numbers, home address, etc. These connections to other metadata are what can be exploited in unexpected ways.

In terms of face recognition technology, the faceprints themselves contain no more information than what was in the original images from which they were derived. If a faceprint database were compromised, the faceprints could not be reverse-engineered to recreate the original face image since the faceprints are stored in a proprietary format. The faceprints are also vendor specific and are of little use outside the system. Therefore, the accessibility of the original face image is typically the gating factor in preventing use of the face for unforeseen applications in the future.

Conclusion

Face recognition is a mature technology capable of searching millions of faces in less than a second on modern computer hardware. The usefulness of the technology has been validated over the last decade by several government customers as a tool for fighting identity fraud, crime, and terrorism. Over the next decade, we expect that face recognition will dramatically improve in matching faces from uncontrolled capture environments and additionally improve match efficiency in the controlled cases, further broadening the scenarios where face recognition can be used effectively.

Thank you for the opportunity to address the Subcommittee on these important issues. I look forward to answering vour questions.

TESTIMONY

Professor Alessandro Acquisti
Heinz College and CyLab, Carnegie Mellon University

Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
U.S. Senate

What Facial Recognition Technology Means for Privacy and Civil Liberties

Wednesday July 18, 2012

Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee: I am honored to appear before you today. I am a tenured associate professor at the Heinz College, Carnegie Mellon University (CMU), a member of CMU CyLab, and the co-director of CMU's Center for Behavioral Decision Research (CBDR).[1] I am an economist by training (I hold Master degrees in economics from Trinity College Dublin and from the London School of Economics), and I am interested in how economics can help us understand the impact of information technology (I hold a PhD in Information Management and Systems from the University of California at Berkeley). For about 10 years, I have been studying the economics and behavioral economics of privacy. My research in this area has combined economics, experimental behavioral decision research, and information technology to investigate the trade-offs associated with the protection and disclosure of personal information, the technologies that enhance the former or the latter,[2] and how individuals value, and make decisions about, those trade-offs.[3]

My remarks in this testimony will concern research that I and others have carried out in the field of privacy and face recognition.[4] I became interested in face recognition indirectly, as a result of my studies of privacy and online social networks, which started in 2005.[5] In the summer of 2011, together with my colleagues Dr. Ralph Gross (a face recognition expert at Carnegie Mellon University) and Dr. Fred Stutzman (an online social networks expert also at Carnegie Mellon University), I presented the results of a series of experiments about the privacy implications of the convergence of more accurate face recognition technology, increasing public availability of personal data (including digital photos), and statistical re-identification techniques.[6]

In my testimony, I will highlight four conclusions from my and other scholars' research in this area:

First, face recognition is "now." The technology has evolved over several decades. While early algorithms vastly underperformed human ability to detect and recognize faces, modern ones have progressed to a point that they are now being deployed in end-user applications.

Second, the convergence of face recognition, online social networks, and data mining has made it possible to use publicly available data and inexpensive off-the-shelf technologies to produce sensitive inferences merely starting from an anonymous face. I will highlight the results of three experiments we conducted in this area, including one in which we predicted portions of the Social Security numbers of students at a North-American college starting from photos of their faces.

Third, face recognition, like other information technologies, can be source of both benefits and costs to society and its individual members. However, the combination of face recognition, social networks data, and data mining, can significantly undermine our current notions and expectations of privacy and anonymity.

Fourth, depending on which goals Congress intends to achieve in the area of face recognition, different policies and interventions may be considered. If the privacy and civil liberties implications of face recognition are the concern, it is unlikely that industry solutions alone (such as self-regulatory efforts) will address those concerns.

1. The State of Face Recognition Research

Research in computer face recognition has been conducted for over forty years.[7] For most of this time, computers underperformed humans in tasks involving the detection and recognition of individuals through their faces. But the progress of algorithms has been steady: since 1993, the error rate of face recognition systems has decreased by a factor of 272.[8] Today, under certain conditions, machine face recognition performance can be comparable or even better than humans at recognizing faces.[9]

As face recognizers' accuracy kept increasing, face recognition started being deployed in more products and services. About 10 years ago, face recognizers remained the domain of government agencies or large corporations, and were mostly used in security and police activities.[10] In the past few years, face detection, face recognition, and other related algorithms (such as the estimation of individual traits from facial images) have started appearing in end-user products, and in particular Web 2.0 services. Following the acquisition of Neven Vision in 2006 and of Like.com in 2010, Google has offered Picasa users face recognition tools to organize photos according to the individuals in them.[11] Apple's iPhoto has employed face recognition to identify faces in a person's album since 2009.[12] Using Face.com's licensed technology, Facebook has used face recognition to suggest "tags" of individuals found in members' photos.[13] Klik, also developed by Face.com, used face recognition to allow real time tagging of Facebook friends through the same mobile camera used to take their pictures.[14] NEC has designed billboards that automatically locate faces of people passing by and estimate their gender and age, in order to target advertising accordingly.[15] SceneTap uses face detection to estimate the size of and gender ratio in a crowd of patrons at a venue – and allows individuals who downloaded its app to find that information online.[16]

Under typical, real life conditions (for instance, when facial shots are not captured in well-lit conditions or through frontal, "mugshot" poses) computer face recognition still underperforms humans. As we further discuss in the next section, however, face recognition's limitations are more transient than systemic: given the growing commercial interest in face recognition and its application, the gap between humans and machines in recognizing faces is likely to keep diminishing.

2. How to Predict Someone's SSN Starting From Their Face

As a privacy researcher, a few years ago I became interested in the privacy implications of the convergence of two trends: the improving ability of computer programs to recognize faces in digital images, and the increasing public availability of identified facial photos online - especially through online social networks. In a study with Ralph Gross and Fred Stutzman presented in the summer of 2011,[17] we investigated whether the combination of publicly available Web 2.0 data and off-the-shelf face recognition software may allow large-scale, automated, end-user individual re-identification. We identified individuals online across different services (Experiment 1); offline – that is, in the physical world (Experiment 2); and then inferred additional, sensitive information about them (their interests and their Social Security numbers), combining face recognition and data mining, thus blending together online and offline data (Experiment 3); finally, we developed a mobile phone application to demonstrate the ability to recognize and then predict someone's sensitive personal data directly from their face, in real time, on a mobile device.

In the first experiment (Experiment 1) we investigated online-to-online re-identification. We took unidentified profile photos from a popular dating site (where people use pseudonyms to protect privacy), compared them - using face recognition - to identified photos from a popular online social network (Facebook; namely, we used the component of a Facebook profile that can be publicly accessed via a search engine; in other words, we did not even need to log on to the network itself). Through this process, we were able to re-identify about 10% of the pseudonymous members of the dating site.

In the second experiment (Experiment 2) we investigated offline-to-online re-identification. Its methodology was conceptually similar to that of Experiment 1, but in this case we attempted to re-identify students on the campus of a North American college. We took photos of them with a webcam and then compared those shots to images from Facebook profiles. Using this approach, we re-identified about one third of the subjects in the experiment.

The first two experiments illustrate how third parties can use publicly available data not just for contextual identification (linking images of the same person in an album of photos) but also for universal, unique identification.[18] In the final experiment (Experiment 3), we predicted the interests and the first five digits of Social Security numbers (SSNs) of some of the individuals who had participated in the second experiment. We did so by combining face recognition with the algorithms we developed in 2009 to predict SSNs from public data.[19]

In the context of Experiment 3, SSNs were merely one example of the many types of information it is possible to infer about a person, starting merely from an anonymous face, through a chain of inferences in a process of *data accretion*.[20] The process illustrates the privacy implications of face recognition technology, and can be summarized in the following manner: First, face recognition links an unidentified subject (for instance, a face among many in the street) to a record in an identified database (such as an identified photo of the subject on Facebook, LinkedIn, Amazon, or in a state's DMV database). Once the link has been established, any online information associated with that record in the identified database (such as names and interests found in the subject's Facebook profile; or demographic data found on Spokeo.com - a social network and data aggregator) can in turn be probabilistically linked to the unidentified subject. Lastly, through data mining and statistical re-identification techniques, such online information can be used for additional, and much more sensitive inferences (such as sexual orientation,[21] or Social Security numbers[22]), which, in turn, can be linked back to the originally unidentified face. Sensitive data is therefore linked to an anonymous face through what we may refer to as a "transitive property" of (personal) information - a process that merely requires publicly available data. Sensitive information thus becomes "personally predictable information."

As a further example of what is already possible to accomplish using existing technologies and publicly available data, we developed a mobile phone application which, once a photo is taken of a person's face, uploads it to a server; there, a program compares it to a database of images downloaded from the Internet – and tries to recognize the person; thereafter, using the same process adopted in Experiment 3, the program attempts to predict the person's sensitive personal information, and finally displays that very same information on the device's screen, overlaid on the face of the subject. Essentially, this application (which we demoed at a security conference in August 2011, with no intention of making it publicly available) demonstrates that it is possible to conduct on a mobile device and in real time the process of Experiment 3.

We use the term *augmented reality* to describe that application: it refers to the merging of online and offline data that new technologies make possible. If an individual's face on the street can be identified using a face recognizer and identified images from social network sites such as Facebook or LinkedIn, then it becomes possible not just to identify that individual, but also to infer additional, and more sensitive, information about her.

2.1 Current Limitations and Why They Are Transient

Our experiments, while successful, were constrained geographically (we focused on the population of a North-American city, and the students at a North-American college campus) and in scope (we used databases with up to a few hundred thousands of images). The results we obtained are not *yet* scalable to the entire American population for a number of reasons: First, computational costs: we estimate that comparing the shot of a person's face to a database with mugshots of 280 million US residents aged 14 years or older, using the same hardware as in our experiments, would take over four hours (rather than the few seconds that process took in our experiments). Second, "false positives:" when comparing millions of human faces, several individuals' faces will be similar to each other, and computers do not yet excel in separating a face of a person from a face of someone who looks very much like that person. Third, light conditions, facial hair, or non-frontal poses impair the accuracy of machine face recognizers. Fourth, photographic images (and in particular frontal mugshots) may not be available for the entire population.

Those hurdles, however, are being progressively overcome. They are transient, not systemic. First, as computers' processing power keeps increasing, and cloud computing costs decrease, it will become more efficient to run end-user applications on mobile devices similar to the one we developed, for mass-scale, automated, peer-to-peer face recognition. Second, false positives will likely keep reducing, as machine face recognition error rates are decreasing by one half about every two years.[23] Third, researchers are actively working on improving computers' ability to recognize faces under varied conditions of light, facial hair, and poses. Fourth, entities such as online social networks are amassing some of the largest known databases of identified photos, from which increasingly accurate biometric models or "faceprints" of increasing portions of the US population can be, and are being, built.

It is likely, therefore, that within a few years, real-time, automated, mass-scale facial recognition will be technologically feasible and economically efficient. It will be feasible for individual end-users, in a peer-to-peer fashion; it will be feasible for firms (both for companies, such as online social networks, that will actually own the data; and for third parties that will rent identity recognition services from or through the former); and it will be feasible for governments that will access or trade biometric data with the private sector. In this world, "facial searches" in the street may become as common as text-based queries on search engines are today.

However, the fact that real time recognition technology may be used, in principle, by individuals, firms, and governments alike, does not guarantee that, in practice, all parties will gain equal access to it. The parties in actual possession of the largest databases of images will be in the better position to make use of face recognition technology and control the access that others will have to it. Similarly, the parties with more resources will be those more likely to be able to exploit it, or avoid being exploited by it.

3. Trade-offs and Privacy Concerns

In economic terms, privacy shares the characteristics of both an *intermediate good* (a good that is valued in an instrumental way, because of its consequences: for instance, loss of personal data can cause identity theft and ensuing economic damage), and a *final good* (a good that is valued for its own sake: for instance, ubiquitous surveillance creates discomfort).[24]

I will first discuss the implications of face recognition for privacy as an intermediate good. As it is often the case with advances in information technology, the ramifications of cheap, powerful facial recognition technology in the hands of individuals, firms, and government agencies, are complex. They include both scenarios where public or individual welfare are increased, and scenarios where significant tangible and intangible costs arise. Consider a peer-to-peer scenario: Your phone (or in some years your glasses, and in a few more your contact lenses) will tell you the name of that person at the party whose name you always forget; or, it will tell the stalker in the bar the address where you live. Consider a third party firm scenario: The hotel will recognize and greet you as you enter the lobby with your luggage (because you friended them on a social network, or because - with or without your consent - the hotel enrolled in some identity recognition service sold by a social network); or, the salesperson will infer your credit score the moment you enter the dealership, and use a psychological profile (also calculated in real time from your online posts) to nudge you to accept a steep price for the car you wanted. Consider a government agency scenario: An investigative agency will be able to find missing or exploited children in databases of online photos; or, an administration will be able to identify from remote, high-definition cameras, all of the thousands of participants in a peaceful protest. More scenarios are unforeseeable today but will be commonplace tomorrow.

In short, face recognition could make our lives easier, or more comfortable, or more secure; conversely, it could limit our freedom, endanger our security, ease the extraction of consumer surplus, and chill free speech by creating a state of constant and ubiquitous surveillance.

Next, I will discuss the implications of face recognition for privacy as a final good: in this regard, there are reasons to believe that the process through which face recognition erodes our notion of privacy has not just started, but is well on its way. Note that the results of our experiments were limited by design: our self-imposed constraint consisted in only using publicly available data and technologies that other third parties and end-users could also get access to: off-the-shelf face recognition technology,[25] limited computational power accessed through cloud computing services, and limited amounts of facial images made publicly available by end users on online social networks. In reality, today, both governmental and private sector entities have access to more powerful computational tools and much larger (and more accurate) repositories of digital photos than we had.

Consider, for instance, Facebook – currently the largest social networking site. Many of its users (estimated at over 900 million worldwide,[26] with more than 90 billion of photos allegedly collectively uploaded[27]) choose photos of themselves as their "primary profile" image. These photos are often identifiable: Facebook has aggressively pursued a "real identity" policy, under which members are expected to join the network under their real names, under penalty of account cancelation.[28] Using tagging features and login security questions, the social network has successfully nudged users to associate their and their friends' names to uploaded photos. These photos are also publicly available: Primary profile photos *must* be shared with strangers under Facebook's own Privacy Policy. [29] Many members also allow those photos to be searchable from outside the network via search engines.

Online social networks such as Facebook are accumulating the largest known databases of facial images. Often, those images are tagged or attached to fully identified profiles, thus providing a linkage between a person's facial biometrics and their real names. Furthermore, many social network users post and tag *multiple* photos of themselves - and their friends, allowing biometric models of their faces, and those of other people as well, to become more accurate. Before Face.com was acquired by Facebook, for instance,[30] its mobile face recognition application Klik effectively used its own users as means of improving the recognition accuracy of its algorithms (since users were asked to select the correct name among a list of possible matches found by the application for a given face). This process would increase the future recognizability even of subjects who did not explicitly consent to more accurate biometric models of their faces being composed, or who had no knowledge of that happening.[31] Furthermore, such vast and centralize biometrics database can be at risk of third-party hacking.[32]

Online social networks are becoming today's de facto "Real IDs" – produced not by legislative mandate but technological capability. We must realize that the notions and expectations of privacy and anonymity, as we have known them for the history of human kind – the idea that, among strangers, you are a stranger, are facing a new challenge that we do not yet fully comprehend.

4. Implications

The evolution of face recognition technology is inescapable, but its applications will not all be equally desirable. Unfortunately, there is no obvious silver bullet that will allow society to continue to enjoy the benefit of face recognition divorced from its more concerning usages. There are, however, policy and technology mechanisms that are worth of investigation, and which carry trade-offs we are only beginning to appreciate: privacy enhancing technologies applied to face capture, detection, or recognition;[33] moratoriums on specific applications of face recognition;[34] explicit consent requirements to having one face's tracked, or matched, in public; do-not-recognize-me mechanisms; or privacy legislation that would place obligations on those who use facial recognition to collect the personal identity and thereby the personal information of others; and so forth. Unfortunately, the mere reliance on industry self-regulation is unlikely to find balance between uses and abuses of face recognition, due to the particular economic value of identified facial information, and recent history in the markets for personal data.

Identified facial information is especially valuable because facial biometric models are peculiarly sensitive and powerful instruments of identification and tracking. First, a person's face is a permanent identifier: it changes over time in patterns that computers are learning to predict, but it cannot be permanently altered to avoid detection without great cost.[35] Second, a person's face is a veritable conduit between her different persona: it can link a person's online world (for instance, her social network presence) to her offline world (the person walking in the street). Third, it can be captured remotely and surreptitiously, and therefore without individual consent or knowledge. Fourth, the technologies necessary to track and identify faces, as discussed, are becoming ubiquitous. As a result, control over vast repositories of identified facial information can give a firm unique power to serve and influence an array of other services and applications; competition for that control, therefore, will be fierce, at the likely cost of the privacy of end users.[36]

An analysis of recent history in the market for personal data also suggests that firms may engage in more invasive applications of face recognition over time. Currently, end-user applications of face recognition have limited capabilities. Yet those limitations are less driven by technological constraints than by firms' concerns over consumers' reaction to too-aggressive deployment of face recognition. Evidence of this can be gleaned from firms' assurances that these services do not (yet) allow indiscriminate face recognition of everybody: for instance, Face.com developed the face recognition tagging services used by Facebook users --- but "if you choose to hide your Facebook tags, [Face.com] services will get blocked out when attempting to recognize you in photos."[37] However, if recent history of privacy in social networks is a guide, the current, almost coy applications of face recognition may be "bridgeheads" designed by firms to habituate end-users into progressively more powerful and intrusive services. Consider the frequency in which, in the past few years, a popular social network such as Facebook has engaged in practices that either a) unilaterally modified settings or defaults associated with users' privacy, so as to force increased sharing or disclosure;[38] and b) reflected a "two steps forward, one step backward" strategy, in which new services were enacted or proposed, then taken back or scaled down due to users' reaction to their invasiveness, and then enacted again, after some time had passed.[39] The fact that, as consumers, we do get eventually habituated to those new services does not necessarily prove that they come without risks: Our attention is captured by what we can see as their immediate benefits; what we pay less attention to are their privacy costs, as they are often delayed.[40]

In the absence of policy intervention, therefore, the patterns we are observing (increasing gathering and usage of individuals' facial biometrics data) are unlikely to abate. The risk exists that some firms may attempt to strategically use default settings, unilateral changes to interfaces and systems, and user habituation to nudge individuals into accepting more capturing and usage of facial data – creating a perception of *fait accompli* which, in turn, will influence individuals' expectations of privacy and anonymity.

Information is power. In the 21st century, the wealth of granular data accumulated about each individual, and the staggering progress of behavioral sciences in understanding how that knowledge can be used to nudge and influence individual behavior, make it so that control over personal information will imply power over the person. It does not matter whether this control will be exercised by a government or by a corporation: as control is tilting from data subjects to data holders, the very balance of power between different entities is at stake. Senators, I do not envy your position. We had the easy task – showing the problem. You have the much harder task of helping steer us towards its solution.

Thank you for inviting me to testify today. I look forward to answering your questions.

[1] See http://www.heinz.cmu.edu/~acquisti/

[2] A. Acquisti, 2010. "The Economics Of Personal Data and The Economics Of Privacy." Commissioned By The OECD, For The OECD Roundtable On The Economics Of Privacy and Personal Data, Paris, December 2010. http://www.heinz.cmu.edu/~acquisti/papers/acquisti-privacy-OECD-22-11-10.pdf.

[3] A. Acquisti, 2004. "Privacy In Electronic Commerce and The Economics Of Immediate Gratification." ACM Electronic Commerce Conference, 21-29.

[4] In this testimony, I use sometimes "face recognition" as a short-hand for machine-based, or computer, face recognition.

[5] R. Gross and A. Acquisti, 2005. "Information Revelation and Privacy in Online Social Networks." Proceedings of the 2005 Workshop on Privacy in the Electronic Society (WPES), ACM, 71-80, 2005; A. Acquisti and R. Gross, 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." Proceedings of Privacy Enhancing Technologies Workshop (PET), Lecture Notes in Computer Science 4258, Springer, 36-58.

[6] A. Acquisti, R. Gross, and F. Stutzman, 2011. "Faces of Facebook: Privacy In The Age Of Augmented Reality." Proceedings of Blackhat USA. http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

[7] Some of the earliest works in this area include, e.g., W.W. Bledsoe, 1964. "The model method in facial recognition." Tech. rep. PRI:15, Panoramic Research Inc., Palo Alto, CA; T. Kanada, 1973. "Computer recognition of human faces." Birkhauser, Basel, Switzerland, and Stuttgart, Germany; M.D. Kelly, 1970. "Visual identification of people by computer." Tech. rep. AI-130, Stanford AI Project, Stanford, CA.

[8] P.J. Phillips, 2011. "Improving Face Recognition Technology" Computer, 44(3), 84-86.

[9] For instance, computers outperform humans in recognizing unfamiliar faces: P.J. Phillips et al, 2007. "FRVT 2006 and ICE 2006 large-scale results." National Institute of Standards and Technology. #7408.

[10] For instance, significant debate accompanied the usage of face recognition during Super Bowl 2001; see http://www.wired.com/politics/law/news/2001/02/41571.

[11] See http://picasa.google.com/support/bin/answer.py?answer=156272. More recently (in the summer of 2011) Google also acquired Pittsburgh-based face recognition company PittPatt.

[12] See http://support.apple.com/kb/ht344.

[13] See http://www.facebook.com/blog.php?post=403838582130. More recently (in the summer of 2012), Facebook has acquired Face.com.

[14] See http://www.face.com. The application is no longer available to end-users after Face.com was acquired by Facebook.

[15] See http://www.guardian.co.uk/media/pda/2010/sep/27/advertising-billboards-facial-recognition-japan.

[16] See http://www.scenetap.com.

[17] A. Acquisti, R. Gross, and F. Stutzman, 2011. "Faces of Facebook: Privacy In The Age Of Augmented Reality." Proceedings of Blackhat USA. http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/.

[18] See S. Garfinkel and B. Rosenberg, 2009. "Face Recognition: Clever or Just Plain Creepy?" MIT Technology Review, February 27.

[19] A. Acquisti and R. Gross, 2009. "Predicting Social Security Numbers From Public Data." Proceedings Of The National Academy Of Science, 106(27), 10975-10980.

[20] P. Ohm, 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." UCLA Law Review, 57, 1701.

[21] C. Jernigan and B.F.T. Mistree, 2009. "Gaydar: Facebook friendships expose sexual orientation." First Monday,14(10).

[22] A. Acquisti and R. Gross, 2009. "Predicting Social Security Numbers From Public Data." Proceedings Of The National Academy Of Science, 106(27), 10975-10980.

[23] P.J. Phillips, 2011. "Improving Face Recognition Technology" Computer, 44(3), 84-86.

[24] J. Farrell, 2011. "Can Privacy Be Just Another Good?" Remarks presented at University of Colorado at Boulder's Conference on the Economics of Privacy.

[25] We used PittPatt, a face recognition application developed by former CMU researchers. Just a few days before our results were publicly presented, PittPatt was acquired by Google, thus the technology is no longer publicly available.

[26] See http://www.facebook.com/press/info.php?statistics.

[27] See http://www.quora.com/How-many-photos-are-uploaded-to-Facebook-each-day.

[28] See http://www.guardian.co.uk/world/2011/mar/09/chinese-blogger-mark-zuckerberg-dog.

[29] Consider: "Facebook is designed to make it easy for you to find and connect with others. For this reason, your name and profile picture do not have privacy settings," from http://www.facebook.com/policy.php, accessed July 22, 2011.

[30] See http://news.cnet.com/8301-1023_3-57455287-93/facebook-acquires-face.com-for-undisclosed-sum/.

[31] At the time of writing, one's images on Facebook by default can be tagged by people in their network, unless the individual explicitly opts-out. The power of default settings in nudging people's privacy choices has been explored, among others, by A. Acquisti, L. John, and G. Loewenstein, 2010. "What Is Privacy Worth?" In Workshop On The Economics of Information Security. (Leading Paper, 2010 Future Of Privacy Forum's Best "Privacy Papers For Policy Makers" Competition.)

http://www.heinz.cmu.edu/~acquisti/papers/acquisti-ISR-worth.pdf. Furthermore, frequent users' errors in choosing privacy settings have been found by A. Acquisti and R. Gross, 2006. "Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook." Proceedings of Privacy Enhancing Technologies Workshop (PET), Lecture Notes in Computer Science 4258, Springer, 36-58.

[32] For instance, security researcher Ashkan Soltani exploited a vulnerability in Klik to gain access to non-public photos and other potentially private data of Facebook users. See F. Rashid, 2012. "Face.com Fixes Facebook Hijacking Flaw in KLIK Mobile App." SecurityWatch, PCMag.com, June 20, 2012.

[33] Research in this area has been carried out by, among others, Ralph Gross and Latanya Sweeney.

[34] See http://epic.org/2012/02/epic-calls-for-moratorium-on-f.html.

[35] Consider, for instance, plastic surgery. We are not referring to temporary solutions (such as masks and cosmetic make-up), whose costs increases with the amount of time the person has to carry them in the course of their lives.

[36] While studies have shown that a significant portion of consumers are willing to pay price premia to purchase from more privacy protective merchants (J. Tsai, S. Egelman, L. Cranor, and A. Acquisti, 2011. "The Effect Of Online Privacy Information On Purchasing Behavior: An Experimental Study." Information Systems Research, 22, 254-268), it is not obvious that competition alone stimulates a market for privacy products. See, for more details. A. Acquisti, 2010. "The Economics Of Personal Data and The Economics Of Privacy." Commissioned By The OECD, For The OECD Roundtable On The Economics Of Privacy and Personal Data, Paris, December 2010.

[37] Extracted from Face.com FAQ in July 2011.

[38] Consider examples such as Facebook News Feed in 2006; Tagging in 2009; the changes in privacy settings in late 2009/early 2010; the lifting of cache time limits in 2010 (previously, user data accessed through APIs could only be cached by developers for 24 hours); the introduction of Facebook Places in 2010 (which allows others to tag a user in a certain location); the compulsory switch to "Timeline" in late 2011/early 2012; and the more recent switching of users to Facebook emails. These examples are discussed in work in progress by Alessandro Acquisti, Fred Stutzman, and Ralph Gross, and have been analyzed by research assistants at Carnegie Mellon University Seth Monteith and Nikolas Smart.

[39] Examples (also discussed in the work in progress mentioned in the previous footnote), include Beacon/Connect (2007-2008); and ToS change relative to the closing of a Facebook account in 2009.

[40] A. Acquisti, 2004. "Privacy In Electronic Commerce and The Economics Of Immediate Gratification." ACM Electronic Commerce Conference, 21-29.

Testimony

of

The Honorable Larry Amerson

Sheriff of Calhoun County, Alabama

Before the United States Senate Judiciary Committee

Subcommittee on Privacy, Technology and the Law

on

"What Facial Recognition Technology Means
for Privacy and Civil Liberties"

On Behalf Of

The National Sheriffs' Association
1450 Duke Street
Alexandria, VA 22314
703-836-7827

Wednesday, July 18, 2012

226 Dirksen Senate Office Building
Washington, DC 20510

Mr. Chairman, Senator Coburn, and Members of the Subcommittee:

Thank you for inviting me to testify today on behalf of the National Sheriff's Association. Chartered in 1940, the National Sheriffs' Association is a professional association dedicated to serving the Office of Sheriff and its affiliates through law enforcement education, training, and information resources. NSA represents thousands of sheriffs, their deputies and other law enforcement professionals, and concerned citizens nationwide.

I applaud the Subcommittee for holding this important hearing on the implications of facial recognition for privacy and civil liberties. These are critical concerns that rightfully need to be debated and the rights of innocent citizens protected from unwarranted interference in their privacy or everyday lives.

On the other hand, advances in technology, and especially facial recognition, which has already been implemented in law enforcement, national defense and the fight against terrorism, are a critical tool in protecting the rights of citizens, in ensuring the accurate identification of suspects, prisoners and potential terrorists is almost immediately ascertained, while protecting the safety of our citizens and law enforcement officers.

There is a critical balance between protecting the rights of law abiding citizens and providing law enforcement agencies with the most advanced tools to combat crime, properly identify suspects, catalog those incarcerated in prisons and jails, and in defending America from acts of terrorism.

Most importantly, advances in facial recognition technology over the last 10 years will result in the end of the total reliance on fingerprinting, where it takes hours and days to identify a suspect, fugitive or person being booked into a jail, to the immediate identification of those known to have criminal records, or who are wanted by law enforcement. It will surprise many in the room today to know that there is no national database of those incarcerated in America's jails at any one time. The use of facial recognition to provide instant identification of those incarcerated or under arrest will eliminate many problems while protecting innocent civilians and law enforcement officers.

For instance, utilizing facial recognition in law enforcement would:

- Interconnect law enforcement and Intel organizations to instantly share vital information with accurate identification results.
- Establish a national database of those incarcerated present and past, fugitives, wanted felons, and persons of interest among all law enforcement agencies.

- Allow officers to quickly determine who they are encountering and provide notification if a suspect is wanted or a convicted felon.
- A simple, cost effective, software based solution delivered in Windows based computers with inexpensive non-proprietary off the shelf cameras provide a huge cost savings.
- Demonstrate new capabilities in alias detection, fugitive apprehension, and speed of suspect recognition
- Ensure correct identification prisoners being released and reduce costs associated with conducted administrative procedures.
- Establish a complete national database of incarcerated persons in for the first time in U. S. history no longer could wanted criminals escape detection and arrest due to inefficient processes.

While fingerprints take hours and days for analysis, some advanced facial recognition in use today by U.S. law enforcement, is as accurate as fingerprints but results are obtained in seconds not hours in identifying criminals and perpetrators attempting to use false identities and aliases.

It is also important to point out that facial recognition comes in two forms, 2D and 3D. Only All-aspect 3D Facial systems can protect the privacy of participants who agree to be enrolled, except for in law enforcement or Homeland Security applications. All-aspect 3D cannot search on 2D facial photographs and cannot be invasive of privacy by design. Advanced facial recognition systems remove skin color and facial hair and therefore have no profiling capability.

Currently, the National Sheriffs' Association, Bureau of Prisons and United States Marshalls Service are all in support of utilizing this new three dimensional, holographic imaging technology to eliminate errors in identification; detecting false identities; and immediately identifying dangerous suspects, fugitives or terrorists rather than learning after they are released on traffic offenses or let go without suspicion because immediate identification is not possible.

Accidental releases, sometimes of dangerous felons, would also be eliminated. This technology has been in use for over 8 years in Georgia Detention Facilities with data bases of approximately 5 million inmates without a single erroneous release.

And just last year, a dangerous murderer was released from the District of Columbia jail by switching a wrist band with another inmate. This cannot happen with facial recognition.

In closing, the proper utilization of facial recognition for intelligence or law enforcement uses, can protect civil liberties, save millions of dollars, and instantly identify fugitives, felons, dangerous suspects and save lives.

Thank you Mr. Chairman and I'll be glad to answer any questions you may have.

DUKE LAW SCHOOL

Testimony and Statement for the Record of

Nita Farahany
Professor of Law, Duke Law School
Research Professor of Genome Sciences & Policy,
Institute for Genome Sciences & Policy

Hearing on
"What Facial Recognition Technology
Means for Privacy and Civil Liberties"

Before the

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

July 18, 2012
226 Dirksen Senate Office Building
Washington, DC

PREPARED STATEMENT OF NITA A. FARAHANY

Senate Judiciary Subcommittee on Privacy, Technology, and the Law: "What Facial Recognition Technology Means for Privacy and Civil Liberties"

July 18, 2012

Prepared Statement of Nita A. Farahany, Professor of Law, Professor of Genome Sciences and Policy, Duke University, Durham, NC

Chairman Franken, Ranking Member Coburn, and distinguished members of the Subcommittee. Thank you for the opportunity to express my views about facial recognition technology, and its implications for privacy and civil liberties. My name is Nita Farahany. I am a Professor of Law and Research Professor of Genome Sciences and Policy at Duke University, and my research focuses on the ethical and legal implications of emerging technologies. I am also a member of the Presidential Commission for the Study of Bioethical Issues. I appear before you today in my individual, scholarly capacity.

I will focus my comments on the legal and constitutional implications of facial recognition technologies. I hope to show that, as a general matter, law enforcement use of these technologies is not, in itself, a Fourth Amendment search, let alone an unreasonable one. Although the Court has not yet addressed facial recognition technology, the doctrine regarding analogous identifying information and "open fields" supports this view.

I. Facial Recognition Technology and Biometric Identifying Information

I will begin by explaining why I believe that law enforcement use of facial recognition technology is not a Fourth Amendment search, let alone an unreasonable one, and I will explain how Supreme Court doctrine is consistent with this view. Because the Fourth Amendment safeguards the right of the people to be secure against unreasonable searches and seizures by the government—but not by private or commercial actors—my remarks will focus on law enforcement use of this technology.

A. Facial Recognition Technology in Context: Identifying Information

Facial recognition technology uses software to try to match one's facial characteristics (such as the distance between eyes, the bridge of the nose, cheekbones, and other facial topography) with an existing database of facial data to identify an individual.[1] As the technology has developed, the accuracy of identity matching has improved by

[1] Chandrakant D. Patel et al., Biometrics in IRIS Technolgy: A Survey, 2 International Journal of Scientific and Research Publications 3 (2012), *available at* (http://www.ijsrp.org/print-journal/ijsrp-jan-2012-print.pdf#page=5) (last accessed July 14, 2012).

capturing biometric features of faces such as skin texture, and by overcoming previous hurdles posed by dim lighting and subject movement with infrared imagery.[2] Facial recognition technology is part of a broader class of identification technology, which uses the physical characteristics of an individual to match identity.[3] Other biometric identification technologies, for example, fingerprinting and iris scans, are already being used by law enforcement.[4] In fact, police forces across the country are rolling out new mobile investigative devices, some of which simply attach to the back of an iPhone, that can scan a fingerprint, an iris, or a face, and compare the results against existing databases.[5] These biometric devices and techniques add more precision to the vast array of identifying information investigators regularly obtain about individuals.[6]

A novel feature of facial recognition technology is that the first step of the process—scanning a face of interest—is usually done from a distance and without the awareness of the individual being scanned. The technology does not require physical contact, close physical proximity, or physical detention of an individual to scan their face. Infrared imagery even allows scanning to occur while a person is moving freely and is in dim lighting.

Facial recognition technology captures the sort of identifying information that is the bread and butter of law enforcement: information about the characteristics, physical likeness, and other descriptive features of a suspect.[7] It is routine practice for investigators to collect identifying information from individuals including their name, birth date, weight, height, clothing size, shoe size, blood type, and traces of shed DNA.[8] Whether collected through police-targeted or automatic photographing, facial recognition technology collects identifying evidence about individuals, a class of evidence that has traditionally received only minimal constitutional protection.

The second step of the process—comparing the scanned face to an existing database of photographs to find a match—is akin to the now-commonplace use by law enforcement of other identifying databases. Police routinely check local and national databases to find the identity of individuals by using their license plates, social security numbers, fingerprints, iris scans, and DNA to probe databases that contain such information. And all of this is nothing more than an automated version of what police have done for centuries: compare information acquired in the world with information held at police headquarters, looking for a match.

[2] Kevin Bonsor & Ryan Johnson, *How Facial Recognition Systems Work*, HOWSTUFFWORKS.COM (http://electronics.howstuffworks.com/gadgets/high-tech-gadgets/facial-recognition.htm) (last visited Dec. 4, 2011).

[3] *See* SUBCOMM. ON BIOMETRICS, NAT'L SCI. & TECH. COUNCIL, PRIVACY & BIOMETRICS: BUILDING A CONCEPTUAL FOUNDATION 4 (2006), *available at* http://www. biometrics.gov/docs/privacy.pdf (defining biometrics as "automated methods of recognizing an individual based on measurable biological . . . and behavioral characteristics").

[4] *See id.* at 15-17 (describing existing technologies for such biometric methods).

[5] Emily Steel, *How a New Police Tool for Face Recognition Works*, WALL ST. J. DIGITS BLOG (July 13, 2011, 7:56 AM), http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works.

[6] *See* Nita A. Farahany, *Incriminating Thoughts*, 64 STANFORD L. REV. 351, 368-70 (2012).

[7] *Id.* at 368.

[8] *Id.*

Neither the first step—scanning—nor the second step—querying government databases—implicates individual interests safeguarded by the Fourth Amendment. Neither step is properly characterized as a Fourth Amendment "search," let alone an "unreasonable" one, because under current law, neither step intrudes upon a legally cognizable privacy interest.

B. Scanning and Database Queries are Not Fourth Amendment "Searches"

a. Scanning from Afar

The Fourth Amendment guarantees "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[9] A Fourth Amendment search only occurs when the government intrudes upon a legally cognizable interest of an individual. Neither scanning an individual's face in public afar, nor querying a database to see if there is a match, intrudes on a cognizable privacy interest of an individual, so neither step constitutes a Fourth Amendment search.

If the police use facial recognition technology to scan an individual's face while in a public place, and that individual is not detained or touched as he is scanned, then no Fourth Amendment search has occurred. Neither his person nor his effects have been disturbed, and he lacks any legal source to support a reasonable expectation that his facial features will be hidden from government observation.[10] He has chosen to present his face to the world, and he must expect that the world, including the police, may be watching. Cameras and machines may now be doing the scanning, but for constitutional purposes, this is no different from an alert police officer "scanning" faces in a public place. This has never been thought to be a Fourth Amendment search.

By analogy, if the police observe an individual while he in public, and then return to the police station to flip through mug shot books to identify the individual they saw, no Fourth Amendment search or seizure has occurred. When the individual appeared in a public place, he relinquished his privacy interest in his seclusion. By subsequently observing the individual or comparing him against mug shot books, the police have not intruded on any legal interest retained by the individual. When an individual voluntarily forgoes seclusion, he cannot insist that the police avert their eyes.[11]

[9] U.S. CONST. amend. IV.

[10] Whether an expectation of privacy is reasonable or not has always turned on bodies of law outside of the Fourth Amendment. Privacy expectations are reflected in laws or societal norms, so a reasonable expectation of privacy "must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society." *See* United States v. Jones, 132 S. Ct. 945, 951 (2012) ("[O]ur very definition of 'reasonable expectation of privacy' . . . we have said [is] an expectation 'that has a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understanding that are recognized and permitted by society.'" (quoting Minnesota v. Carter, 525 U.S. 83, 88 (1988))).

[11] *See* California v. Greenwood, 486 U.S. 35 (1988) (holding that the Fourth Amendment does not prohibit the warrantless search and seizure of garbage left for collection outside the curtilage of a home).

If the police were to use sense-enhanced technology to surreptitiously peer through the walls of a person's home, the police will intrude upon his real property interests and seclusion he has sought by taking refuge in his home.[12] Those interests support a reasonable expectation of privacy that an individual can exclude the police from surreptitiously observing him while secluded from public view inside his home. Because his reasonable expectation of privacy will be invaded if the police observe him this manner, a Fourth Amendment search will have occurred. Yet notice a crucial difference here between facial scanning in public and spying on an individual while inside their home: to obtain the facial scan, the police do not in any way invade the personal security or property of the individual.[13] They merely observe the individual from afar, in public, and capture the image that they see.[14] This does not constitute a search.

But even if it did constitute a search, it would likely be a constitutionally reasonable one, consistent with the Fourth Amendment. An unreasonable search occurs when the degree of insult or intrusion of an individual's legal interest outweighs the societal interest in the evidence being sought. So if the police surreptitiously observe an individual inside his home, the search will only be unreasonable if the degree of intrusion on the individual outweighs the societal need for the evidence sought. Since the Court primarily uses property rights to inform Fourth Amendment privacy interests, it likewise measures the intrusiveness of the search by assessing the physical intrusion upon the property, instead of the personal indignity that one may have endured by having their personal information revealed. Because protection of the home receives the most stringent Fourth Amendment protection, even a legitimate societal need for observing an individual inside their home is unlikely to be found reasonable.[15] By contrast, searching or seizing a person's likeness by scanning their face from afar does not interfere with their personal security or a right to exclude others they may otherwise enjoy. No physical violence or even physical interference occurs: Mere observation is not tantamount to a search, and certainly not an unreasonable one.

[12] *See* Kyllo v. United States, 533 U.S. 27 (2001) (finding the use of thermal imaging to scan a person's home to be a Fourth Amendment "search").

[13] E.g., Florida v. Riley, 488 U.S. 445 (1989) (holding that no Fourth Amendment search had occurred when a police helicopter flew overhead at low altitude a greenhouse and the pilot looked through a hole in the roof of the greenhouse and saw drugs being grown inside); California v. Ciraolo, 476 U.S. 207 (1986) (finding that aerial surveillance of a person's yard blocked from view by an outer fence because the Fourth Amendment does not require that police "shield their eyes when passing by a home on public thoroughfares," so the surveillance was not a search when it took place from a public place); Dow Chemical v. United States, 476 U.S. 227 (1986) (determining that the taking of photography from navigable airspace was not a Fourth Amendment search).

[14] *See* generally Orin S. Kerr, *An Equilibrium Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 522-29 (2011) (discussing Fourth Amendment "open fields" cases that allow surveillance of the curtilage of one's home).

[15] *See* Nita A. Farahany, *Searching Secrets*, 160 U. Penn. L. Rev. 1239, 1255 (2012), citing *Payton v. New York*, 445 U.S. 573, 585 (1980) ("[P]hysical entry of the home is the chief evil against which the Fourth Amendment was directed." (quoting United States v. U.S. Dist. Court, 407 U.S. 297, 313 (1972))); Mincey v. Arizona, 437 U.S. 385, 391 (1978) (holding that one does not forfeit her Fourth Amendment rights to her home by committing a crime); Alderman v. United States, 394 U.S. 165, 171-72 (1969) (linking property rights to the ability to raise a motion to exclude evidence based upon the Fourth Amendment).

b. Probing A Database

Is using a captured image to query a photographic database for a match a Fourth Amendment search? Just as a criminal suspect lacks a cognizable legal basis to complain when the police peruse mug shots at the police station, neither can an individual successfully claim that a police query of a photographic database constitutes a search of *their* persons, houses, or effects.

If the information within the database and the probe used to search it have been lawfully collected, there is no additional Fourth Amendment interest that a claimant has in preventing the police from matching their identity.[16] Ultimately, the privacy concern usually advanced regarding the inclusion in or probing of forensic databases is whether an individual has a right to *secrecy* of identifying information. But the Court has never recognized a Fourth Amendment privacy interest in the secrecy of identifying information.[17] So the probe of a photographic database is not properly considered a separate Fourth Amendment search.

c. Scanning During "Stops"

The police might instead choose to use facial scanning technology during a brief investigative stop, which requires a slightly different constitutional analysis. Beginning with *Terry v. Ohio*,[18] the Court has held that if a police officer has a reasonable suspicion that someone has committed, is committing, or is about to commit a crime, the officer may detain the individual without a warrant for a brief investigative stop. While such stops are Fourth Amendment "searches" and a person is "seized" while they are detained, a warrantless stop based on reasonable suspicion may nevertheless be a reasonable search and/or seizure.

During a *Terry* stop, the police may require an individual to disclose his identity,[19] and a facial recognition scan for identification is not meaningfully different. Indeed, a suspect can be "arrested and prosecuted for refus[ing]" to disclose his identity during a stop based on reasonable suspicion.[20] As the Court has explained, states may require a suspect to disclose his name during an investigative stop because the individual privacy interest in identity is negligible compared to the legitimate government interests promoted by the inquiry.[21]

[16] See, e.g., Jack M. Balkin, Essay, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 20 (2008) ("The Fourth Amendment does not require governments to discard any information they have already lawfully collected.")

[17] *See* Nita A. Farahany, *Searching Secrets*, 17, at 1277-82 (discussing Fourth Amendment doctrine concerning identifying information); Nita A. Farahany, *Incriminating Thoughts*, supra note 6, at 368-72 (discussing the category of identifying evidence and constitutional protections of the same).

[18] 392 U.S. 1 (1968).

[19] Hiibel v. Sixth Judicial District Court of Nevada, 542 U.S. 177 (2004).

[20] *Id.* at 186-87 (citation omitted).

[21] *See id.* at 188 (noting that the "stop and identify" statute at issue in the case served the useful purpose of increasing the likelihood that a suspect would actually disclose his identity to a police officer).

If a police officer detains an individual based on reasonable suspicion, using facial recognition technology during that stop would not meaningfully change the Fourth Amendment reasonableness of the search and seizure. The individual privacy interest that the Court recognizes during "stop and frisk" detentions is the personal security the individual and an interest against interference with his free movement, not the secrecy of their personal information or his personal identity. In other words, the Court has not included secrecy of personally identifying information as a relevant privacy interest in determining the reasonableness of a "stop and frisk" detention.[22] If the police can take the more intrusive step of requiring a suspect to state his name, it can surely take the less intrusive approach of connecting a name to the face automatically.

In fact, when it comes to identifying information, the Court has held that individuals have minimal, if any, expectation of privacy in the secrecy of their identifying information.[23] This is because the Fourth Amendment provides no protection for what "a person knowingly exposes to the public, even in his own home or office."[24] The physical characteristics of a person's face, its shape and contours are constantly exposed to the public, so no person can have a reasonable expectation that others will not observe his facial features. Indeed, the Court has held that compelling a suspect to provide physically identifying information—such as fingerprints[25] or voice exemplars[26]—is usually reasonable because such techniques intrude upon no cognizable individual interest. A facial scan is far less intrusive than either of these. Lower courts have held similarly in other identification and location-determination cases, even including the use of beepers to pinpoint location.[27] In short, in each of these identifying-information cases, the Court has held that the relevant individual interest at stake is in personal security or privacy as seclusion, but has not acknowledged a privacy interest in keeping personal information a secret.

The measure of personal intrusion during an investigative stop using facial recognition scanning will likely be the length of the detention and the physical intrusiveness of the

[22] For example, the Court in *United States v. Dionisio*, 410 U.S. 1 (1973), noted that

> the Fourth Amendment provides no protection for what "a person knowingly exposes to the public, even in his own home or office . . . ." The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. . . . No person can have a reasonable expectation that others will not know the sound of his voice . . . .

Id. at 14 (first alteration in original) (citation omitted) (quoting Katz v. United States, 389 U.S. 347, 351 (1967)).

[23] *See* Farahany, supra note 17.

[24] *United States v. Dionisio*, 410 U.S. 1, 14 (1973) (describing the reasonable expectation that others will be familiar with one's physical features).

[25] *See* Davis v. Mississippi, 394 U.S. 721, 727 (1969) ("Detention for fingerprinting may constitute a much less serious intrusion upon personal security than other types of police searches and detentions. Fingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search.").

[26] *See Dionisio*, 410 U.S. at 14 ("No person can have a reasonable expectation that others will not know the sound of his voice, any more than he can reasonably expect that his face will be a mystery to the world.").

[27] *See* Recent Development, *Who Knows Where You've Been?: Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 HARV. J.L. & TECH. 307, 314-15 (2004) (describing *United States v. Forest*, 355 F.3d 942 (6th Cir. 2004), which held that pinpointing one's location or movement through one's beeper is not subject to a reasonable expectation of privacy).

search techniques employed. If by using such technology the police held an individual for longer, or required that he pose in a compromising or otherwise physically arduous manner, then *those* actions could render the search more intrusive and affect its reasonableness. But since the police can use facial recognition software unobtrusively and almost instantaneously, its use should not change the constitutional calculus of a *Terry* stop or convert an otherwise reasonable search and seizure into an unreasonable one.

C. Supreme Court Doctrine Protects Privacy as Seclusion but not Secrecy

Real property law informs whether an individual has a reasonable expectation of privacy in secluding—i.e. restricting access to others—the property searched.[28] Facial recognition technology does not interfere with a cognizable Fourth Amendment privacy interest, such as interference with real or intellectual property rights, nor does it intrude upon personal security or movement. As such, there is no source of law upon which a reasonable expectation of privacy to object to facial recognition scanning could be grounded.[29]

Concepts of possession and property are at the core of the Fourth Amendment, as its possessive pronoun makes clear: "the right of the people to be secure in *their* persons, houses, papers, and effects." And so, from the beginning,[30] the Court has turned to property law to inform Fourth Amendment interests.[31] When the Court first encountered the modern investigative technique of wiretapping, for example, which like facial recognition enables investigators to obtain evidence without any physical interference with one's property, the Court found that no search had occurred because conversations are not tangible property or "material things" that the Fourth Amendment protects.[32] Likewise, facial recognition technology does not implicate any property interests.

Now, to be sure, the Court has subsequently extended the Fourth Amendment beyond property, as Justice Brandeis had urged in dissent. In *Katz v. United States*, the Court held that the Fourth Amendment applies to tangible and intangible interests such as private conversations,[33] because it safeguards from unreasonable search and seizure what an

[28] Richard A. Posner, *Privacy, Secrecy, and Reputation*, 28 BUFF. L. REV. 1, 3-4 (1979); *see also id.* ("An equivalent term is 'retirement' in its complex modern sense in which we speak of a person being 'retiring' and also of a person being 'retired.'").

[29] *See* Farahany, supra note 15, at 1254 (explaining that the most consistently recognized subjective and objective expectation of privacy is one that derives, at least in part, "'from the right to exclude others from the property in question.'")(internal citations omitted).

[30] U.S. Const. amend IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

[31] *See* Boyd v. United States, 116 U.S. 616, 627 (1886) (stating that the "sacred and incommunicable" right of property is only set aside "for the good of the whole" (quoting Entick v. Carrington, (1765) 19 How. St. Tr. 1029 (C.P.) 1066 (Eng.)). *See also* Farahany, supra note 17, at 1244-49 (reviewing how property law has informed Fourth Amendment privacy interests).

[32] Olmstead v. United States, 277 U.S. 438, 457 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

[33] In *Katz v. United States*, 389 U.S. 347 (1967), FBI agents attached a device to the outside of a public telephone booth to listen to the defendant's conversations, and the Government argued that this eavesdropping did not implicate the Fourth Amendment because no trespass upon the defendant's property occurred. The government rejected the idea that an intrusion upon a constitutionally protected area must occur for the Fourth Amendment to apply.

individual "seeks to preserve as private."[34] Justice Harlan concurred and proposed the expectation-of-privacy analysis[35] that the Court eventually adopted.[36] This privacy test holds that a Fourth Amendment search occurs when an individual has a subjective expectation of privacy, that society recognizes as reasonable, which has been invaded.[37] Consistent with this analysis, the key Fourth Amendment question concerning facial recognition technology is whether its investigative use intrudes upon a privacy interest that society recognizes as reasonable.

Even with this expanded view of individual interests, however, an individual who is scanned in public cannot reasonably claim that facial recognition technology captures something he has sought to seclude from public view. Instead, he must argue that he has a reasonable expectation of privacy in his personal identity associated with his facial features. Under current doctrine, courts would properly reject such a claim. Despite the shift in *Katz* from purely property-based privacy protections to seclusion more generally, the Court has not recognized an independent privacy interest in the secrecy of identifying information per se.

Consequently, it is the physical intrusiveness of facial recognition technology, and not the extent to which it reveals personally identifying information, that will determine its reasonableness in a Fourth Amendment inquiry.[38] And because the technology is physically unobtrusive and does not reveal information that is secluded or otherwise hidden from public view, it is not properly characterized as a Fourth Amendment search.

Most recently, in *United States v. Jones*,[39] the Court revisited its property-invasion-as-privacy rationale, holding that the government's installation of a GPS tracking device on a suspect's vehicle constitutes a search subject to the Fourth Amendment.[40] In so doing, it left open whether the Fourth Amendment protects more than just intrusion upon seclusion. Justice Scalia, writing for the majority, emphasized that the government had "physically occupied private property for the purpose of obtaining information."[41] Invoking Lord Camden's opinion in *Entick v. Carrington*[42] and the text of the Fourth Amendment itself, Justice Scalia reaffirmed the significance of property rights to search and seizure analysis.[43] Although acknowledging that the Court had expanded beyond a strictly property-based approach in *Katz*, the opinion nevertheless emphasized that

[34] *Id.* at 351-52.

[35] *See id.* at 361 (Harlan, J., concurring).

[36] *See* Smith v. Maryland, 442 U.S. 735, 740-41 (1979) (The court held that the government's use of a pen register—a device that records the phone numbers one dials—was not a Fourth Amendment search. The Court explained that "a pen register differs significantly from the listening device employed in *Katz*, for pen registers do not acquire the *contents* of communications.")

[37] *Katz*, 389 U.S. at 361. Since *Katz*, Fourth Amendment law has also addressed the concealment of information. But even in *Katz*, the Court ultimately focused on Katz's seclusion of himself in the phone booth and not on his interest in the substantive secrecy of his conversation.

[38] *See* Terry v. Ohio, 392 U.S. 1, 30-31 (1968) (holding that the Fourth Amendment permits "reasonable inquiries" to determine a suspect's identity).

[39] 132 S. Ct. 945 (2012).

[40] *Id.* at 949 (2012).

[41] *Id.*

[42] (1765) 19 How. St. Tr. 1029 (C.P.) (Eng.).

[43] *Jones*, 132 S. Ct. at 949.

property rights remain the central source of individual interests protected by the Fourth Amendment.[44] While the police could have obtained the same information in *Jones* without a physical trespass, and such an intrusion might still be unconstitutional under *Katz*, the facts in *Jones* did not require the Court to resolve that question.[45]

What remains after *Jones* is an incomplete picture of which individual interests beyond real property interests, if any, that the Fourth Amendment protects. At the very least, *Jones* repudiates the view that *Katz* was "a shift in Fourth Amendment jurisprudential paradigms from a property-based framework to an expectation-of-privacy framework."[46] Real property law remains central to Fourth Amendment individual interests. And under a property analysis, facial recognition is clearly not a search.

To be sure, the *Jones* majority also emphasized that trespass upon property and the *Katz* expectation-of-privacy test coexist in Fourth Amendment jurisprudence. But even under a privacy-based analysis, the use of facial recognition technology is not analogous to the wiretap in *Katz*, and as such is not properly characterized as a search. If facial recognition technology captures facial features that an individual has not secluded,[47] then unlike *Katz*, its investigative use does not intrude upon information that an individual has kept hidden. Without trespass upon real property, or upon information that a person has sought to hide, there is no legitimate source of law upon which a reasonable expectation of privacy could be founded.

Conclusion

As I have explained, governmental use of facial recognition technology does not generally constitute a Fourth Amendment search, let alone an unreasonable one. Nevertheless, this technology does raise novel privacy concerns, which are certainly the proper concern of Congress.

As some of the other panelists have emphasized, it is a brave new world, in which our reasonable expectation of privacy may seem to be under assault by technology. And Congress may indeed have a role to play in striking the proper balance between privacy and security in this area. I would emphasize, though, that the legal and ethical landscape here is very complex, implicating a variety of cross-cutting interests. (The answers may be different depending on whether these tools are being used by governments or by private actors, and it may matter whether people have opted into a database or been included against their will.). These sorts of technological advances may indeed diminish our privacy. But they are also extraordinarily useful, to private individuals, to corporations, to social networks, and to law enforcement. I am not at all certain that legislation is required in this area. But in any case, I would encourage the Subcommittee to consider carefully the legal,

[44] *Id.* at 950.

[45] *Id.* at 954. Since the government took the position that GPS tracking did not constitute a search, the Court left for another day the further question of which individual interests, beyond intrusion upon property, an individual could claim to assess the reasonableness of the search that had occurred.

[46] David A. Sullivan, A Bright Line in the Sky?: Toward a New Fourth Amendment Search Standard for Advancing Surveillance Technology, 44 ARIZ. L. REV. 967, 974 (2002).

[47] E.g. by wearing a mask, a veil, or other head covering that hides their visage.

ethical, and social implications of any legislative response. Again, I thank you for the opportunity to appear before you today, and I look forward to your questions.

TESTIMONY OF ROBERT SHERMAN
MANAGER, PRIVACY & PUBLIC POLICY
FACEBOOK

HEARING ON WHAT FACIAL RECOGNITION TECHNOLOGY MEANS
FOR PRIVACY AND CIVIL LIBERTIES

BEFORE THE PRIVACY, TECHNOLOGY AND THE LAW SUBCOMMITTEE
OF THE SENATE COMMITTEE ON THE JUDICIARY

JULY 18, 2012

Chairman Franken, Ranking Member Coburn, and Members of the Committee, my name is Robert Sherman, and I am the Manager of Privacy and Public Policy at Facebook. Thank you for the opportunity to share Facebook's views on what the increasing use of facial recognition technology means for the American people. Facebook is committed to building innovative tools that enhance people's online experiences while giving them control over their personal information. Our integration of facial recognition technology into tag suggestions on Facebook exemplifies this commitment, and I look forward to discussing with you the privacy and security protections that we have built into this feature.

At Facebook, we understand the importance of continuing to build innovative technologies that help people communicate and share in a way that honors and preserves the trust that they have placed in us. Indeed, we believe that our success as an innovator is largely due to the work that we do every day to build and maintain people's confidence that we will be good stewards of their data.

In my testimony today, I will first describe the important user controls that we include in our tag suggestions feature. Second, I will address the steps we take to safeguard the data we maintain in connection with tag suggestions.

I. Facebook's Photo Management Tools, Including Tag Suggestions, Were Designed With Privacy at the Forefront

At Facebook, we implement facial recognition technology in our popular and innovative tag suggestions tool, which helps users manage and share their photos. In the early days of Facebook, we learned how important photo sharing was to our users when we realized that people were frequently changing their profile photos to show friends their most recent snapshots. In response to that feedback, in 2005 we built a feature that allowed people to upload and share photos on Facebook, and we have continued building those features ever since. One component of our photo management and sharing features is photo tagging, which is the 21st century's version of handwriting captions on the backs of photographs, and it allows users to instantaneously link photos from birthdays, vacations, and other important events with the people who participated. To help our users more efficiently tag their friends in photos, we built tag suggestions, which uses facial recognition technology to suggest people they already know and whom they might want to tag. In recent years, other companies have begun using facial recognition technology as well, and many photo management services incorporate tools similar to ours. Today, photo sharing is so popular on Facebook that as many as 300 million new photos are uploaded to our service each day. To keep up with that demand, a few months ago we took our tag suggestions feature down to improve its efficiency. We plan to restore the feature to our site soon.

To understand how tag suggestions work, and how we designed the feature to protect our users' privacy, it helps to have a general understanding of the core tools and controls we provide to help people organize and share their photos.

A. Photos and Tagging on Facebook

Facebook's photo management tools are among the most popular features on our service in large part because they build upon things people could always do with their photos — such as placing them in albums and adding captions — by making photos more social. The key to making photos social on Facebook is our "tagging" feature. On Facebook, a "tag" is a special link that can be used to associate a photo with a particular user's page on Facebook, which we call a "timeline," and, depending on the person's privacy settings, share that photo with others. The popularity of tagging is no doubt due to the social interaction it encourages. Tags also help promote transparency and control on Facebook because when a person is tagged, by default Facebook lets that person know. This allows the person included in the photo to interact with the user who uploaded it or to take action if he or she does not like the photo, such as removing the tag or requesting that the photo be removed entirely. And the photo may be shared with others (again, depending on privacy settings), who may "Like" or comment on the photo.

Another reason why photos and tagging are such popular features on Facebook is the fine-grained privacy controls built into those tools. For example:

- Inline privacy controls. When people share photos on Facebook, our inline audience selectors enable them to determine with precision the audience with whom the photos will be shared. These controls are presented at a time and in a way that allows a person to make a meaningful decision about her photos when he or she is posting them.

- Tag review. Tag review allows people to pre-approve stories where they are tagged before they appear on their timeline.

- Tag removal. A person can "untag" a photo in which she appears, thereby unlinking it from her account.

- Blocking. Facebook's privacy settings allow people to "block" others who tag them in photos. Blocking prevents the blocked person from tagging the person again in photos.

- Reporting. Photos on Facebook contain a "Report" link, which enables people to request removal of objectionable photos. Through this link, a person can easily contact the person who posted the photo to make a deletion request or refer the photo to Facebook for professional review.

As with all our products and services, we constantly strive to make our photo management tools more responsive to the needs of people who use Facebook. After we introduced tagging, many people told us that the feature was useful but that manually entering tags for each person in every photo required a great deal of time and effort. We developed tag suggestions in response to this feedback.

B. Tag Suggestions

Tag suggestions automate the process of identifying and, if the user chooses, tagging friends in the photos he or she uploads. Convenience features like this, which are designed to automate tools, are common with online services and often greatly enhance everyone's experience – especially with popular products like photo sharing. Tag suggestions works by determining what several photos in which a person has been tagged have in common and storing a summary of the data derived from this comparison in a file that we call a "template". When a person uploads a new photo, we compare that photo to the summary information in the templates of the people on Facebook with whom the person communicates most frequently. This allows us to make suggestions about whom the user should tag in the photo, which the user can then accept or reject.

Tag suggestions has been enthusiastically embraced by millions of people on our service because it is convenient and the uploader is in control of their photos. We recently acquired Face.com, the company from which we licensed the technology that we use to operate tag suggestions. The engineers who worked at Face.com are working with us to improve the efficiency of our tag suggestion systems. In the interim, we are working to wind down Face.com's operations.

When we first designed tag suggestions, we considered how to implement the technology in a way that would respond to people's demand for better tagging tools without diminishing their ability to control the collection, use, and disclosure of their information. We launched the feature with several important privacy protections.

First, we are transparent about our use of the technology. Our Data Use Policy[1] contains a clear and concise explanation of tag suggestions and links to a series of frequently

[1] *See* https://www.facebook.com/full_data_use_policy.

asked questions in our Help Center,[2] which describes how tag suggestions work and how people can control the feature.

Second, tag suggestions only use data people have voluntarily provided to Facebook — photos and the tags people have applied to them — and derives information from that data to automate the process of future tagging. We do not collect any new information beyond the photos themselves in order for tag suggestions to work. In this regard, tag suggestions are similar to the recommendations offered by popular sites such as Amazon and Netflix. Like those services, tag suggestions simply takes data that people have provided and uses that data to make helpful, time-saving predictions about how people may want to use our site. Unlike implementations of facial recognition that rely on the direct collection of data from people with whom the collector has no preexisting relationship, the people who provide the data that powers tag suggestions have established relationships with Facebook and choose to use our service because they want to share information about themselves in a safe and controlled way.

Third, Facebook's technology does not enable people to identify others with whom they have no relationship. Tag suggestions simply use a list of a person's friends who have been tagged in other photos and suggests which of those friends might be in the photos she uploads. Facebook's technology is not designed to search for random strangers – rather, it is optimized to help you automate the tagging of the people in your photos so you can share those photos with them.

Fourth, and perhaps most importantly, Facebook enables people to prevent the use of their image for facial recognition altogether. Through an easy-to-use privacy setting, people can choose whether we will use our facial recognition technology to suggest that their friends tag

[2] *See* https://www.facebook.com/help/tag-suggestions.

them in photos. If a person chooses not to allow this, as we explain on our website: "When you turn off tag suggestions, Facebook won't suggest that friends tag you when photos look like you. The template that we created to enable the tag suggestions feature will also be deleted."[3] Facebook's tag suggestions feature, unlike other facial recognition products, is based specifically on individual control. It makes suggestions based on the networks that people have formed expressly on Facebook, rather than seeking to identify unknown people. And it further empowers people to control the experience, even within those expressly created networks, by notifying them when they are tagged and giving them a range of choices about how information derived from that tag will be used.

II. Facebook Provides Strong Safeguards for the Data Used For Tag Suggestions

In addition to providing appropriate privacy controls, Facebook has implemented strong technical and procedural safeguards for the personal information we store, including the templates used to power tag suggestions. We encrypt these templates as they are stored on our servers and limit the ability of people within Facebook to access this information.

In addition, the nature of our technology, federal law, and our internal policies restrict the facial recognition data we disclose to third parties, including law enforcement. Two aspects of our unique technology severely limit its usefulness to law enforcement agencies. First, our templates work only with our proprietary software. Alone, the templates are useless bits of data. Second our software cannot be used to compare a photo of an unknown person against our database of user templates. Our technology is designed to search only a limited group of templates — namely, an individual user's friends — and law enforcement agencies accordingly cannot use our technology to reliably identify an unknown person.

[3] https://www.facebook.com/help/?faq=187272841323203#How-can-I-turn-off-tag-suggestions?

Moreover, as we describe in our Law Enforcement Guidelines[4] — we are one of only a handful of major Internet companies to post them online — Facebook has implemented rigorous procedures meant to ensure that information is shared with law enforcement only in very limited circumstances pursuant to applicable law. As we describe on our website, we disclose account records solely in accordance with our terms of service and applicable law. Indeed, a dedicated team of professionals scrutinizes each request for legal sufficiency and compliance with Facebook's internal requirements, and we regularly oppose requests that we believe violate the law. Our Data Use Policy also provides the ability to share information with law enforcement in emergency situations including risk of death or bodily harm. Such situations are rare, and we take very seriously the commitments we have made to people who use Facebook in our Data Use Policy.

III. Conclusion

I hope that my testimony today has helped the Members of this Committee understand how Facebook uses facial recognition technology and, more importantly, the privacy and security protections that define our implementation of the technology. The tools we create to enable people to share information with friends and family — and the innovative ways in which we let users control their information — will no doubt continue to evolve. But our fundamental commitment to protect the privacy and security of the people who use Facebook will not change. We look forward to continuing cur dialogue with you on this important subject.

Thank you for the opportunity to testify today. I look forward to answering any questions you may have.

[4] https://www.facebook.com/safety/groups/law/guidelines/.

Written Testimony of Jennifer Lynch
Staff Attorney with the Electronic Frontier Foundation (EFF)

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology, and the Law

What Facial Recognition Technology Means for Privacy and Civil Liberties

July 18, 2012

Mr. Chairman and Members of the Subcommittee:

Thank you very much for the opportunity to testify today on facial recognition. My name is Jennifer Lynch, and I am an attorney with the Electronic Frontier Foundation (EFF) in San Francisco. For the last few years, first at the Samuelson Law, Technology & Public Policy Clinic at Berkeley Law School and then at EFF, I have studied the privacy implications of new technologies, including facial recognition. I have written and presented on federal, state and local law enforcement efforts to expand biometrics databases by adding facial recognition capabilities and on the impact that would have on all Americans and especially on immigrant communities. At EFF I file and litigate Freedom of Information Act requests, including several related to biometrics and facial recognition, and analyze and report on the records I receive. I have been interviewed for and quoted on biometrics and other privacy-threatening technologies in mainstream and technical press including the *New York Times*, *The Economist*, *Los Angeles Times*, *Wall Street Journal*, *NPR*, *Wired*, *Huffington Post*, *CNet*, *Forbes*, and elsewhere.

Although the collection of biometrics—including face recognition-ready photographs—seems like science fiction; it is already a well-established part of our lives in the United States. The Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) each have the largest biometrics databases in the world,[1] and both agencies are working to add extensive facial recognition capabilities. The FBI has partnered with several states to collect face recognition-ready photographs of all suspects arrested and booked,[2] and, in December 2011, DHS signed a $71 million dollar contract with Accenture to incorporate facial recognition and allow real-time biometrics sharing with the Department of Justice (DOJ) and Department of Defense (DOD). State and local law-enforcement agencies are also adopting and expanding their own biometrics databases to

[1] FBI, *Integrated Automated Fingerprint Identification System*, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited July 16, 2012); Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

[2] *See* Aliya Sternstein, "FBI to Launch Nationwide Facial Recognition Service," *Nextgov.com* (Oct. 7, 2011), *available at* http://www.nextgov.com/nextgov/ng_20111007_6100.php.

incorporate face recognition, and are using handheld mobile devices to allow biometrics collection in "the field."[3]

The scope of government-driven biometrics data collection is well-matched by private-sector collection. Facebook, which uses face recognition by default to scan all photos uploaded to its site, states that its users uploaded more than 300 million photos *every day* in the three months ending on March 31, 2012.[4] And Face.com, which developed Facebook's face recognition tools and was recently acquired by the company, stated in March that it had indexed 31 billion face images.[5] Other companies, from large technology companies like Google and Apple to small smartphone app providers, also provide face recognition products to their customers, and private companies are using biometric identification for everything from preventing unauthorized access to computers and corporate facilities to preventing unauthorized access to the gym.[6]

Face recognition is here to stay, and, though many Americans may not realize it, they are already in a face recognition database. Facebook refuses to say how many face prints it has in its database and whether it creates a face print for photos of non-Facebook users.[7] However, given that Facebook has approximately 170 million active monthly users in the United States alone, at least 54% of the United States population already has a face print.[8]

Face recognition technology, like other biometrics programs that collect, store, share and combine sensitive and unique data poses critical threats to privacy and civil liberties. Biometrics in general are immutable, readily accessible, individuating and can be highly prejudicial. Face recognition, though, takes the risks inherent in other biometrics to a new level because Americans cannot take precautions to prevent the collection of their image.

[3] *See* Emily Steel, "How a New Police Tool for Face Recognition Works," *Wall St. J. Digits Blog* (July 13, 2011) http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/ (describing the Mobile Offender Recognition and Information System (MORIS), which attaches to an iPhone and allows face, fingerprint and iris scanning and identification). As I have written, law enforcement appears to be using these devices with little or no precursor level of suspicion. *See* Jennifer Lynch, *From Fingerprints to DNA: Biometric Data Collection in U.S. Immigrant Communities and Beyond*, Electronic Frontier Foundation & Immigration Policy Council Whitepaper, 3 (May 23, 2012) available at https://www.eff.org/wp/fingerprints-dna-biometric-data-collection-us-immigrant-communities-and-beyond.

[4] Facebook, *Key Facts: Statistics* (last visited July 9, 2012) http://newsroom.fb.com/content/default.aspx?NewsAreaId=22.

[5] See Yaniv Taigman and Lior Wolf, "Leveraging Billions of Faces to Overcome Performance Barriers in Unconstrained Face Recognition," Face.com, http://face.com/research/faceR2011b.html (last visited Mar. 15, 2012).

[6] Demian Bulwa, "Fingerprint check-in tried at 24 Hour Fitness," *S.F. Chron.* (Aug 23, 2010) http://www.sfgate.com/bayarea/article/Fingerprint-check-in-tried-at-24-Hour-Fitness-3255272.php

[7] For example, many Facebook users regularly upload photographs of their non-Facebook using babies and children and identify these images with a name in the description field for the photo. Others create Facebook profiles for their unborn children. *See* Steven Leckart, "The Facebook-Free Baby," *Wall St. J.*, http://online.wsj.com/article/SB10001424052702304451104577392041180138910.html

[8] This is a conservative estimate based on the latest U.S. population figures. It doesn't account for the fact that Facebook, which uses face recognition to scan all photographs uploaded, may be creating a face print for non-Facebook users as well.

Face recognition allows for covert, remote and mass capture and identification of images—and the photos that may end up in a database include not just a person's face but also how she is dressed and possibly whom she is with. This creates threats to free association and free expression not evident in other biometrics.

Americans cannot participate in society without exposing their faces to public view. Similarly, connecting with friends, family and the broader world through social media has quickly become a daily (and some would say necessary) experience for Americans of all ages. Though face recognition implicates important First and Fourth Amendment values, it is unclear whether the Constitution would protect against over-collection. Without legal protections in place, it could be relatively easy for the government or private companies to amass a database of images on all Americans.

This presents opportunities for Congress to develop legislation that would protect Americans from inappropriate and excessive biometrics collection. The Constitution creates a baseline, but Congress can legislate significant additional privacy protections. As I discuss further below, Congress could use statutes like the Wiretap Act[9] and the Video Privacy Protection Act[10] as models for this legislation. Both were passed in direct response to privacy threats posed by new technologies and each includes meaningful limits and protections to guard against over-collection, retention and misuse of data.

My testimony will discuss some of the larger current and proposed facial recognition collection programs and their implications for privacy and civil liberties in a democratic society. It will also review some of the laws that may govern biometrics collection and will outline best practices for developing effective and responsible biometrics programs—and legislation to regulate those programs—in the future.

Government Use of Facial Recognition Technologies

Law Enforcement and government at all levels in the United States regularly collect biometrics; combine them with biographic data such as name, address, immigration status, criminal record, gender and race; store them in databases accessible to many different entities; and share them with other agencies and governments. These collection programs have, in the past, typically included only one biometric identifier (generally a fingerprint or DNA). However, many are rapidly expanding to include facial recognition-ready photographs.

Federal and State Biometrics Databases

The two largest biometrics databases in the world are the FBI's Integrated Automated Fingerprint System (IAFIS) and DHS's Automated Biometric Identification System (IDENT), a part of its U.S. Visitor and Immigration Status Indicator Technology (US-VISIT) program.[11] Each database holds more than 100 million records—more than one

[9] 18 U. S. C. §§2510–2522.

[10] 18 U.S.C. § 2710.

[11] Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

third the population of the United States. Although each of these databases currently relies on fingerprints, both are in the process of incorporating facial recognition.

IAFIS's criminal file includes records on people arrested at the local, state, and federal level and latent prints taken from crime scenes. IAFIS's civil file stores biometric and biographic data collected from members of the military, federal employees and as part of a background check for many types of jobs, such as childcare workers, law-enforcement officers, and lawyers.[12] IAFIS includes over 71 million subjects in the criminal master file and more than 33 million civil fingerprints,[13] and supports over 18,000 law-enforcement agencies at the state, local, tribal, federal, and international level.

IDENT stores biometric and biographical data for individuals who interact with the various agencies under the DHS umbrella, including Immigration and Customs Enforcement (ICE), U.S. Citizenship and Immigration Services (USCIS), Customs and Border Protection (CBP), the Transportation Security Administration (TSA), the U.S. Coast Guard, and others.[14] Through US-VISIT, DHS collects fingerprints from all international travelers to the United States who do not hold U.S. passports.[15] USCIS also collects fingerprints from citizenship applicants and all individuals seeking to study, live, or work in the United States.[16] And the State Department transmits fingerprints to IDENT from all visa applicants.[17] IDENT processes more than 300,000 "encounters" every day and has 130 million records on file.[18]

In addition to the federal databases, each of the states has its own biometrics databases, and some larger metropolitan areas like Los Angeles also have regional databases. The

[12] *Privacy Impact Assessment (PIA) for the Next Generation Identification (NGI) Interstate Photo System (IPS)* (hereinafter "2008 IPS PIA"), FBI (June 9, 2008), http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[13] *See* http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/iafis/iafis (last visited Apr. 26, 2012).

[14] *See* DHS, "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)," (July 31, 2006), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit _ident_final.pdf.

[15] Customs and Border Protection (CBP) feeds biometrics data into IDENT while also maintaining its own database, called TECS, which includes personally identifiable information on and biometrics obtained from travelers crossing the border into the United States. *See* DHS, "Privacy Impact Assessment for the TECS System: CBP Primary and Secondary Processing" ("TECS PIA"), DHS/CBP/PIA-009(a), (Dec. 22, 2010), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-cbp-tecs-sar-update.pdf.

[16] DHS, "Privacy Impact Assessment for the Refugees, Asylum, and Parole System and the Asylum Pre-Screening System" (Nov. 24, 2009), *available at* http://www.dhs.gov/xlibrary/assets/ privacy/privacy_pia_cis_rapsapss.pdf. USCIS also maintains its own database of "biometric images," including a digital photograph and signature, both of which appear on an applicant's naturalization certificates. *See* DHS, "Privacy Impact Assessment Update for the Computer Linked Application Information Management System, DHS/USCIS/PIA-015(a)" (Aug. 31, 2011), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_claimsupdate.pdf (describing capturing of "digitized biometric images" through the Benefits Biometric Support System (BBSS)).

[17] *See* DHS, "Government Agencies Using US-VISIT," http://www.dhs.gov/files/programs/gc_ 1214422497220.shtm.

[18] Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

prints entered into these databases are shared with the FBI, and under the Secure Communities program, with DHS.

Incorporating Face Recognition Capabilities into Existing Government Databases
In the last few years, federal, state and local governments have been pushing to develop "multimodal" biometric systems that collect and combine two or more biometrics (for example, photographs and fingerprints[19]), arguing that collecting multiple biometrics from each subject will make identification systems more accurate.[20] The FBI's Next Generation Identification (NGI) database represents the most robust effort to introduce and streamline multimodal biometrics collection. FBI has stated it needs "to collect as much biometric data as possible . . . and to make this information accessible to all levels of law enforcement, including International agencies."[21] Accordingly, it has been working "aggressively to build biometric databases that are comprehensive and international in scope."[22]

The biggest and perhaps most controversial change brought about by NGI will be the addition of face-recognition ready photographs.[23] The FBI has already started collecting such photographs through a pilot program with a handful of states.[24] Unlike traditional mug shots, the new NGI photos may be taken from any angle and may include close-ups of scars, marks and tattoos.[25] They may come from public and private sources, including from private security cameras, and may or may not be linked to a specific person's record (for example, NGI may include crowd photos in which many subjects may not be identified). NGI will allow law enforcement, correctional facilities, and criminal justice agencies at the local, state, federal, and international level to submit and access photos, and will allow them to submit photos in bulk.

The FBI has stated that a future goal of NGI is to allow law-enforcement agencies to identify subjects in "public datasets," which could include publicly available

[19] Existing biometric databases have allowed users to input some photographs, but they have been limited to traditional mug shots and have not incorporated facial recognition capabilities. *See* 2008 IPS PIA, http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[20] *Next Generation Identification*, FBI, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited April 27, 2012).

[21] *See Statement: Interoperability Initiatives Unit* (December 2010), Bates No. SC-FBI-FPL-1043, available at http://uncoverthetruth.org/wp-content/uploads/S-Comm-Hot-Docs-Released-11-10-11.zip (download archive; unzip; open "SC-FBI-FPL-1043.pdf").

[22] *Id.*

[23] Once NGI is complete, it will include iris scans, palm prints, and voice data, in addition to fingerprints.

[24] According to *Nextgov.com*, these states include Michigan, Washington, Florida, and North Carolina. *See* Aliya Sternstein, "FBI to Launch Nationwide Facial Recognition Service," *Nextgov.com* (Oct. 7, 2011), *available at* http://www.nextgov.com/nextgov/ng_20111007_6100.php. However, recently-released records from an FBI Criminal Justice Information Services Advisory Board meeting show that the FBI signed MOUs in December 2011 with Maryland, Michigan and Hawaii and may also be working with Oregon. *See* Jennifer Lynch, "FBI's Facial Recognition is Coming to a State Near You," *EFF.org* (forthcoming) https://www.eff.org/deeplinks/2012/07/fbis_facial_recognition_coming_state_near_you.

[25] *See* 2008 IPS PIA, http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

photographs, such as those posted on Facebook or elsewhere on the Internet.[26] Although a 2008 FBI Privacy Impact Assessment (PIA) stated that the NGI/IAFIS photo database does not collect information from "commercial data aggregators," the PIA acknowledged this information could be collected and added to the database by other NGI users such as state and local law-enforcement agencies.[27] The FBI has also stated that it hopes to be able to use NGI to track people as they move from one location to another.[28]

Another big change in NGI will be the addition of non-criminal photos. If someone applies for any type of job that requires fingerprinting or a background check, his potential employer could require him to submit a photo to the FBI. And, as the 2008 FBI PIA notes, "expanding the photo capability within the NGI [Interstate Photo System] will also expand the searchable photos that are currently maintained in the repository." Although noncriminal information has always been kept separate from criminal, the FBI is currently developing a "master name" system that will link criminal and civil data and will allow a single search query to access all data. The Bureau has stated that it believes that electronic bulk searching of civil records would be "desirable."[29]

DHS is poised to expand IDENT to include face recognition, which would further increase data sharing between DHS and DOJ through Secure Communities and between both agencies and DOD through other programs.[30] DHS has not yet released a Privacy Impact Assessment discussing this change.

Technological Advancements Will Make Face Recognition More Prevalent
Recent advancements in camera and surveillance technology over the last few years support law enforcement goals to use face recognition to track Americans. For example, the National Institute of Justice has developed a 3D binocular and camera that allows realtime facial acquisition and recognition at 1000 meters.[31] The tool wirelessly transmits images to a server, which searches them against a photo database and identifies the photo's subject. As of 2010, these binoculars were already in field-testing with the Los Angeles Sheriff's Department. Presumably, the back-end technology for these binoculars

[26] *See, e.g.*, Richard W. Vorder Bruegge, *Facial Recognition and Identification Initiatives*, 5, FBI available at http://biometrics.org/bc2010/presentations/DOJ/vorder_bruegge-Facial-Recognition-and-Identification-Initiatives.pdf (noting a goal of NGI is to "Identify[ ] subjects in public datasets").

[27] *See* 2008 IPS PIA, http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system.

[28] *See* Vorder Bruegge, *Facial Recognition and Identification Initiatives*, 5.

[29] *See* 2008 IPS PIA, http://www.fbi.gov/foia/privacy-impact-assessments/interstate-photo-system. The FBI has recognized that "electronic bulk searching of civil file images (such as via facial recognition technology) would constitute a significant new privacy consideration," *id.*, but the FBI has not yet released a new PIA.

[30] *See* "Accenture Awarded Biometric Identity System Contract from U.S. Department of Homeland Security," *Wall Street Journal Market Watch* (Dec. 21, 2011), at http://www.marketwatch.com/story/accenture -awarded-biometric-identity-system-contract-from-us-department-of-homeland-security-2011-12-21; Elizabeth Montalbano, "DHS Expands US-VISIT Biometric Capabilities," *Information Week* (Dec. 22, 2011), http://www.informationweek.com/news/government/security/232300942.

[31] William Ford, *State of Research, Development and Evaluation at NIJ*, 17, National Institute of Justice, http://biometrics.org/bc2010/presentations/DOJ/ford-State-of-Research-Development-and-Evaluation-at-NIJ.pdf.

could be incorporated into other tools like body-mounted video cameras or the MORIS (Mobile Offender Recognition and Information System) iPhone add-on that some police officers are already using.[32]

Private security cameras and the cameras already in use by police departments have also advanced. They are more capable of capturing the details and facial features necessary to support facial recognition-based searches, and the software supporting them allows photo manipulation that can improve the chances of matching a photo to a person already in the database. For example, Gigapixel technology, which creates a panorama photo of many megapixel images stitched together (like those taken by security cameras), allows anyone viewing the photo to drill down to see and tag faces from even the largest crowd photos.[33] It also shows not just a face but also what that person is wearing; what books and political or religious materials he is carrying; and whom he is with. And image enhancement software, already in use by some local law enforcement, can adjust photos "taken in the wild"[34] so they work better with facial recognition searches.

Cameras are also being incorporated into more and more devices that are capable of tracking Americans and that can provide that data to law enforcement. For example, one of the largest manufacturers of highway toll collection systems filed a patent application in 2011 to incorporate cameras into the transponder that sits on the dashboard in your car.[35] This manufacturer's transponders are already in 22 million cars, and law enforcement already uses this data to track subjects. While a patent application does not mean the company is currently manufacturing or trying to sell the devices, it certainly shows it's interested.

Interoperability and Data Sharing

Before September 11, 2001, the federal government had many policies and practices in place to silo data and information within each agency. Since that time the government has enacted several measures that allow—and in many cases require—information sharing within and among federal intelligence and federal, state, and local law-enforcement agencies.[36] For example, currently the FBI, DHS, and Department of Defense's biometrics databases are interoperable, which means the systems can easily share and

[32] *See* Emily Steel, "How a New Police Tool for Face Recognition Works," *Wall St. J. Digits Blog* (July 13, 2011) http://blogs.wsj.com/digits/2011/07/13/how-a-new-police-tool-for-face-recognition-works/.

[33] James Fallows, "Technology Is Our Friend ... Except When It Isn't," *The Atlantic* (Aug. 27, 2011) http://www.theatlantic.com/technology/archive/2011/08/technology-is-our-friend-except-when-it-isnt/244233/.

[34] *Pinellas County Sheriff's Office: DHS Future Opportunities*, 10 (2010) http://biometrics.org/bc2010/presentations/DHS/mccallum-DHS-Future-Opportunities.pdf.

[35] Bob Sullivan, "Gov't cameras in your car? E-toll patent hints at Big Brotherish future," *MSN* (Oct. 14, 2011) http://redtape.msnbc.msn.com/_news/2011/10/14/8308841-govt-cameras-in-your-car-e-toll-patent-hints-at-big-brotherish-future.

[36] This was achieved through provisions in the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272 (2001), several Executive Orders (Exec. Order No. 13356, 69 C.F.R. 53599 (2004), Exec. Order No. 13355, 69 C.F.R. 53593 (2004), Exec. Order No. 13354, 69 C.F.R. 53589 (2004), Exec. Order No. 13311, 68 C.F.R. 45149 (2003)), and the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (2004).

exchange data.[37] This has allowed information sharing between FBI and DHS under ICE's Secure Communities program.[38]

And states are collecting and sharing biometric data with the federal government as well. At least 31 states have already started using some form of facial recognition with their DMV photos,[39] generally to stop fraud and identity theft, and the FBI has already worked with North Carolina, one of a handful of states reported to be in the NGI pilot program, to track criminals using the state's DMV records.[40] States also share fingerprints (and face prints soon) indirectly with DHS through Secure Communities. According to the FBI, NGI will allow all states to share and access face prints as easily as they now share and access fingerprints by 2014.[41]

The federal government also exchanges biometric data with foreign governments through direct and ad-hoc access to criminal and terrorist databases.[42] And ICE and the FBI share biometric data on deportees with the countries to which they are deported.[43]

[37] The National Institute for Standards and Technology (NIST), along with other standards setting bodies, has developed standards for the exchange of biometric data. See National Institute for Standards and Technology, ANSI/NIST-ITL 1-2011, *American National Standard for Information Systems: Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information* (2011), available at http://www.nist.gov/customcf/get_pdf.cfm?pub_id=910136.

[38] For more on Secure Communities, *see* Michele Waslin, *The Secure Communities Program: Unanswered Questions and Continuing Concerns*, Immigration Policy Center (Nov. 2011). Similarly, DHS is now sharing its data on asylum applicants more broadly with non-DHS agencies, per federal regulation 8 CFR §208.6(a). According to a June 30, 2011, Privacy Impact Assessment, DHS now shares the entire Refugees, Asylum and Parole Services (RAPS) database with the National Counter Terrorism Center (NCTC), a division of the Office of the Director of National Intelligence, under a Memorandum of Understanding (MOU). Dep't of Homeland Sec., *Privacy Impact Assessment Update for the Refugees, Asylum, and Parole System and the Asylum Pre-Screening System,* DHS/USCIS/PIA-027(a) (June 30, 2011), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_ raps_update_nctc.pdf. DHS has been sharing asylum data with the FBI since October 8, 2001, per an MOU signed by the agencies on that date. See USCIS Asylum Division, *Fact Sheet on Confidentiality*, 6 (June 15, 2005), available at http://www.usa-federal-forms.com/uscis-index-html/uscis-fact-sheet-on-confidentiality-uscis-5413.html.

[39] Thomas Frank, "Four states adopt 'no-smiles' policy for driver's licenses," *USA Today*, (May 26, 2009) http://www.usatoday.com/news/nation/2009-05-25-licenses_N.htm.

[40] Mike Baker, "FBI uses facial-recognition technology on DMV photos," *USA Today* (Oct. 13, 2009), http://www.usatoday.com/tech/news/2009-10-13-fbi-dmv-facial-recognition_N.htm. British Columbia attempted to use its DMV's face recognition database to identify people involved in the 2011 Stanley Cup riots, though this was later determined by B.C.'s Privacy Commissioner, Elizabeth Denham, to be a violation of Canada's privacy law. Jonathan Fowlie, "Court order required to use facial recognition to identify Stanley Cup rioters," *Vancouver Sun* (Feb. 17, 2012). http://www.vancouversun.com/business/Court+order+required+facial+recognition+identify+Stanley+rioters/6163995/story.html.

[41] *See* Kimberley Del Greco, "FBI Facial Services Program," FBI 5 (Sept. 29, 2011) *available at* http://www.biometrics.org/bc2011/presentations/DOJ/0929_1105_BrA_DelGreco.pdf.

[42] The FBI's Criminal Justice Information Service (CJIS) division has information-sharing relationships with 77 countries, and is working with several countries to allow real-time access to their respective biometrics databases. *See* FBI/CJIS Advisory Policy Board Identification Services Subcommittee, *Issue Paper: Biometrics Information Sharing Update* (Spring 2011), Bates No. SC-FBI-FPL-1088-89, available at http://uncoverthetruth.org/wp-content/uploads/S-Comm-Hot-Docs-Released-11-10-11.zip (download archive; unzip; open "SC-FBI-FPL-1081.pdf") (noting these relationships are "in the form of both informal

Private Sector Use of Facial Recognition Technologies[44]

Private sector use of facial recognition has expanded exponentially in the last few years as well. Facebook uses face recognition for each of its 900 million users.[45] Google offers face recognition to its 170 million Google+ users,[46] and Google and Apple both provide face recognition capabilities in their photo editing systems.[47] App developers offer face recognition to unlock a phone[48] or make tagging easier,[49] and software and hardware developers and manufacturers offer face recognition systems to identify users, and prevent unauthorized access to documents, computers and facilities.

Due to the large number of Facebook users and the fact that these users actively tag each other and themselves in photos, Facebook's face recognition system is the most robust and well-developed of all of these private sector products, and will likely become even more so with the recent purchase of Face.com. Facebook allows users to tag themselves in photos they upload and be tagged in others' photos. Facebook's "Tag Suggest" feature, introduced in December 2010, uses face recognition to automatically match uploaded photos to other photos a Facebook user is tagged in, grouping similar photos together and

(ad hoc, verbal) agreements and formal agreements (Memoranda of Agreement, Memoranda of Understanding, Letter of Cooperation).").

[43] *Id.* at SC-FBI-FPL-1089; DHS, "Privacy Impact Assessment for the Automated Biometric Identification System (IDENT)," 8 (July 31, 2006) available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf. This kind of biometrics sharing could prove disastrous for repatriated refugees or immigrants from countries with a history of ethnic cleansing.

[44] My testimony focuses on face recognition, rather than face detection. However, for an excellent discussion of face detection and digital signage, *see* Pam Dixon, "The One-Way-Mirror Society: Privacy Implications of the new Digital Signage Networks," *World Privacy Forum* (Jan 27, 2010) *available at*: www.ftc.gov/os/comments/privacyroundtable/544506-00112.pdf; *see also* Harley Geiger, "Seeing is ID'ing: Facial Recognition & Privacy," Center for Democracy & Technology (Decl 6, 2011) https://www.cdt.org/report/seeing-iding-facial-recognition-and-privacy.

[45] Facebook, "Newsroom: Key Facts: Statistics," http://newsroom.fb.com/content/default.aspx?NewsAreaId=22 (last visited July 10, 2012).

[46] The Google+ "Find My Face" feature is different from Facebook's facial recognition tools because, unlike Facebook, users must first opt-in to the system. Chester Wisniewski, "Facial recognition comes to Google+, but unlike Facebook it's opt-in," *Naked Security* (Dec. 9 2011) http://nakedsecurity.sophos.com/2011/12/09/google-introduces-facial-recognition-feature-opt-in-unlike-facebooks-effort/; Matt Steiner, "Making photo tagging easier with Find My Face," *Google*, https://plus.google.com/110260043240685719403/posts/jKQ35ajJ4EU.

[47] *See* Matt Hickey, "Picasa Refresh Brings Facial Recognition," *TechCrunch* (Sept. 2, 2008) http://techcrunch.com/2008/09/02/picasa-refresh-brings-facial-recognition/; Wilson Rothman, "What To Know About iPhoto '09 Face Detection and Recognition," *Gizmodo* (Jan. 29, 2009) http://gizmodo.com/5141741/what-to-know-about-iphoto-09-face-detection-and-recognition.

[48] Christina Bonnington, "FaceVault App Brings Facial Recognition Unlocking to iOS," *Wired Gadget Lab Blog* (April 25, 2012) http://www.wired.com/gadgetlab/2012/04/facevault-app-face-recognition/.

[49] Face.com developed an app called KLIK that allowed users to tag people in photographs before the photo was even taken. However, after Facebook bought Face.com, the app was removed from the Apple app store. *See* David Murphy, "Facebook Kills Face.com Face-Recognition APIs, KLIK app," *PC Magazine* (July 7, 2012) http://www.pcmag.com/article2/0,2817,2406822,00.asp.

suggesting the name of a user's friend in the photo.[50] Facebook markets this tool by stating it will make sorting, tagging and finding photos easier,[51] but it does not make clear that the feature will create a unique biometric—a faceprint—for all its users.

Facebook has stirred up significant controversy with its face recognition tools, in large part because it turned these features on by default. It first enrolled all its users in the system without prior consent and then continued to opt-in users every time they uploaded a photograph. Users may opt-out of tagging on a photo-by-photo basis, but opting out of the system as a whole is complicated. Given the steps necessary to delete the face print "summary" data associated with each user's account[52] and the fact that Facebook uses persuasive language to try to dissuade users from deleting the data completely,[53] it is unlikely most users would go this far. And even if a user deletes the summary data, it is unclear whether taking this step will prevent Facebook from continuing to collect biometric data going forward.[54] As a result of these policies, Facebook has amassed possibly the largest database of face prints in the world[55]—with face prints for about 1/7 of the world population[56]—and will continue to collect more and more face prints every day as more users join the site.

Facebook and other companies using facial recognition combine this data with sensitive and personal biographic data and information on users' networks and associations, exacerbating privacy concerns. Facebook requires each of its users to sign up under their

[50] Justin Mitchell, "Making Photo Tagging Easier," *The Facebook Blog* (Dec. 15, 2010), https://www.facebook.com/blog.php?post=467145887130.

[51] *Id.* (noting, "[n]ow if you upload pictures from your cousin's wedding, we'll group together pictures of the bride and suggest her name. Instead of typing her name 64 times, all you'll need to do is click 'Save' to tag all of your cousin's pictures at once.").

[52] *Id.* (noting users may turn off automatic tagging and remove tags added by others); *See also* Eva Galperin, "How to Disable Facebook's Facial Recognition Feature," *EFF* (June 9, 2011) www.eff.org/deeplinks/2011/06/how-disable-facebooks-facial-recognition-feature; Electronic Privacy Information Center (EPIC), "Complaint: In the Matter of Facebook, Inc, and the Facial Identification of Users," 12-15 (June 10, 2011) *available at* http://epic.org/privacy/facebook/EPIC_FB_FR_FTC_ Complaint_ 06_10_11.pdf.

[53] Facebook, "How Can I Turn Off Tag Suggestions?" https://www.facebook.com/help/?faq= 187272841323203#How-can-I-turn-off-tag-suggestions ("Before you opt out of using this feature, we encourage you to consider how tag suggestions benefit you and your friends. Our tagging tools . . . are meant to make it easier for you to share your memories and experiences with your friends.")

[54] *Id.* EPIC Complaint at 16.

[55] Facebook users uploaded more than 300 million photos every day in the three months ending on March 31, 2012. Facebook, *Key Facts: Statistics* (last visited July 9, 2012) http://newsroom.fb.com/content/ default.aspx?NewsAreaId=22. *See also* Facebook Photo Trends [INFOGRAPHIC], *PIXABLE* (Feb. 14, 2011) http://blog.pixable.com/2011/02/14/facebook-photo-trends-infographic/ (estimating that as of Summer 2011, users would have uploaded 100 billion photos to Facebook). Face.com, which developed face recognition tools for Facebook and was recently acquired the company, stated in March that it had indexed 31 billion face images. *See* Yaniv Taigman and Lior Wolf, "Leveraging Billions of Faces to Overcome Performance Barriers in Unconstrained Face Recognition," *Face.com*, http://face.com/research/faceR2011b.html (last visited Mar. 15, 2012).

[56] Facebook estimates it has 900 million users. Facebook, "Newsroom: Key Facts: Statistics," http://newsroom.fb.com/content/default.aspx? NewsAreaId=22 (last visited July 10, 2012). The world population is currently estimated at between six and seven billion people.

real names,[57] and then makes users' names, profile photos, gender and networks public by default.[58] Facebook is designed to promote social engagement, and as part of this users can and do provide extensive additional personal information, from email addresses and birthdates to partners' and family members' names, dating preferences, activities and interests, location information, and political and religious beliefs. Facebook also encourages users to communicate with each other through status updates, "likes," posts on other users' walls, and direct messages. Facebook then records all of this information as part of the user's profile, along with other less evident information, such as when users look at another person's profile; when they search for their friends; location, time and date information recorded in their photos; GPS information; and which device or computer they use to log into their account.[59] Through all of this, Facebook establishes associations between and among users and between users and the companies, organizations and causes they find relevant to their lives. All of this information is stored indefinitely by Facebook and, depending on a user's privacy settings, may be available beyond a user's friends or networks—even available to the public at large.

Some or all of this information may be shared with third parties such as other companies, app developers, and advertisers, depending on a user's privacy settings. In addition, the government regularly reviews and requests this data to verify citizenship applications,[60] for evidence in criminal cases,[61] and to look for threats to U.S. safety and security.[62]

[57] *See* Emil Protalinski, "Facebook has over 845 million users," *ZDNet* (Feb. 1, 2012), http://www.zdnet.com/blog/facebook/facebook-has-over-845-million-users/8332; Facebook "Statement of Rights and Responsibilities" (April 26, 2011), https://www.facebook.com/legal/terms ("Facebook users provide their real names and information . . . You will not provide any false personal information on Facebook[.]").

[58] Facebook, "Understand Your Internet Search Listing: Is my information visible to people who aren't logged into Facebook?" https://www.facebook.com/help/privacy/public-search-listings (last visited July 10, 2012).

[59] Facebook, "Information we receive and how it is used: Other information we receive about you," https://www.facebook.com/about/privacy/your-info#inforeceived (last visited July 10, 2012).

[60] *See* Jennifer Lynch, "Applying for Citizenship? U.S. Citizenship and Immigration Wants to Be Your 'Friend,'"*EFF* (Oct. 12, 2010), https://www.eff.org/deeplinks/2010/10/applying-citizenship-u-s-citizenship-and (describing how USCIS agents "friend" applicants for citizenship on social networking sites in order to monitor them).

[61] In warrant for Facebook data, the Department of Justice Criminal Division regularly requests all photos in which a user is tagged. *See* Jennifer Lynch, "DOJ Wants to Know Who's Rejecting Your Friend Requests," *EFF* (Jan. 24, 2012), https://www.eff.org/deeplinks/2012/01/doj-wants-know-who%E2%80%99s-rejecting-your-friend-requests.

[62] Jennifer Lynch, "New FOIA Documents Reveal DHS Social Media Monitoring During Obama Inauguration," *EFF* (Oct. 13, 2010), https://www.eff.org/deeplinks/2010/10/new-foia-documents-reveal-dhs-social-media; Jennifer Lynch, "Government Uses Social Networking Sites for More than Investigations," EFF.org (Aug. 16, 2010), https://www.eff.org/deeplinks/2010/08/government-monitors-much-more-social-networks. The FBI is currently looking for software to make its mining of social-media data more efficient and to allow it to map communities of interest. *See* Jim Giles, "FBI releases plans to monitor social networks," *New Scientist* (Jan. 25, 2012), http://www.newscientist.com/blogs/onepercent/2012/01/fbi-releases-plans-to-monitor.html.

As discussed in further detail below, few laws regulate private biometric collection on this scale. In general the public must rely on a company's privacy policies, terms of use, and user-managed privacy settings. However, as the public has seen with the extensive changes Facebook has made to its privacy settings and policies,[63] the fact that it implemented an opt-out based facial recognition system with little fanfare or explanation, and that the first facial recognition app developed to make tagging even easier (KLIK) was quickly hacked to allow access to private information in users' Facebook and Twitter accounts and automatically "recognize" anyone walking down the street,[64] industry self-regulation and consumer control are not enough to protect against critical privacy and security risks inherent in facial recognition data collection.

Concerns about Biometrics, Databases, and Data Sharing

The extensive collection and sharing of biometric data at the local, national, and international level should raise significant concerns among Americans. Data accumulation and sharing can be good for solving crimes across jurisdictions or borders, but can also perpetuate racial and ethnic profiling, social stigma, and inaccuracies throughout all systems and can allow for government tracking and surveillance on a level not before possible.

Some of these concerns are endemic to all data collection and are merely exacerbated by combining biographic data with any non-changeable biometric. For example, courts have recognized the "social stigma" involved with merely having a record in a criminal database.[65] Additionally, data inaccuracies—such those common in immigration[66] and

[63] *See* Matt McKeon, Infographic: "The Evolution of Privacy on Facebook," http://mattmckeon.com/facebook-privacy/ (last visited July 11, 2012).

[64] *See* http://ashkansoltani.org/docs/face_palm.html (describing how independent privacy and security researcher Ashkan Soltani hacked Face.com's KLIK app); *See also* Alessandro Acquisti, Face Recognition Study—FAQ, http://www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/; Will Oremus, "Facebooked in the Crowd," *Slate.com* (June 19, 2012) http://www.slate.com/blogs/future_tense /2012/06/19/facebook_buys_face_com_will_mobile_facial_recognition_kill_privacy_.html (describing Acquisti's research combining "off-the-shelf facial recognition software . . . with Facebook data and a computer algorithm to guess, not only people's names, but in some cases their social security numbers, based solely on snapshots taken with a webcam").

[65] *Menard v. Saxbe*, 498 F.2d 1017, 1024 (D.C. Cir. 1974) ("disabilities flowing from a record of arrest have been well documented: There is an undoubted 'social stigma' involved in an arrest record. It is common knowledge that a man with an arrest record is much more apt to be subject to police scrutiny -- the first to be questioned and the last to be eliminated as a subject in any investigation. . . . Most significant is its use in connection with subsequent inquiries on applications for employment and licenses to engage in certain fields of work. An arrest record often proves to be a substantial barrier to employment." Id. at 1024" (internal citations and footnotes omitted)).

[66] *See generally* Joan Friedland, National Immigration Law Center, *INS Data: The Track Record*, available at www.nilc.org/document.html?id=233 (citing multiple Government Accountability Office and Inspector General reports on inaccuracies in immigration records). These problems persist. *See generally, e.g,* U.S. Government Accountability Office (GAO), *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO-11-146 (Jan. 18, 2011), available at http://www.gao.gov/products/ GAO-11-146 (noting errors in USCIS's e-Verify system and difficulties in correcting those errors). This has happened with the Secure Communities program, where approximately 3,600 United States citizens have been caught up in the program due to incorrect immigration records. *See, e.g.*, Aarti Kohli, et al.

Automated Targeting System[67] records—become much more damaging and difficult to correct as they are perpetuated through cross-database sharing.

Data sharing can also mean that data collected for non-criminal purposes, such as immigration-related records or employment verification, are combined with and used for criminal or national-security purposes with little or no standards, oversight, or transparency. When some of this data comes from sources such as local fusion centers and private security guards in the form of Suspicious Activity Reports (SARs),[68] it can perpetuate racially or politically motivated targeting.[69]

Standardization of biometrics data (necessary to enable data sharing) causes additional concerns. Once data are standardized, they become much easier to use as linking identifiers, not just in interactions with the government but also across disparate databases and throughout society. For example, Social Security numbers were created to serve one purpose—to track wages for Social Security benefits—but are now used to identify a person for credit and background checks, insurance, to obtain food stamps and student loans, and for many other private and government purposes.[70] If biometrics become similarly standardized, they could replace Social Security numbers, and the next time someone applies for insurance, sees her doctor, or fills out an apartment rental application, she could be asked for her face print. This is problematic if records are ever compromised because, unlike a Social Security Number or other unique identifying number, a person cannot change her biometric data.[71] And the many recent security breaches and reports of falsified data show that the government and private sector can

Secure Communities by the Numbers: An Analysis of Demographics and Due Process, at p.4, Chief Justice Earl Warren Institute on Law and Social Policy, UC Berkeley School of Law (Oct. 2011), *available at* www.law.berkeley.edu/files/Secure_Communities_by_the_Numbers.pdf.

[67] The Automated Targeting System (ATS), which assigns everyone who crosses United States borders, a computer-generated 'risk assessment' score. Data collected by ATS is "stored for 15 years, even for individuals who have not been flagged as a threat or potential risk." *See* Shana Dines, "Interim Report on the Automated Targeting System: Documents Released through EFF's FOIA Efforts," *EFF.org* (Summer 2009), https://www.eff.org/pages/interim-report-autom. Under ATS, individuals have no way to access information about their "risk assessment" scores or to correct any false information about them. *See* "Lawsuit Demands Answers About Government's Secret 'Risk Assessment' Scores," *EFF* (Dec. 19, 2006), https://www.eff.org/press/archives/2006/12/19.

[68] *See, e.g.*, G.W. Schulz & Andrew Becker, "Finding Meaning In Suspicious Activity Reports," *NPR* (Sept. 7, 2011), http://www.npr.org/2011/09/07/140237086/finding-meaning-in-suspicious-activity-reports; ACLU, *More About Suspicious Activity Reporting* (June 29, 2010), http://www.aclu.org/spy-files/more-about-suspicious-activity-reporting.

[69] *See, e.g.*, Robert Smith, "Julia Shearson tells how a weekend trip to Canada became 5-year fight for rights," *The Plain Dealer* (June 4, 2011), available at http://blog.cleveland.com/metro/2011/06/julia_shearson_tells_how_a_wee.html (describing how Executive Director of the Cleveland Council on American-Islamic Relations (CAIR) ended up on an FBI terrorist watchlist and her struggle to correct inaccuracies in her government files).

[70] *See* "Legal requirements to provide your SSN," *Social Security Online*, http://ssa-custhelp.ssa.gov/app/answers/detail/a_id/78/~/legal-requirements-to-provide-your-ssn.

[71] Records could be compromised in several ways. For example, faceprints are stored as algorithms rather than images. These algorithms could be changed within the database such that when a person tries to use her biometric to identify herself, the database doesn't recognize her or thinks she's someone else.

never fully protect against these kinds of data losses.[72] Data standardization also increases the ability of government and the private sector to locate and track a given person throughout her life.

And finally, extensive data retention periods[73] can lead to further problems; data that may be less identifying today, such as a photograph of a large crowd or political protest, could become more identifiable in the future as technology improves.

However, advanced biometrics like face recognition create additional concerns because the data may be collected in public without a person's knowledge. For example, the addition of crowd and security camera photographs into NGI means that anyone could end up in the database—even if they're not involved in a crime—by just happening to be in the wrong place at the wrong time, by fitting a stereotype that some in society have decided is a threat, or by, for example, engaging in suspect activities such as political protest in areas rife with cameras.[74] Given the FBI's history of misuse of data gathered on people during former FBI director J. Edgar Hoover's tenure[75] and the years following September 11, 2001,[76]—data collection and misuse based on religious beliefs, race, ethnicity and political leanings—Americans have good reason to be concerned about expanding government biometrics databases to include face recognition technology.

Technical issues specific to facial recognition make its use worrisome for Americans. For example, facial recognition's accuracy is strongly dependent on consistent lighting

[72] *See, e.g.*, David Stout and Tom Zeller Jr., "Vast Data Cache About Veterans Is Stolen," *N.Y. Times* (May 23, 2006), available at https://www.nytimes.com/2006/05/23/washington/23identity.html; *see also* European Parliament News, *MEPs question Commission over problems with biometric passports* (Apr. 19, 2012) (noting that "In France 500,000 to 1 million of the 6.5 million biometric passports in circulation are estimated to be false, having been obtained on the basis of fraudulent documents.") *available at* http://www.europarl.europa.eu/news/en/headlines/content/20120413STO42897/html/MEPs-question-Commission-over-problems-with-biometric-passports. *See also* discussion of KLIK app hack and Alessandro Acquisti's work supra n. 64.

[73] Biometric records stored in IDENT are retained for 75 years or until the statute of limitations for all criminal violations has expired. DHS, *Privacy Impact Assessment (PIA) for the Automated Biometric Identification System (IDENT)* (Jul. 31, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf. Civil fingerprints stored in IAFIS are not destroyed until "the individual reaches 75 years of age," and criminal fingerprints are not destroyed until "the individual reaches 99 years of age." FBI, *Privacy Impact Assessment for the Fingerprint Identification Records System (FIRS) Integrated Automated Fingerprint Identification System (IAFIS) Outsourcing for Noncriminal Justice Purpose –Channeling* (May 5, 2008), http://www.fbi.gov/foia/privacy-impact-assessments/firs-iafis.

[74] For example, in Lower Manhattan, where the Occupy protests started, the New York Police Department has installed as many as 3,000 security cameras. *See* Noah Shachtman, "NYC Is Getting a New High-Tech Defense Perimeter. Let's Hope It Works," *Wired* (Apr. 21, 2008), http://www.wired.com/politics/security/magazine/16-05/ff_manhattansecurity.

[75] *See generally* Tim Weiner, *Enemies: A History of the FBI* (2012).

[76] *See, e.g.*, DOJ, Office of Inspector General (OIG), *A Review of the Federal Bureau of Investigation's Use of National Security Letters*, Special Report (March 2007); DOJ, OIG, *A Review of the FBI's Use of National Security Letters: Assessment of Corrective Actions and Examination of NSL Usage in 2006*, Special Report, (March 2008); DOJ, OIG, *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records* (January 2010).

conditions and angles of view.[77] It may be less accurate with certain ethnicities and with large age discrepancies (for example, if a person is compared against a photo taken of himself when he was ten years younger). These issues can lead to a high rate of false positives—when, for example, the system falsely identifies someone as the perpetrator of a crime or as having overstayed their visa. In a 2009 New York University report on facial recognition, the researchers noted that facial recognition "performs rather poorly in more complex attempts to identify individuals who do not voluntarily self-identify . . . Specifically, the "face in the crowd" scenario, in which a face is picked out from a crowd in an uncontrolled environment."[78] The researchers concluded the challenges in controlling face imaging conditions and the lack of variation in faces over large populations of people make it unlikely that an accurate face recognition system will become an "operational reality for the foreseeable future."[79]

Some have also suggested the false-positive risk inherent in large facial recognition databases could result in even greater racial profiling by disproportionately shifting the burden of identification onto certain ethnicities.[80] This can alter the traditional presumption of innocence in criminal cases by placing more of a burden on the defendant to show he is *not* who the system identifies him to be. And this is true even if a face recognition system such as NGI offers several results for a search instead of one, because each of the people identified could be brought in for questioning, even if he or she was not involved in the crime. In light of this, German Federal Data Protection Commissioner Peter Schaar has noted that false positives in facial recognition systems pose a large problem for democratic societies: "in the event of a genuine hunt, [they] render innocent people suspects for a time, create a need for justification on their part and make further checks by the authorities unavoidable."[81]

[77] Face recognition technologies perform well when all the photographs are taken with similar lighting and shot from a frontal perspective (like a mug shot). However, with different lighting, shadows, different backgrounds, different poses or expressions, or as a person ages, the error rates are significant. See, e.g., P. Jonathon Phillips, et al., "An Introduction to the Good, the Bad, & the Ugly Face Recognition: Challenge Problem," *National Institute of Standards & Testing* (Dec. 2011), available at www.nist.gov/itl/iad/ig/upload/05771424.pdf (noting only 15% accuracy for face image pairs that are "difficult to match"). Security researcher Bruce Schneier has noted that even a 90% accurate system "will sound a million false alarms for every real terrorist" and that it is "unlikely that terrorists will pose for crisp, clear photos." Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World,* 190 (2003).

[78] Lucas D. Introna & Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, p. 3, N.Y.U. (April 2009), available at http://www.nyu.edu/ccpr/pubs/Niss_04.08.09.pdf.

[79] *Id.* at 47. In layman's terms, this means that because so many people within a given population look alike, the probability that any facial recognition system will regularly misidentify people becomes much higher as the data set (the population of people you are checking against) gets larger.

[80] *Id.* at 45-46.

[81] *Id.* at 37.

Legal Protections for Privacy in Biometric Data

Face recognition implicates important Constitutional values, including privacy, free speech and association, and the right to be free from unlawful searches and seizures. If the government starts regularly collecting and indexing public photographs—or obtains similar data from private companies—this would have a chilling effect on Americans' willingness to engage in public debate and to associate with others who's values, religion or political views may be considered questionable. And yet the fact that face images can be captured without a detention and in public, or may be uploaded voluntarily to a third party such as Facebook, or may be collected and stored by private security firms and data aggregators, presents significant challenges in applying Constitutional protections.

The Fourth Amendment

The Fourth Amendment's prohibition of unreasonable searches and seizures presents a baseline protection for governmental biometrics collection in the United States.[82] Although there are significant exceptions to Fourth Amendment protections that may make it difficult to map to biometric collection such as facial recognition,[83] a recent Supreme Court case, *U.S. v. Jones*,[84] and a few other cases[85] show that courts are

[82] The Supreme Court has noted that the collection of biometrics like fingerprints has some Fourth Amendment protection, *see Davis v. Mississippi*, 394 U.S. 721, 723-24 (1969) (excluding from evidence fingerprints obtained during an illegal detention), however, the Court has declined to define the boundaries of that protection and suggested in dicta that because "[f]ingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search[,]" perhaps that protection is limited. *Id.* at 727. Courts have found greater protection in the collection of biological material that "can reveal a host of private medical facts about an [individual]," finding the collection "intrudes upon expectations of privacy that society has long recognized as reasonable." *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 617 (1989).

[83] For example, in each of the key Supreme Court cases to address collection of biometrics or biological material, the legal analysis hinged in large part on the detention required to obtain the biometric data or on "a meaningful interference with [one's] possessory interest in his bodily fluids." *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 618 n.4 (1989). However, biometrics such as face prints can be obtained without an initial detention and without the subject's knowledge while the subject is in a public place. Several cases have held that suspects have no legitimate expectation of privacy in biological material obtained under similar circumstances, *See* Erin Murphy, *The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence*, 95 Calif. L. Rev. 721, 736 n.63 and accompanying text (2007) (citing cases), or in discarded or abandoned material (such as garbage) or evidence in public view, making Fourth Amendment protection for face prints more tenuous. See, e.g., *California v. Greenwood*, 486 U.S. 35 (1988) (no reasonable expectation of privacy in garbage left on the street); *California v. Ciraolo*, 476 U.S. 207 (1986) (no expectation of privacy in backyard that can be viewed from a plane flying above); Elizabeth Joh, *Reclaiming "Abandoned" DNA: The Fourth Amendment and Genetic Privacy*, 100 Nw. U. L. Rev. 857, 863-64 (2006) (distinguishing cases where courts have found a "meaningful interference with an individual's possessory interests" from cases where "suspects 'knowingly expose' items to public view").

[84] 565 U.S. ____ (2012).

[85] *See, e.g.*, *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010) (holding email users have the same reasonable expectation of privacy in their stored email as they do in their phone calls and postal mail); *Montana State Fund v. Simms*, 270 P.3d 64 (Mont. 2012) (in concurring, two justices applied *US v. Jones*, finding the State Fund's "admitted practice of tracking, monitoring, and videotaping workers' compensation claimants as they go about their daily lives" implicated constitutional rights despite the fact that the videotaping occurred in public. The two justices further noted "Montanans do not reasonably expect that

concerned about mass collection of identifying information—even collection of information revealed to the public or a third party—and are trying to identify solutions.

Cases like *Jones* suggest support for the premise that although we may tacitly consent to someone noticing our face or our movements when we walk around in public, it is unreasonable to assume that consent extends to our data being collected and retained in a database, to be subject to repeated searches for the rest of our lives. This is buttressed by important privacy research showing that even though people voluntarily share a significant amount of information about themselves with others online, they still consider much of this information to be private in that they don't expect it to be shared outside of the networks they designate.[86]

In *United States v. Jones*,[87] nine justices held that a GPS device planted on a car without a warrant and used to track a suspect's movements constantly for 28 days violated the Fourth Amendment. For five of the justices, a person's expectation of privacy in not having his movements tracked constantly—even in public—was an important factor in determining the outcome of the case.[88]

Justice Sotomayor would have gone even further, questioning the continued validity of the third-party doctrine (holding that people lack a reasonable expectation of privacy in data such as bank records that they share with a third-party such as the bank).[89] She also recognized that:

> [a]wareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse.[90]

She questioned whether "people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[91]

state government, in its unfettered discretion and without a warrant, is recording and aggregating their everyday activities and public movements in a manner which enables the State to ascertain and catalog their political and religious beliefs, their sexual habits, and other private aspects of identity." *Id.* at 71).

[86] danah boyd, *The Future of Privacy: How Privacy Norms Can Inform Regulation*, Oct. 29, 2010, available at http://www.danah.org/papers/talks/2010/PrivacyGenerations.html

[87] 565 U.S. ____ (2012).

[88] *Id.* (slip op. at 2-3) (Sotomayor, J. concurring); *Id.* (slip op. at 9–12) (Alito, J., concurring).

[89] *See also United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010); *Montana State Fund v. Simms*, 270 P.3d 64 (Mont. 2012).

[90] *United States v. Jones*, 132 S. Ct. 945 (Sotomayor, J. concurring), 956; *see also NAACP v. Alabama*, 357 U.S. 449 (1958) (holding that requiring NAACP to disclose membership lists to the government would violate due process and a right to "associate freely with others").

[91] *Id.*

The fact that several members of the Court were willing to reexamine the reasonable expectation of privacy test[92] in light of newly intrusive technology could prove important for future legal challenges to biometrics collection. And some of the questions posed by the justices, both during oral argument and in their various opinions, could be used as models for establishing greater protections for data like facial recognition that is both shared with a third party such as Facebook and gathered in public.[93]

Other Laws May Provide Only Limited Protection to Face Recognition Data Collected by Government and the Private Sector

Privacy Act

The federal Privacy Act[94] "regulates the collection, maintenance, use, and dissemination of information about individuals by federal agencies . . . [and] authorizes civil suits by individuals . . . whose Privacy Act rights are infringed."[95] Although it applies to "personally identified information" collected by the government and gives citizens a way of gaining access to records and requesting their amendment, it has significant exceptions that minimize its effectiveness in actually protecting Americans' privacy rights. For example, it does not offer a remedy for "constitutional claims arising from alleged wrongs covered by the Privacy Act."[96] And law enforcement exemptions that allow agencies to shield criminal justice records from Privacy Act protections[97] make it unlikely it would offer any meaningful protections against face recognition data collection.

Stored Communications Act

The Stored Communications Act,[98] a law passed in 1986, would likely apply to protect face recognition-ready photographs and underlying face print data because it addresses voluntary and compelled disclosure of "stored wire and electronic communications and transactional records" held by or in storage with third-party service providers like

[92] See *Katz v. United States*, 389 U. S. 347, 361 (1967) (Harlan, J., concurring).

[93] Recently, privacy law scholars proposed several ways that Fourth Amendment doctrine could evolve in the wake of *Jones*. *See* www.usvjones.com. Susan Freiwald, who submitted the winning proposal, identified a four-factor test that incorporated factors the Supreme Court and appellate courts already identified. *See* Susan Freiwald, "The Four Factor Test," http://usvjones.com/2012/06/04/the-four-factor-test/ (noting that this four factor test "identifies when a surveillance method intrudes on Fourth Amendment rights and requires heightened judicial oversight to protect against abuse." These factors include whether the surveillance is *hidden* (the target is unaware of it), whether it is *intrusive* (offering access to "things people consider private"), *continuous*, and *indiscriminate* (gathering up "more information than necessary to establish guilt"). These factors could apply to restrict the collection of photographs taken from a hidden security camera that is always on and includes facial recognition.

[94] 5 U.S.C. §552a.

[95] *Jimenez v. Exec. Office for United States Attys.*, 764 F. Supp. 2d 174, 183 (D.D.C. 2011) (citing *Wilson v. Libby*, 535 F.3d 697, 707 (D.C. Cir. 2008)).

[96] *Id.* at 183.

[97] *See e.g.*, 28 C.F.R. § 16.81(a)(4) & (b)(3) (exempting from Privacy Act records maintained in US attorney criminal files).

[98] 18 U.S.C. §§ 2701–2712.

Facebook and Google.[99] However, because the definition of communications and content of communications was written to apply to more traditional oral or written communications,[100] it is unclear how the Act would map to the underlying face print data within a photograph, and whether the government would be required to obtain a warrant or some lesser legal process prior to requesting a copy of this data.[101]

FTC Act

The Federal Trade Commission Act[102] gives the FTC some power to investigate and seek relief for practices that are "unfair" and "deceptive."[103] A trade practice is unfair if it "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and is not outweighed by countervailing benefits to consumers or competition."[104] A trade practice is "deceptive" if it involves a "material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances, to the consumer's detriment."[105]

The FTC has settled several actions related to privacy in social media or web search that could show how the FTC might address an action related to collection of face recognition data.[106] However, FTC actions are limited, and, unlike court-developed law, the standards for determining whether a trade practice is unfair or deceptive area hazy. In addition, the FTC has so far failed to address the Electronic Privacy Information Center's complaint related to Facebook's face recognition program, despite the fact that it was filed over a year ago.[107] Further, commentators and media regularly recognize that the lack of universal privacy laws in the United States and the limited powers allotted to the FTC to regulate privacy issues, mean that companies have little incentive to change their practices.[108]

[99] *Id.* at §2703.

[100] *See* EFF, "Content of Communications," *EFF Internet Law Treatise*, https://ilt.eff.org/index.php/Privacy:_Data_Terminology# Content_of_Communications.

[101] For further discussion of the Stored Communications Act, *see* EFF, "Privacy: Stored Communications Act," *EFF Internet Law Treatise*, https://ilt.eff.org/index.php/Privacy:_Stored_Communications_Act.

[102] 15 U.S.C. §§ 41-58.

[103] *See* 15 U.S.C. § 45 (more commonly known as Section 5 of the FTCA) which declares "unfair or deceptive acts or practices in or affecting commerce" to be unlawful.

[104] 15 U.S.C. § 45(n).

[105] *See* Fed. Trade Comm'n, FTC Policy Statement on Deception, Letter from Fed. Trade Comm'n to Hon. John D. Dingell. Chairman, H. Comm. on Energy and Commerce (Oct. 14, 1983), http://www.ftc.gov/bcp/policystmt/addecept.htm ("Deception Statement").

[106] *See* Julianne Pepitone, "Facebook settles FTC charges over 2009 privacy breaches," *CNN.com* (Nov. 29, 2011) http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.htm; FTC, "FTC Gives Final Approval to Settlement with Google over Buzz Rollout" (Oct. 24, 2011) http://www.ftc.gov/opa/2011/10/buzz.shtm.

[107] *See* EPIC, "Complaint: In re Facebook and the Facial Identification of Users," (June 10, 2011) https://epic.org/privacy/facebook/facebook_and_facial_recognitio.html#complaint.

[108] *See, e.g.*, Ryan Singel, "FTC's $22M Privacy Settlement With Google Is Just Puppet Waving," *Wired Threat Level Blog* (July 10, 2012) http://www.wired.com/threatlevel/2012/07/ftc-google-fine/ (noting that even the FTC's proposed $22.5 million fine to Google for violating the Google Buzz consent decree did not prevent the company from combining all user data).

State Laws[109]

Three states—Illinois, Texas and Washington—have so far implemented laws that expressly apply to biometrics collection. While these laws have some holes, some of their protections could be used as models for federal legislation.

Illinois's law[110] applies to private entities and requires them to notify an individual in writing and obtain a written release before collecting the individual's biometric information, including "face geometry." Entities must disclose "purpose and length of term for which [the] biometric information is being collected, stored, and used," and may further not disclose a collected biometric without the individual's consent, unless the disclosure is required by law. Because this is a state law, it only applies to transactions in Illinois. However, as a state populated with almost 13 million people, Illinois residents could use this law to enforce changes that would likely affect the rest of the country. The law creates private right of action in encourage residents to pursue their own remedies against violations of the law, but with no agency designated to enforce compliance, it does not appear that the law has had much effect so far.

Texas' law[111] similarly regulates collection and use of biometric data, including "face geometry" & prohibits the collection of an individual's biometric data for a commercial purpose without first informing that individual and obtaining her consent. The law does not permit transfers of biometric data for any purpose other than: (1) to identify a deceased or missing individual if that individual previously consented to such identification; (2) for a transaction upon an individual's request or authorization; or (3) to disclose the data pursuant to a state or federal statute or for a law enforcement purpose pursuant to a warrant. Similar to the Illinois law, it creates private right of action for enforcement. It also allows the state Attorney General to bring an action for damages. However, it doesn't appear the Attorney General or any private citizen has yet brought an enforcement action under the law, despite the fact that a base-level reading of the statute would suggest it applies to Facebook's opt-out system.

Washington has had a law regulating biometric drivers' licenses since 2004,[112] which was recently updated to apply to face recognition.[113] The changes, which go into effect this summer, limit the purposes for which face recognition may be used,[114] set standards for

[109] Special thanks to EFF Intern Yana Welinder for help with this section on state laws. *See* Yana Welinder, *A Face Tells More than a Thousand Posts: Developing Face Recognition Privacy in Social Networks*, (working paper) (July 16, 2012) *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2109108.

[110] 740 Ill. Comp. Stat. 14/5.

[111] Tex. Bus. & Com. Code Ann. § 503.001.

[112] Chris Ingalls, "State shuts down successful crime-fighting tool," *King5.com* (Sept. 12, 2011) http://www.king5.com/news/investigators/Facial-recognition-program-shutdown--129663433.html.

[113] *See* Rev. Code. Wash. § 46.20.037 (revised by Substitute Senate Bill 6150, to take effect in 2012).

[114] *Id.* Sec. 1 ("Any facial recognition matching system selected by the department must be used only to verify the identity of an applicant for or holder of a driver's license to determine whether the person has been issued a driver's license, permit, or identicard under a different name or names.")

the accuracy of the system and security of the data,[115] provide for a notice requirement,[116] and clarify the legal process required for state and federal law enforcement to access the data.[117] The new version of the statute also includes a reporting requirement.[118] However, where the old version of the law created a voluntary biometrics system for licenses in Washington, the new version appears to remove this voluntariness language.

California may also be worth looking at when considering different protections for biometrics data, especially given how proposed biometrics bills have fared in the state legislature. California has no law specifically protecting biometrics but California's strong constitutional privacy rights,[119] which also apply against private companies, could offer some protections for abuse of those rights. Since 1998, the California legislature has introduced several bills that would directly regulate biometrics collection. However, due in part to industry pushback, none of these laws has moved out of the legislature. Most recently, Senate Bill 761, which would require a company that collects or uses "sensitive information," including biometric data, to allow users to opt-out of its collection, use, and storage, has faced stiff opposition from technology companies and their trade organizations.[120]

The lack of robust protections at the state level makes it even more important for the federal government to consider legislation to prevent improper biometrics collection and search.

Proposals for Change

The over-collection of biometrics has become a real concern, but there are still opportunities—both technological and legal—for change.

Given the current uncertainty of Fourth Amendment jurisprudence in the context of biometrics and the fact that biometrics capabilities are undergoing "dramatic technological change,"[121] legislative action could be a good solution to curb the over-collection and over-use of biometrics in society today and in the future. If so, the federal government's response to two seminal wiretapping cases in the late 60s could be used as

[115] *Id.* Sec. 2.

[116] *Id.* Sec. 3, 5 (notice "must address how the facial recognition matching system works, all ways in which the department may use results from the facial recognition matching system, how an investigation based on results from the facial recognition matching system would be conducted, and a person's right to appeal any determinations made under this chapter").

[117] *Id.* Sec. 4 (face recognition data "[m]ay only be disclosed [to state and local law enforcement] when authorized by a court order; [and m]ay only be disclosed to a federal government agency if specifically required under federal law").

[118] *Id.*

[119] Cal. Const. Art 1, sec. 1.

[120] *See* Opp'n Letter to Sen. Lowenthal (Apr. 27, 2011), *available at* http://static.arstechnica.com/oppositionletter.pdf.

[121] *Jones*, 565 U.S. ____, (slip op. at 13) (Alito, J., concurring).

a model.[122] In the wake of *Katz v. United States*[123] and *New York v. Berger*,[124] the federal government enacted the Wiretap Act,[125] which laid out specific rules that govern federal wiretapping, including the evidence necessary to obtain a wiretap order, limits on a wiretap's duration, reporting requirements, and a notice provision.[126] Since then, law enforcement's ability to wiretap a suspect's phone or electronic device has been governed primarily by statute rather than Constitutional case law.

Congress could also look to the Video Privacy Protection Act (VPPA),[127] enacted in 1988, which prohibits the "wrongful disclosure of video tape rental or sale records" or "similar audio-visual materials," requires a warrant before a video service provider may disclose personally identifiable information to law enforcement, and includes a civil remedies enforcement provision.

If legislation or regulations are proposed in the biometrics context, the following principles should be considered to protect privacy and security. These principles are based in part on key provisions of the Wiretap Act and VPPA and in part on the Fair Information Practice Principles (FIPPs), an internationally recognized set of privacy protecting principles.[128]

Limit the Collection of Biometrics—The collection of biometrics should be limited to the minimum necessary to achieve the government's stated purpose. For example, collecting more than one biometric from a given person is unnecessary in many situations. Similarly, the government's acquisition of biometrics from sources other than the individual to populate a database should be limited. For example, the government should not obtain biometrics en masse to populate its criminal databases from sources such as state DMV records, where the biometric was originally acquired for a non-criminal purpose, or from crowd photos or data collected by the private sector. Techniques should

[122] In Justice Alito's concurrence in *Jones*, he specifically referenced post-*Katz* wiretap laws and called out for legislative action, noting "[i]n circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative." *Id.* (slip op. at 11, 13) (Alito, J., concurring).

[123] 389 U.S. 347 (1967).

[124] 388 U.S. 41 (1967). *Berger* was unique in that it struck down a state wiretapping law as facially unconstitutional. In striking down the law, the Court laid out specific principles that would make a future wiretapping statute constitutional under the Fourth Amendment.

[125] 18 U. S. C. §§2510–2522.

[126] *See, e.g.*, Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 Mich. L. Rev. 801, 851-52 (2004).

[127] 18 U.S.C. § 2710.

[128] *See* Privacy Act of 1974, 5 U.S.C. § 552a (2010). *See also* Organization for Economic Co-operation and Development, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980) available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html. The full version of the FIPPs as used by DHS includes eight principles: Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing. *See* Hugo Teufel III, Chief Privacy Officer, DHS, Mem. No. 2008-01, Privacy Policy Guidance Memorandum (Dec. 29, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. *See also Fair Information Practice Principles*, FTC, http://www.ftc.gov/reports/privacy3/fairinfo.shtm (last modified June 25, 2007).

also be employed to avoid over-collection of face prints (such as from security cameras or crowd photos) by, for example, scrubbing the images of faces that are not central to an investigation.

Define Clear Rules on the Legal Process Required for Collection—Each type of biometric should be subject to clear rules on when it may be collected and which specific legal process—such as a warrant based on probable cause—is required prior to collection. Collection and retention should be specifically disallowed without legal process unless the collection falls under a few very limited and defined exceptions. For example, clear rules should be defined to govern when law enforcement or similar agencies may collect biometrics revealed to the public, such as a face print.

Limit the Amount and Type of Data Stored and Retained—For biometrics such as a face print that can reveal much more information about a person than his or her identity, rules should be set to limit the amount of data stored. Retention periods should be defined by statute and should be limited to no longer than necessary to achieve the goals of the program. Data that is deemed to be "safe" from a privacy perspective today could become highly identifying tomorrow. For example, a data set that includes crowd images could become much more identifying as technology improves. Similarly, data that was separate and siloed or unjoinable today might be easily joinable tomorrow. For this reason retention should be limited, and there should be clear and simple methods for a person to request removal of his or her biometric from the system if, for example, the person has been acquitted or is no longer under investigation.[129]

Limit the Combination of More than One Biometric in a Single Database—Different biometric data sources should be stored in separate databases. If biometrics need to be combined, that should happen on an ephemeral basis for a particular investigation. Similarly, biometric data should not be stored together with non-biometric contextual data that would increase the scope of a privacy invasion or the harm that would result if a data breach occurred. For example, combining facial recognition technology from public cameras with license plate information increases the potential for tracking and surveillance. This should be avoided or limited to specific individual investigations.

Define Clear Rules for Use and Sharing—Biometrics collected for one purpose should not be used for another purpose. For example, face prints collected for use in a criminal context should not automatically be used or shared with an agency to identify a person in an immigration context. Similarly, photos taken in a non-criminal context, such as for a driver's license, should not be shared with law enforcement without proper legal process. For private sector databases, users should be required to consent or opt-in to any face recognition system.

[129] For example, in *S. and Marper v. United Kingdom*, the European Court of Human Rights held that retaining cellular samples and DNA and fingerprint profiles of people acquitted or people who have had their charges dropped violated Article 8 of the European Convention on Human Rights. *S. and Marper. v. United Kingdom*, App. Nos. 30562/04 and 30566/04, 48 Eur. H.R. Rep. 50, 77, 86 (2009).

Enact Robust Security Procedures to Avoid Data Compromise—Because biometrics are immutable, data compromise is especially problematic. Using traditional security procedures, such as basic access controls that require strong passwords and exclude unauthorized users, as well as encrypting data transmitted throughout the system, is paramount. However security procedures specific to biometrics should also be enacted to protect the data. For example, data should be anonymized or stored separate from personal biographical information. Strategies should also be employed at the outset to counter data compromise after the fact and to prevent digital copies of biometrics. Biometric encryption[130] or "hashing" protocols that introduce controllable distortions into the biometric before matching can reduce the risk of problems later. The distortion parameters can easily be changed to make it technically difficult to recover the original privacy-sensitive data from the distorted data, should the data ever be breached or compromised.[131]

Mandate Notice Procedures—Because of the real risk that face prints will be collected without their knowledge, rules should define clear notice requirements to alert people to the fact that a face print has been collected. The notice provision should also make clear how long the biometric will be stored and how to request its removal from the database.

Define and Standardize Audit Trails and Accountability Throughout the System—All database transactions, including biometric input, access to and searches of the system, data transmission, etc. should be logged and recorded in a way that assures accountability. Privacy and security impact assessments, including independent certification of device design and accuracy, should be conducted regularly.

Ensure Independent Oversight—government entities that collect or use biometrics must be subject to meaningful oversight from an independent entity. Individuals whose biometrics are compromised, whether by the government or the private sector should have a strong and meaningful private right of action.

Conclusion

Face recognition and its accompanying privacy concerns are not going away. Given this, it is imperative that government act now to limit unnecessary biometrics collection; instill proper protections on data collection, transfer, and search; ensure accountability; mandate independent oversight; require appropriate legal process before government collection; and define clear rules for data sharing at all levels. This is important to preserve the democratic and constitutional values that are bedrock to American society.

Thank you once again for the invitation to testify today. I am happy to respond to your questions.

[130] *See, e.g.*, Information and Privacy Commissioner, Ontario, Canada, *Privacy-Protective Facial Recognition: Biometric Encryption—Proof of Concept* (Nov. 2010), available at www.ipc.on.ca/images/Resources/pbd-olg-facial-recog.pdf.

[131] *See, e.g.*, Center for Unified Biometrics and Sensors, "Cancellable Biometrics," SUNY Buffalo, http://www.cubs.buffalo.edu/cancellable.shtml (last visited Mar. 15, 2012).

OPENING STATEMENT OF CHAIRMAN FRANKEN "WHAT FACIAL RECOGNITION TECHNOLOGY MEANS FOR PRIVACY AND CIVIL LIBERTIES."

This hearing will be called to order. Welcome to the fourth hearing of the Subcommittee on Privacy, Technology and the Law. Today's hearing will examine the use of facial recognition technology by the government and the private sector — and what that means for our privacy and civil liberties.

I want to be clear: there is nothing inherently right or wrong with facial recognition technology. Just like any other new and powerful technology, it is a tool that can be used for great good. But if we do not stop and carefully consider the way we use this technology, it may also be abused in ways that could threaten basic aspects of our privacy and civil liberties. I called this hearing so we can start that conversation.

I believe that we have a fundamental right to control our private information--and biometric information is already among the most sensitive of our private information, mainly because it is both unique and permanent. You can change your password. You can get a new credit card. But you can't change your fingerprint, and you can't change your face. Unless I guess you go to a great deal of trouble.

Indeed, the dimensions of our faces are unique to each of us—just like our fingerprints. And just like fingerprint analysis, facial recognition technology allows others to identify you with what's called a "faceprint," a unique file describing your face.

But facial recognition creates acute privacy concerns that fingerprints do not. Once someone has your fingerprint, they can dust your house or your surroundings to figure out what you've touched.

Once someone has your faceprint, they can get your name, they can find your social networking account and they can find and track you in the street, in the stores you visit, the government buildings you enter, and the photos your friends post online. Your face is a conduit to an incredible amount of information about you. And facial recognition technology can allow others to access all of that information from a distance, without your knowledge and in about as much time as it takes to snap a photo.

People think of facial recognition as something out of a science fiction movie. In reality, facial recognition technology is in broad use today. If you have a drivers' license, if you have a passport, if you are a member of a social network, chances are good that you are part of a facial recognition database.

There are countless uses of this technology, and many of them are innovative and quite useful. The State Department uses facial recognition technology to identify and stop passport fraud—preventing people from getting multiple passports under different names. Using facial recognition technology, Sheriff Larry Amerson of Alabama, who is with us here today, can make sure that a prisoner being released from the Calhoun County jail is actually the same prisoner that is supposed to be released. Similarly, some of the latest smartphones can be unlocked by the owner by just looking at the phone and blinking.

But there are uses of this technology that should give us pause.
In 2010, Facebook, the world's largest social network, began signing up all of its then-800 million users in a program called Tag Suggestions. Tag Suggestions made it easier to tag close friends in photos. That's a good thing.

But the feature did this by creating a unique faceprint for every one of those friends. And in doing so, Facebook may have created the world's largest privately-held database of faceprints--without the explicit consent of its users. To date, Tag Suggestions is an opt-out program. Unless you have taken the time to turn it off, it may have already been used to generate your faceprint.

Separately, last year, the FBI rolled out a facial recognition pilot program in Maryland, Michigan and Hawaii that will soon expand to three more states. This pilot lets officers in the field take a photo of someone and compare it to a federal database of criminal mugshots. The pilot can also help ID a suspect in a photo from an actual crime. Already, several other states are setting up their own facial recognition systems independently of the FBI. These efforts will catch criminals: they already have.

Now many of you may be thinking that that's an excellent thing. I agree. But unless law enforcement facial recognition programs are deployed in a very careful manner, I fear that these gains could eventually come at a high cost to our civil liberties.

I fear that the FBI pilot could be abused to not only identify protesters at political events and rallies, but to target them for selective jailing and prosecution, stifling their First Amendment rights. Curiously enough, a lot of the presentations on this technology by the Department of Justice show it being used on people attending political events or other public gatherings.
I also fear that without further protections, facial recognition technology could be used on unsuspecting civilians innocent of any crime — invading their privacy and exposing them to potential false identifications.

Since 2010, the National Institute of Justice, which is a part of DOJ, has spent $1.4 million to develop facial recognition-enhanced binoculars that can be used to identify people at a distance and in crowds. It seems easy to envision facial recognition technology being used on innocent civilians when all an officer has to do is look at them through his binoculars.

But facial recognition technology has reached a point where it is not limited to law enforcement and multi-billion dollar companies: it can also be used by private citizens. Last year, Professor Alessandro Acquisti of Carnegie Mellon University, who is testifying today, used a consumer-grade digital camera and off-the-shelf facial recognition software to identify one out of three students walking across a campus.

I called this hearing to raise awareness about the fact that facial recognition already exists right here, today, and we need to think about what that means for our society. I also called this hearing to call attention to the fact that our federal privacy laws are almost totally unprepared to deal with this technology.

with the Department of Justice, the Council of State Governments, and philanthropic organizations to develop a set of consensus recommendations to improve discipline practice, reduce disproportionality, and dismantle the "school to prison pipeline."

At a minimum, we know that schools and communities should implement a multi-pronged, multi-disciplinary and comprehensive strategy to improve discipline practices that includes a deliberate and proactive effort to ensure that students are equitably treated. School discipline policies and practices, including those that govern school-based arrests and referrals to law enforcement, must also comply with federal civil rights laws prohibiting discrimination, including on the basis of race, color, national origin, disability, sex and religion.

The pieces of this strategy would encourage schools and communities to:

- Proactively monitor their discipline practices for disproportionality. This can mean instituting steps such as the following:

  - Collect and evaluate data regarding all referrals for student discipline, including those that did not result in disciplinary sanctions or referrals to law enforcement, consistent with the Family Educational Rights and Privacy Act's protections. Such a recordkeeping system should include demographic information for all students involved (race, sex, disability, age, and English-learner status), as well as a description of the misconduct, grade level of each student referred for discipline, description of attempts to address the behavior prior to referral for discipline, witnesses to the incident, prior history of the student, referring staff member, law enforcement involvement and discipline imposed.

- Assess for root causes where disproportionality exists. This can mean instituting steps such as the following:

  - Work with a consultant or other expert to review and modify disciplinary policies to ensure that rules are clearly defined and that students, staff and parents share a common understanding of the rules. School authorities should strive to reinforce positive student behavior and consider alternatives to expulsion and suspension that manage student misbehavior while keeping students in the classroom.

  - Establish a discipline review team to examine how discipline referrals and sanctions imposed at the school compare to those at other schools. Such a team can, for example, randomly review a percentage of the disciplinary actions taken at each school on an on-going basis to ensure the actions taken were non-discriminatory and consistent with the school's discipline practices.

  - Implement school climate surveys for students, parents, and school staff to measure their perceptions of school safety and fairness in discipline, as well as their understanding of disciplinary rules and behavioral expectations.

- Engage in a broad-based community and school effort to develop an action plan to root out discrimination in the administration of discipline. This can mean steps such as the following:

Questions for Witnesses from Senator Al Franken

In the end, though, I also think that Congress may need to act — and it wouldn't be the first time it did. In the era of J. Edgar Hoover, wiretaps were used freely with little regard to privacy. Under some Supreme Court precedents of that era, as long as the wiretapping device did not actually penetrate the person's home or property, it was deemed constitutionally sound — even without a warrant. And so in 1968, Congress passed the Wiretap Act. Thanks to that law, wiretaps are still used to stop violent and serious crimes. But police need a warrant before they get a wiretap. And you can't wiretap someone just because they're a few days late on their taxes — wiretaps can be used only for certain categories of serious crimes.

I think that we need to ask ourselves whether Congress is in a similar position today as it was 50 or 60 years ago—before passage of the Wiretap Act. I hope the witnesses today will help us consider this and all of the different questions raised by this technology. With that, I will turn to my friend and the Ranking Member, Senator COBURN.

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken
for Mr. Jerome Pender

1. **In 2009, the FBI used facial recognition technology to compare the photos of fugitives to the driver's license photos in the North Carolina DMV. I'm told that the FBI is looking to expand this program. What plans, if any, does the FBI have to expand its DMV pilot, and how will it protect against innocent citizens getting falsely accused as a result of false positives?**

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken
for Ms. Maneesha Mithal

1. **Is there currently anything in federal law that would require a company to get someone's consent before that company generates a faceprint for that person?**

2. **Both Facebook and Google are under either final or proposed settlement orders with the Commission that require those companies to protect their customers' data in particular ways. These orders also subject those companies to 20 years of Commission privacy audits.**

   Do these settlement orders cover these companies' use of facial recognition data like faceprints, and if so, how do they protect that data?

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken for Dr. Brian Martin

1. **What are the error rates for verification uses of facial recognition technology, and what are they for identification uses?**

2. **What happens to error rates—false negative and false positive rates—when you're working with photos of people who don't know they're being photographed?**

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken for Professor Alessandro Acquisti

1. **Your research showed that you could use off-the-shelf hardware and software to predict an incredible amount of information about someone you've never met before just by taking a photo of them. How hard and how expensive would it be for someone to commercialize your experiment—to basically create an app that lets people identify strangers?**

2. **Based on your different experiments, can you tell us what you can more or less predict about a stranger using off-the-shelf facial recognition technology?**

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken for Mr. Rob Sherman

1. **After it purchased Face.com, Facebook deleted all of the faceprint data that the company held. But Facebook has a database of faceprints of its own: Facebook has around 900 million users—close to a billion. How many users' facial templates (or "faceprints") does Facebook have?**

2. **Illinois and Texas state law requires that a company get a person's consent before generating a faceprint for him or her. You have millions users in each of those states. If Tag Suggestions is on by default—if it is an opt-out program—how are you complying with those laws?**

3. **Facebook recently bought Face.com. Does Facebook have any plans for producing a real-time facial recognition application, and if so, what precautions will the company take to make sure it can't be used to identify strangers?**

QUESTIONS AND ANSWERS

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken
for Ms. Jennifer Lynch

1. **I think it is really important to recognize that whatever the Supreme Court thinks about the Fourth Amendment, Congress is free to go above that and pass a law that does more to protect civil liberties. Can you explain how the Constitution really works as a floor, not a ceiling, when it comes to civil liberties?**

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

October 31, 2012

The Honorable Patrick J. Leahy
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Jerome Pender, Deputy Assistant Director, Criminal Justice Information Services Division, Federal Bureau of Investigation, before the Subcommittee on Privacy, Technology and the Law on July 18, 2012, at a hearing entitled "What Facial Recognition Technology Means for Privacy and Civil Liberties." We hope that this information is of assistance to the Committee.

Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

Judith C. Appelbaum
Acting Assistant Attorney General

Enclosure

cc: The Honorable Charles Grassley
Ranking Member

Questions for the Record
Jerome Pender
Deputy Assistant Director
Criminal Justice Information Services Division
Federal Bureau of Investigation

Subcommittee on Privacy, Technology and the Law
Committee on the Judiciary
United States Senate

"What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Question Posed by Senator Franken

In 2009, the FBI used facial recognition technology to compare the photos of fugitives to the driver's license photos in the North Carolina DMV. I'm told that the FBI is looking to expand this program. What plans, if any, does the FBI have to expand its DMV pilot, and how will it protect against innocent citizens getting falsely accused as a result of false positives?

Response:

"Project Facemask" was initiated in 2007 as a collaborative effort by the FBI and the North Carolina (NC) Department of Motor Vehicles (DMV) to use the NC DMV's facial recognition program as a means of locating fugitives and missing persons. This pilot received national attention in 2009 when the NC driver's license photograph of "Jose Luis Solis" was compared with a 1991 California booking photograph of double-homicide suspect Rodolfo Corrales. "Solis" was later confirmed to be Corrales, who was arrested in his NC home and extradited to California for prosecution. The project also resulted in the apprehension of six state fugitives and the resolution of one missing person case.

Upon the successful conclusion of the pilot in 2010, the capabilities were evaluated to assess the operational value of creating an FBI facial searching service. Based on this evaluation, the FBI created a Facial Analysis Comparison and Evaluation (FACE) Services Unit. The FACE Services Unit has begun establishing Memoranda of Understanding (MOUs) with the DMVs of states whose laws allow them to share DMV information for law enforcement purposes, as permitted by Federal law regarding the use of state motor vehicle records (18 U.S.C. §§ 2721-25). This process is being carried out in coordination with the Office of the General Counsel and the FBI's Records Management Division to ensure compliance with laws, regulations, and policies governing this kind of information.

The FACE team will compare the facial images of subjects of active FBI investigations with images housed in select FBI databases and other databases to which the FBI has access for law enforcement purposes. In addition, for states with which we have established MOUs, FBI fugitives' and subjects' identities will also be queried in the DMV records, with the results returned to the FACE team for comparison analysis.[1] The FACE team, consisting of personnel who have been specially trained in facial recognition comparisons, will identify any likely matches to the subject of the FBI investigation.

While the procedures will vary somewhat by state, typically the DMV will receive an inquiry from the FBI and will conduct an automated search of its image repository (in NC, for example, this search is conducted using a facial recognition algorithm). The DMV will provide image galleries to FACE Services Unit specialists, who will conduct manual comparisons in order to exclude unassociated persons and to identify any likely candidates. A blind verification ("double check") will then be conducted as part of the internal quality review process. If this confirms the original identification, the results of the manual comparison will be provided to the Special Agent working the open case with the caution that the information is to be used for lead purposes only. The case Agent will be responsible for further investigation to determine whether any possible matches are relevant to the investigation.

Communications with DMVs regarding facial recognition services will be conducted through a secure e-mail portal, and incoming and outgoing case work will be tracked and stored in an internal work log. This information will be retained for audit purposes. Access to the FACE Services Unit work log will be limited to that unit and to other authorized FBI personnel who need access to the log for audit or legal purposes. The FACE Services team is well aware of the need to conduct its activities in a manner that protects civil liberties. Therefore, in order to protect the civil liberties of innocent individuals, procedures have been developed to ensure that the FACE team appropriately disposes of any personally identifiable information (both hard copy and electronic) of individuals determined not to be candidate matches.

[1] Among other protections, all MOUs require that participating states protect privacy by: ensuring that the photos related to an FBI inquiry are not transmitted in internal or external state systems except through secure Law Enforcement Online transmissions; mandating the immediate, permanent, and appropriate destruction of these photos and related records once the inquiry is answered; and ensuring that states comply with their privacy laws and immediately report any unauthorized information dissemination or loss.

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken
for Ms. Maneesha Mithal

1. **Is there currently anything in federal law that would require a company to get someone's consent before that company generates a faceprint for that person?**

I am not aware of any federal laws currently in effect that specifically require a company to obtain an individual's consent before generating a faceprint for that individual. However, Section 5 of the Federal Trade Commission Act ("FTC Act") prohibits unfair or deceptive acts or practices. 15. U.S.C. § 45 *et seq.* In certain instances, a company's generation of an individual's faceprint without consent may be unfair or deceptive, such that the Federal Trade Commission ("FTC" or "Commission") could bring an action under the FTC Act. For example, if a company represents to consumers that it will not generate faceprints from the images that consumers provide to the company, and then subsequently begins generating faceprints from the previously provided images without obtaining the consent of those users, this may be deceptive under Section 5. If a company generates a faceprint in a way that causes or is likely to cause substantial injury that is not outweighed by countervailing benefits to consumers or to competition and is not reasonably avoidable by consumers, this would be an unfair practice under Section 5. We would examine these issues on a case-by-case basis.

2. **Both Facebook and Google are under either final or proposed settlement orders with the Commission that require those companies to protect their customers' data in particular ways. These orders also subject those companies to 20 years of Commission privacy audits.**

Do these settlement orders cover these companies' use of facial recognition data like faceprints, and if so, how do they protect that data?

Both the final order in the Google matter, as well as the proposed consent order in the Facebook matter, define the information covered by various provisions of the orders ("covered information") broadly. The Google order defines covered information as, "information respondent collects from or about an individual..." Similarly, the proposed Facebook consent order defines covered information as, "information from or about an individual consumer..." Because faceprints, as well as the consumer images they are derived from, are "from or about an individual" they fall under the definition of covered information in both orders.

The orders require the companies to protect covered information in a number of ways. For example, it would be a violation of both the Google order and the proposed Facebook order for the companies to misrepresent the extent to which they protect consumers' faceprints. Further, if either company were to have or launch a facial recognition feature without conducting a review to assess and address the privacy risks associated with that feature, this conduct would violate the provision of the orders that require the companies to implement a comprehensive privacy program.

Additionally, the proposed Facebook order requires that the company obtain users' affirmative express consent before sharing information that is restricted by a privacy setting with any third party in a way that materially exceeds that privacy setting. Thus, once the order is finalized, if Facebook did not obtain users' affirmative express consent before implementing a facial recognition feature that overrode users' privacy settings, this conduct would violate the order. A similar prohibition applies in the case of Google.

The FTC can obtain civil penalties of up to $16,000 per violation per day for violations of final orders.

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken
For Dr. Brian Martin

1. **What are the error rates for verification uses of facial recognition technology, and what are they for identification uses?**

This is a good question, the answer to which is not black and white. There are two error rates that one can make a tradeoff between by varying the match threshold of the system. By turning up the match threshold, you can reduce the **false positive** match rate (the chance of incorrectly saying two faces are the same person when they are not) and in exchange this would increase the **false negative** match rate (the probability that the algorithm fails to match two faces that were from the same person). Therefore, when we talk about error rates, we talk about both error rates simultaneously.

In quoting accuracy or the error rates of a technology, the value will depend strongly on the quality of the images and the strength of the algorithm. You can probably find experiments to support almost any result. Therefore, it is best to look at independently conducted, controlled tests. The National Institute of Standards and Technology (NIST) is arguably the best organization for ensuring independent non-biased faced recognition accuracy tests on sequestered data. In the 2010 NIST Interagency Report 7709, the stated **error rate for Verification is 4% false negative rate when you are operating at a threshold for 0.1% false positives** (Figure 12 in the report). This is based on FBI data; the accuracy can be better or worse depending on the quality of the face images. In real life, this would mean if you used this particular algorithm for face matching to unlock your phone, it would not let you unlock your phone about once in every 25 attempts (or would not work very well for 1 out of 25 people) since the false negative rate is 4%. At the same time it would let one of 1000 other people's faces unlock your phone since the false positive rate is 0.1%.

Identification error rates are more complex to nail down to a single set of values since the results depend on the number of faces in the database or gallery of faces. If the database has 1 person in it, then the error rate is the same as seen with Verification. If the database has 1,000,000 faces, there are 999,999 more chances to falsely match a face and get a false positive. A false positive in this sense means that out of 1,000,000 faces in the gallery, there was at least one false positive. To help separate the fact that this is a different measure, in identification we call it the **false positive <u>identification</u> rate** and the **false negative <u>identification</u> rate.** The false negative rate, however, does not necessarily increase with the larger database size since this rate depends on just a single image (the person it is supposed to match). In order to have a false positive identification rate of 0.1%, we would need to set our matching threshold to be much higher to discriminate against the 1,000,000 chances of a false positive. In fact, the match threshold needed to ensure a 0.1% false positive rate for identification of 1,000,000 faces will correspond to the Verification threshold of 0.0000001%. Setting the threshold this high, has the tradeoff that the false negative identification rate will increase as compared to the Verification scenario. From the 2010 NIST report, the false negative identification rate for the FBI data is roughly 25% at a corresponding 0.1% false positive identification rate for a database of 10,000 faces. If the database grows to 1,600,000 faces, the false negative identification rate is about 43% at 0.1% false positive identification rate. This is 10 times more false negatives (missed matches) than seen with Verification. Even with good quality data, the expected false negative rate would likely be on the order of 10% for a database of 1,000,000 good quality faces and still an order of magnitude or more worse than with Verification. To compensate for the higher error rates in Identification, a human is put in the loop to validate Identification results. With a human reviewing the top 10 best matches from every identification attempt, and ignoring the match threshold, face recognition can produce a 'hit' over 95% of the time (or inversely a 5% false missed hit rate) on a database of over 1,000,000 records. This investigative measure of accuracy (hit rate) shows that even though the error rate may be relatively high compared to Verification, face recognition is still a useful tool when combined with a human operator.

2. What happens to error rates—false negative and false positive rates—when you're working with photos of people who don't know they're being photographed?

For face recognition, as the quality of the face image deviates from the ideal image of a frontal looking face in good focus with good lighting, the accuracy will deteriorate. The extent of the drop in accuracy will depend on the capabilities of the face recognition algorithm (as it can be robust or trained to handle some of the issues). As an example, NIST presented at Biometrics 2010 in London a presentation "The limits of face recognition in law enforcement" where they showed Identification from a database of controlled quality images gave a 'hit rate' of 93% for a vendor, but when the images were less controlled and from a web cam the 'hit rate' dropped to 54%. They did not publish the false positive and false negative identification rates, but at a false positive identification rate of 0.1% I would estimate the false negative identification rate to be on the order of 60%. If the images are more uncontrolled, such as when taken far away when people do not know they are being photographed the error rates could be anywhere from 10% to 100% false negative identification rate – all depending on if they are caught looking at the camera, with good lighting and good focus.

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken
for Professor Alessandro Acquisti

1. **Your research showed that you could use off-the-shelf hardware and software to predict an incredible amount of information about someone you've never met before just by taking a photo of them. How hard and how expensive would it be for someone to commercialize your experiment—to basically create an app that lets people identify strangers?**

The costs and technical challenges of replicating our experimental results are, and will keep, falling. In fact, an application such as "Klik" (an app made available by Face.com before it was acquired by Facebook) supports the conclusions of our experiment, as it shows that real-time face recognition on mobile devices is already becoming a consumer product – notwithstanding the undeniable current limitations of these technologies.

One of the goals of our experiment was, in fact, to only use publicly available data and technologies that other third parties and end-users could also get access to: off-the-shelf face recognition technology,[i] limited computational power accessed through cloud computing services, and limited amounts of facial images made publicly available by end users on online social networks. In reality, today, both governmental and private sector entities have access to more powerful computational tools and much larger (and more accurate) repositories of digital photos than we had.

In other words, what we did can be replicated. Of course it would take time to re-create the procedure and mine the data necessary for face matching. Furthermore, the results we obtained are not yet scalable to the entire American population for a number of reasons: First, computational costs: we estimate that comparing the shot of a person's face to a database with mugshots of 280 million US residents aged 14 years or older, using the same hardware as in our experiments, would take over four hours (rather than the few seconds that process took in our experiments). Second, "false positives:" when comparing millions of human faces, several individuals' faces will be similar to each other, and computers do not yet excel in separating a face of a person from a face of someone who looks very much like that person. Third, light conditions, facial hair, or non-frontal poses impair the accuracy of machine face recognizers. Fourth, photographic images (and in particular frontal mugshots) may not be available for the entire population.

Those hurdles, however, are being progressively overcome. They are transient, not systemic. First, as computers' processing power increases, and cloud computing costs decrease, it will become more efficient to run end-user applications on mobile devices similar to the one we developed, for mass-scale, automated, peer-to-peer face recognition. Second, false positives will likely keep reducing, as machine face recognition error rates are decreasing by one half about every two years. Third, researchers are actively working on improving computers' ability to recognize faces under varied conditions of light, facial hair, and poses. Fourth, entities such as online social networks are amassing some of the largest known databases of identified photos, from which increasingly accurate biometric models or "faceprints" of increasing portions of the US population can be, and are being, built.

2. **Based on your different experiments, can you tell us what you can more or less predict about a stranger using off-the-shelf facial recognition technology?**

In our experiment (summarized at www.heinz.cmu.edu/~acquisti/face-recognition-study-FAQ/) we demonstrated how to predict individuals' Social Security numbers (SSNs) starting from their face. This is possible through a process of *data accretion*[ii] that involves a chain of inferences. The process itself, however, is not limited to the prediction of SSNs; hence, a priori, there is no specific limit to the amount of personal data which can be linked to (and therefore can be inferred from) a person's face. In other words, once someone develops the appropriate chain of inferences, that person may infer, for instance, a stranger's sexual orientation, credit score, or current address.

By this, I do not mean that all sensitive inferences will be equally possible or likely. I am also not implying that all these inferences are possible right now: the accuracy of the predictions depend on a large number of factors, including the amount of data publicly available and the accuracy of face recognizers. However, what I do mean is that the process itself is sufficiently universal to be applicable to a vast set of potentially sensitive inferences.

To explain, the process can be summarized in the following manner: First, face recognition links an unidentified subject (for instance, a face among many on the street) to a record in an identified database (such as an identified photo of the subject on Facebook, LinkedIn, Amazon, or in a state's DMV database). Once the link has been established, any online information associated with that record in the identified database (such as names and interests found in the subject's Facebook profile; or demographic data found on Spokeo.com - a social network and data aggregator) can in turn be probabilistically linked to the unidentified subject. Lastly, through data mining and statistical re-identification techniques, such online information can be used for additional, and much more sensitive inferences (such as sexual orientation,[iii] or Social Security numbers[iv]), which, in turn, can be linked back to the originally unidentified face. As I wrote in my testimony, sensitive data is therefore linked to an anonymous face through what we may refer to as a "transitive property" of (personal) information - a process that merely requires publicly available data. Sensitive information thus becomes "personally predictable" information.

This process (that we applied to SSNs) is generalizable for the following reason: In recent years, research in statistical re-identification and data mining has shown that you can predict sensitive data starting from non-sensitive information. While in 2009 we used dates of birth and states of birth to successful predict individuals SSNs, other researchers have identified medical conditions starting from demographic data, sexual orientation based on a Facebook users' network of friends, psychological profiles/psychiatric conditions based on their online social network profiles, credit scores based on someone's purchase history, and so forth. This is why I stated that, *in principle,* there is no ex ante barrier to what one can predict, starting from public data, since more and more individual data about individuals is being captured, and techniques for finding patterns in that data are getting more sophisticated.

Hence, a person's face becomes a veritable conduit between her different personas: it can link a person's online world (for instance, her social network presence) to her offline world (the person walking in the street). If an application can link a person's face to her name, and can link her name to public data about that person, then that application can also make sensitive inferences based on that data (as in the examples above, her SSN, your sexual orientation, or credit score) and link them back to the person's face.

[i] We used PittPatt, a face recognition application developed by former CMU researchers. Just a few days before our results were publicly presented, PittPatt was acquired by Google, thus the technology is no longer publicly available.

[ii] P. Ohm, 2010. "Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization." UCLA Law Review, 57, 1701.

[iii] C. Jernigan and B.F.T. Mistree, 2009. "Gaydar: Facebook friendships expose sexual orientation." First Monday,14(10).

[iv] A. Acquisti and R. Gross, 2009. "Predicting Social Security Numbers From Public Data." Proceedings Of The National Academy Of Science, 106(27), 10975-10980.

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken for Mr. Rob Sherman

1. **After it purchased Face.com, Facebook deleted all of the faceprint data that the company held. But Facebook has a database of faceprints of its own: Facebook has around 900 million users—close to a billion. How many users' facial templates (or "faceprints") does Facebook have?**

   Although we consider the specific number of facial recognition records, or "templates," that we store to be sensitive and proprietary information and do not disclose it outside of the company, we understand the importance of taking appropriate steps to help protect the security of this information. That is why we store templates in encrypted form and maintain them in a monitored and access-restricted database. We also have engineered our systems so that our facial recognition data is not interoperable with other systems and, therefore, would be of little use to anyone outside of Facebook. We provide our users with specific details about how our system works, as described below.

2. **Illinois and Texas state law requires that a company get a person's consent before generating a faceprint for him or her. You have millions users in each of those states. If Tag Suggestions is on by default—if it is an opt-out program—how are you complying with those laws?**

   We operate the Facebook service in compliance with all applicable laws, and our implementation of the tag suggestions feature does not conflict with the laws of either state identified in this question.

   At Facebook, we work hard to be clear about how we use information about people and how we obtain their consent. All of our users must specifically agree to our Terms and to have reviewed our Data Use Policy, which is presented to users when they sign up for Facebook accounts and is linked to throughout our website. With regard to our tag suggestions feature, the Data Use Policy states:

   > We are able to suggest that your friend tag you in a picture by scanning and comparing your friend's pictures to information we've put together from the other photos you've been tagged in. This allows us to make these suggestions. You can control whether we suggest that another user tag you in a photo using the "How Tags work" settings. Learn more at: https://www.facebook.com/help/tag-suggestions

This tag suggestions help page provides more information about how we use facial recognition technology to power tag suggestions. Specifically, it explains:

> We currently use facial recognition software that uses an algorithm to calculate a unique number ("template") based on someone's facial features, like the distance between the eyes, nose and ears. This template is based on photos you've been tagged in on Facebook. We use this template to suggest tags to you when you're adding a new photo to Facebook. Note that templates are only created for people on Facebook who've been tagged in a photo. If you un-tag yourself from a photo, that photo is not used to create the template. We also couldn't use a template to recreate an image of you.

The same page provides instructions on how users can easily opt out of participating in tag suggestions and indicates:

> When you turn off tag suggestions, Facebook won't suggest that friends tag you when photos look like you. The template that we created to enable the tag suggestions feature will also be deleted. Note that friends will still be able to tag photos of you manually.

3. Facebook recently bought Face.com. Does Facebook have any plans for producing a real-time facial recognition application, and if so, what precautions will the company take to make sure it can't be used to identify strangers?

Facebook's tag suggestions feature uses software to examine a photograph that a Facebook user provides to us and suggest which of a person's friends we believe may be in the photo, and whom that user might want to tag. This allows us to help streamline the process of tagging photos on Facebook. We do not have any current plans to expand our facial recognition application to one that identifies strangers in real time – our focus is on facilitating the tagging of photographs on Facebook.

Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
Hearing on "What Facial Recognition Technology Means for Privacy and Civil Liberties"
July 18, 2012

Questions for the Record from U.S. Senator Al Franken
for Ms. Jennifer Lynch

1. **I think it is really important to recognize that whatever the Supreme Court thinks about the Fourth Amendment, Congress is free to go above that and pass a law that does more to protect civil liberties. Can you explain how the Constitution really works as a floor, not a ceiling, when it comes to civil liberties?**

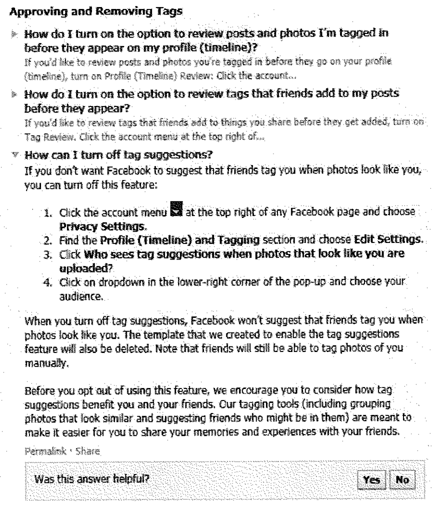
Response from Jennifer Lynch:

It is a well-recognized legal premise that Congress can legislate privacy and civil liberties protections beyond those explicit in the text of the Constitution. This ensures that the Constitution works as a floor and not a ceiling.

Two examples demonstrate this premise. First, in *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), the Supreme Court held that the First and Fourth Amendments provided no special protection against the search and seizure of materials in the possession of the press. In so doing, the Court noted, "Of course, the Fourth Amendment does not prevent or advise against legislative or executive efforts to establish nonconstitutional protections against possible abuses of the search warrant procedure[.]" *Id.* at 567. In response, Congress passed the Privacy Protection Act, 42 U.S.C. §2000aa *et seq*, protecting holders of pre-publication material from searches and seizures as well as mandating the development of internal federal guidelines designed to minimize the invasiveness of other types of third party searches. *See* S. Rep. No. 96-874, at 4-5 (1980), reprinted in 1980 U.S.C.C.A.N. 3950, 3951. In passing the legislation, Congress recognized that the Supreme Court had "issued an open invitation to Congress to draw statutory lines where the Constitution did not apply[,]" S. Rep. No. 96-874, at 5, noting "this legislation was prompted by *Zurcher v. Stanford Daily* . . . [which] held that the Fourth Amendment does not confer any special protections against search and seizure for the possessor of documentary evidence who is not himself a suspect in the offense under investigation." *Id.* at 4. The Privacy Protection Act increased journalists' protection against governmental searches by providing a new statutory private right of action for damages for conduct that violates the Act. 42 U.S.C. § 2000aa-6(a).

Second, Congress passed the Wiretap Act, 18 USC § 2510 *et seq*., in direct response to the Supreme Court's decisions in *Katz v. United States*, 389 U.S. 347 (1967), and *New York v. Berger*, 388 U.S. 41 (1967), both of which discussed Fourth Amendment limitations on law enforcement recording of and eavesdropping on communications. The Wiretap Act incorporated the *Berger* opinion's proposed limitations on wiretaps, *see Berger*, 388 U.S. at 59-60, and laid out specific rules that govern wiretapping, including the evidence necessary to obtain a wiretap order, limits on a wiretap's duration, reporting requirements, and a notice provision. *See, e.g.,* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution,* 102 Mich. L. Rev. 801, 851-52 (2004). Since the law was passed, a person's privacy rights in his communications on phones and electronic devices (and law enforcement's ability to listen in on and wiretap those communications) have been governed primarily by statute rather than case law and the Constitution. *Id.* at 850.

Miscellaneous Submissions for the Record



Approving and Removing Tags

- **How do I turn on the option to review posts and photos I'm tagged in before they appear on my profile (timeline)?**
  If you'd like to review posts and photos you're tagged in before they go on your profile (timeline), turn on Profile (Timeline) Review: Click the account...
- **How do I turn on the option to review tags that friends add to my posts before they appear?**
  If you'd like to review tags that friends add to things you share before they get added, turn on Tag Review. Click the account menu at the top right of...
- **How can I turn off tag suggestions?**
  If you don't want Facebook to suggest that friends tag you when photos look like you, you can turn off this feature:

1. Click the account menu ▾ at the top right of any Facebook page and choose **Privacy Settings**.
2. Find the **Profile (Timeline) and Tagging** section and choose **Edit Settings**.
3. Click **Who sees tag suggestions when photos that look like you are uploaded?**
4. Click on dropdown in the lower-right corner of the pop-up and choose your audience.

When you turn off tag suggestions, Facebook won't suggest that friends tag you when photos look like you. The template that we created to enable the tag suggestions feature will also be deleted. Note that friends will still be able to tag photos of you manually.

Before you opt out of using this feature, we encourage you to consider how tag suggestions benefit you and your friends. Our tagging tools (including grouping photos that look similar and suggesting friends who might be in them) are meant to make it easier for you to share your memories and experiences with your friends.

Detroit, Michigan, Code of Ordinances >> Part III - CITY CODE >> Chapter 50 - STREETS, SIDEWALKS AND OTHER PUBLIC PLACES >> ARTICLE II. - OBSTRUCTIONS AND ENCROACHMENTS >> DIVISION 1. - GENERALLY >>

DIVISION 1. - GENERALLY

Sec. 50-2-1. - Prohibited generally; violations and penalties; presumptions concerning identity of violator; enforcement; exceptions.

(a) No person shall obstruct or encumber any public wharf, street, alley or any public place with animals, boxes, signs, barrels, posts, fences, buildings, dirt, stones, bricks, rubbish or with any other material or thing whatsoever, except as otherwise provided in this Code, or encroach upon or permit to remain or maintain in any such street, alley or public space, any building, structure or thing owned, occupied or used by him or her, provided, that the department of public works, city engineering division may grant permission for a temporary obstruction of a sidewalk in front of business buildings for the purpose of elevating and receiving heavy merchandise, further provided, that the same shall not be piled over six (6) feet high, and the owner shall be responsible for any damage from such use of the walk. Power to revoke such permission at any time shall be expressly reserved to the department.

(b) With respect to any advertisement, sign, or other obstruction or encumbrance that violates any provision of this section, a rebuttable presumption exists that the advertisement, sign, or other obstruction or encumbrance was erected, placed or displayed at its location by, or with the consent of, the promoter of the event, offer, or service that is the subject of the advertisement, sign, or other obstruction or encumbrance.

(d) It shall be unlawful for any person to violate any provision of this section, or to aid and abet another to violate such provisions.

(e) Any person who violates this section may be issued a violation for each day that the violation continues.

(f) Any person who is found guilty of violating this section shall be convicted of a misdemeanor for each violation that is issued, and, in the discretion of the court, may be fined up to five hundred dollars ($500.00) and sentenced up to ninety (90) days in jail, or both, for each violation that is issued.

(g) This section shall be enforced by the police department.

(h)

This section shall not be construed to prohibit merchants and other business persons from using and occupying, for a width of three (3) feet, the inside of the sidewalk space next to the building or lot line immediately in front of their place of business in all streets whereon the sidewalk space is ten (10) or more feet in width, where such use and occupation will not obstruct public travel, for the purpose of receiving and shipping their goods, wares and merchandise, during the hours between sunrise and sunset.

(i) The department of public works city engineering division may permit merchants or other occupants of the buildings located on the south side of the Fisher Freeway Service Drive, between Russell Street and Riopelle Street; on the west side of Russell Street from the Fisher Freeway Service Drive to the alley north of and parallel with Adelaide Street, and on the east side of Market Street from the Fisher Freeway Service Drive to Winder Street, to use and occupy, where such use and occupation will not obstruct public travel, all of the space of eight (8) feet in width, outside of a line three (3) feet distant from the lot line, for the purpose of receiving and shipping their goods, wares, products and merchandise, or for displaying their goods, wares, products and merchandise used for exhibiting and advertising their business between the hours of sunrise and 11:00 a.m.

(j) This section shall not be construed to prevent the moving of goods, wares and merchandise across any sidewalk in the way of trade or for the use of pedestrians.

(k) This section shall not be construed as giving authority to any owner or occupant of any premises to let, sub-let, rent, lease or grant, free use to any person whatsoever any of the sidewalk space (meaning the space between the lot line of the property and the curbstone or any space outside of the lot line, on, above, or below ground) for business stands of any kind or for any purpose whatsoever. Any person so found doing business in such space may be summarily removed by the police department and shall be deemed in violation of this section.

(Code 1964, § 58-2-1; Ord. No. 13-07, § 1, 5-9-07)

Sec. 50-2-2. - Projecting structures prohibited.

Nothing in the way of a structure or framework, covered or uncovered, of even a quasi-permanent character, attached to the front or in front of any building, shall be permitted to be constructed or maintained so as to extend into the street beyond any lot line. Any such item constructed shall be removed within twenty-four (24) hours after notice from the environmental protection and maintenance department to the owner or occupant of the building to remove the same, failing obedience to which notice the department may summarily remove the same and may also enter complaint in the recorder's court against both owner and the occupant for violation of this section.

(Code 1964, § 58-2-2)

Sec. 50-2-3. - Sidewalk telephone booths.

The city council may, by resolution, authorize the environmental protection and maintenance department to issue a permit for the installation of outdoor commercial telephone booths on that portion of the highway located between the property lot lines and the curb, subject to a finding by the community and economic development department that such use will not be injurious to the adjacent or contiguous properties, and also subject to a finding by the department of transportation that the location thereof will not imperil the public safety. A building permit shall be secured from the department of buildings and safety engineering. Before any such permit is issued by the community and economic development department, the petition shall file a surety bond, with form approved by the corporation counsel, in the penal sum of not less than five thousand dollars ($5,000.00), saving and protecting the city harmless from any claims, damages or expenses that may arise by reason of the issuance of such permit and the occupancy of the property thereunder. Any permit issued under this section is revocable at the will, whim and caprice of the city council, and the permittee shall, as a condition of the permit, shall waive any right to claim damages against the city for the removal of such installation. The city council may include additional conditions and limitations it finds necessary to protect the interests of the city.

(Code 1964, § 58-2-3)

Sec. 50-2-4. - Flag poles.

(a) The city council may, by resolution, authorize the environmental protection and maintenance department to issue a permit for the temporary installation and maintenance of flag staffs or flag poles for the display of the American Flag only on the marginal area of the street, upon petition of the owner or lessee of the abutting property.

(b) Such request shall be made by petition to the city council, and such petition shall have attached to it a survey of plan drawn to scale showing the proposed installation. The petition shall be referred to the environmental protection and maintenance department and the department of building and safety engineering for report and recommendation as to whether such use of the street will create a material hazard to the public, and whether the provision for closing the hole or openings for the flag staffs or flag poles is sufficient to protect the public from injury.

(c) Upon receipt of the aforesaid reports, the city council may, by resolution, authorize the environmental protection and maintenance department to issue permits for the installation and maintenance of the flag staffs or flag poles for displaying the American Flag only, on condition that petitioner file a corporate surety bond in the amount of not less than two thousand dollars ($2,000.00), to be approved by the office of the corporation counsel, conditioned on his faithful performance of the terms of this article and that the permittee will indemnify the city against all actions or claims of any kind whatsoever made by any person for injury to person or property by reason of the issuance of the permit for the installation or maintenance of the flag staffs or flag poles, and that the permittee will assume full liability and that he will pay for the removal and restoration of the marginal area when ordered to do so. Such permission is given at the will and caprice of the city council.

(Code 1964, § 58-2-4)

Sec. 50-2-5. - Fences, signs and other approved obstructions.

(a) The city council may, by resolution, authorize the environmental protection and maintenance department to issue a permit for the installation of fences, signs or any other approved obstruction by the owner of private property on city property between the established line of sidewalk and the property line adjacent thereto.

(b) The owner of such private land shall attach to his petition to the city council a plan or survey, explaining in detail his proposed use of the city land, and an agreement that the petitioner will keep the city property in a neat and orderly condition at all times; that he agrees to make and execute an agreement saving and protecting the city from any claims, damages or expenses that may arise by reason of the issuance of a permit and the permitted occupancy of the property thereunder; that he confesses judgment on any claims, damages or expenses thereunder; that he agrees to remove, at his own expense, any fences, signs or other approved obstruction erected under this section when so notified to do so. If such obstruction is not removed when the permittee is notified for its removal, the environmental protection and maintenance department is hereby authorized and directed to remove such obstruction and to assess the cost of such removal against the adjoining property of the permittee.

(c) Any permit issued under this section is revocable at the will, whim, and caprice of the city council. The permittee under this section shall, as a condition of the permit, waive any right to claim damages against the city for the removal of such installation. The city council may include additional conditions and limitation it finds necessary to protect the interests of the city.

(d) The city council shall take no action relative to issuing a permit under this section until an investigation and report is received from the environmental protection and maintenance department and a report from the department of buildings and safety engineering that such installation will not be in violation of any other provision of this Code or other city ordinance or of the zoning ordinance of the city. The permit shall be issued by the director of the environmental protection and maintenance department when so authorized by the city council.

(Code 1964, § 58-2-5)

Sec. 50-2-6. - Notice to remove obstructions; environmental protection and maintenance department authorized to remove obstructions.

(a) In all cases of violation of the provisions of this division, the owner or occupant of the building or premises shall remove such obstructions within twenty-four (24) hours after notice to do so from the environmental protection and maintenance department, and if the owner shall fail to remove the same, such removal shall be forthwith effected by the environmental protection and maintenance department.

(b) The notices to be given by the environmental protection and maintenance department, as provided by this section, shall be served upon the owner or occupant of such obstruction or the adjoining premises. If they cannot be found, it shall be securely posted in some conspicuous place on such premises or abutting building. A compliance with such notice or the removal of the obstruction by the environmental protection and maintenance department shall not operate as a suspension of the penalties provided in section 1-1-9

(Code 1964, § 58-2-6)

Sec. 50-2-7. - Disposition of removed property.

(a) All goods enumerated in sections 50-2-1 and 50-2-2, which have been removed by the environmental protection and maintenance department, as provided in section 50-2-6 shall be considered abandoned thirty (30) days after such removal or posting of the notice provided for in section 50-2-6. Upon the removal of such goods, material or property by the environmental protection and maintenance department from the street, sidewalk or other public property, an inventory of such goods shall be made and signed by a representative of the environmental protection and maintenance department and a representative of the police department from the precinct wherein the property is located. A copy of such inventory shall be held by the environmental protection and maintenance department, and a copy shall be held by the police department for a period of six (6) years from the date of such removal.

(b) Where an owner shall appear to claim such goods, he shall pay the cost of removal and a reasonable storage charge. Such charges shall be paid within ten (10) days after such claim is filed with the environmental protection and maintenance department. Where no person appears to reclaim such property or material, the environmental protection and maintenance department shall endeavor to secure bids for the sale of such property, and, in the failure thereof, shall be empowered to sell or dispose of such goods.

(Code 1964, § 58-2-7)

Secs. 50-2-8—50-2-18. - Reserved.

July 18, 2012

The Honorable Al Franken
Chairman, Subcommittee on Privacy, Technology, and the Law
United States Senate Committee on the Judiciary
Washington, D.C. 20519

Re: "What Facial Recognition Technology Means for Privacy and Civil Liberties"

Dear Chairman Franken:

Thank you for your invitation to submit this statement for the record for the hearing "What Facial Recognition Technology Means for Privacy and Civil Liberties." The Electronic Privacy Information Center ("EPIC") would like to bring to your attention comments submitted to the Federal Trade Commission ("FTC") regarding commercial facial recognition technology.

EPIC's comments discussed issues raised at an FTC workshop on facial recognition. EPIC explained that facial recognition threatens the ability of individuals to control the disclosure of their identity. Some companies have adopted techniques that are more favorable to privacy, as they allow users to control the image database, while others undermine privacy, as the image database is centrally maintained. Ultimately, EPIC recommended the suspension of facial recognition technology deployment until adequate safeguards and privacy standards are established.

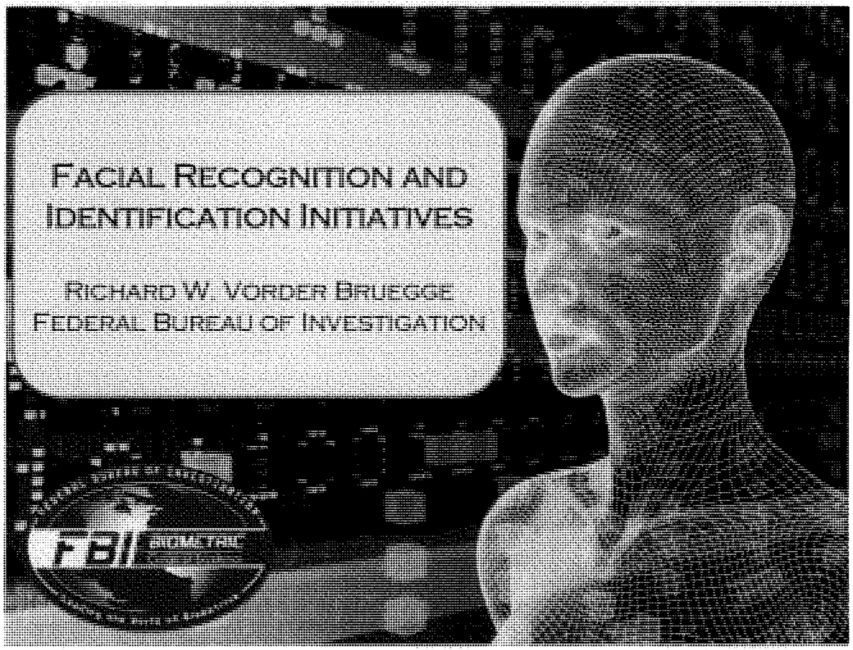
EPIC thanks you and members of the Subcommittee for your attention to this important issue. As facial recognition technology becomes more sophisticated and widely-used, the measures taken to preserve privacy will grow in importance. Your decision to hold this hearing will help protect important American rights.

Sincerely,

/s/
Marc Rotenberg, Executive Director
Electronic Privacy Information Center (EPIC)

/s/
Ginger P. McCall, Director, Open Government Program
Electronic Privacy Information Center (EPIC)

/s/
David Jacobs, Consumer Protection Fellow
Electronic Privacy Information Center (EPIC)



Facial Recognition and Identification Initiatives

Richard W. Vorder Bruegge
Federal Bureau of Investigation

FBI
BIOMETRIC

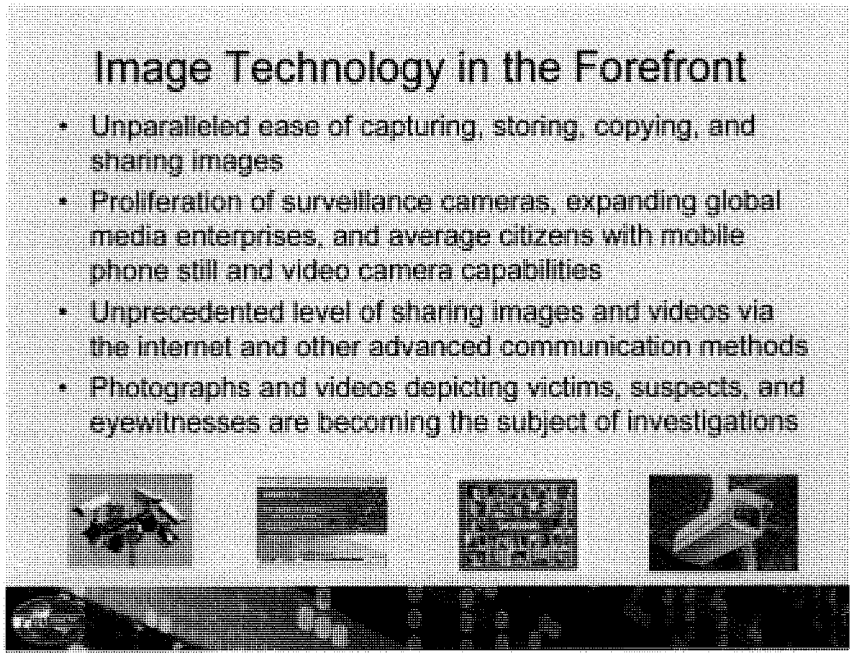
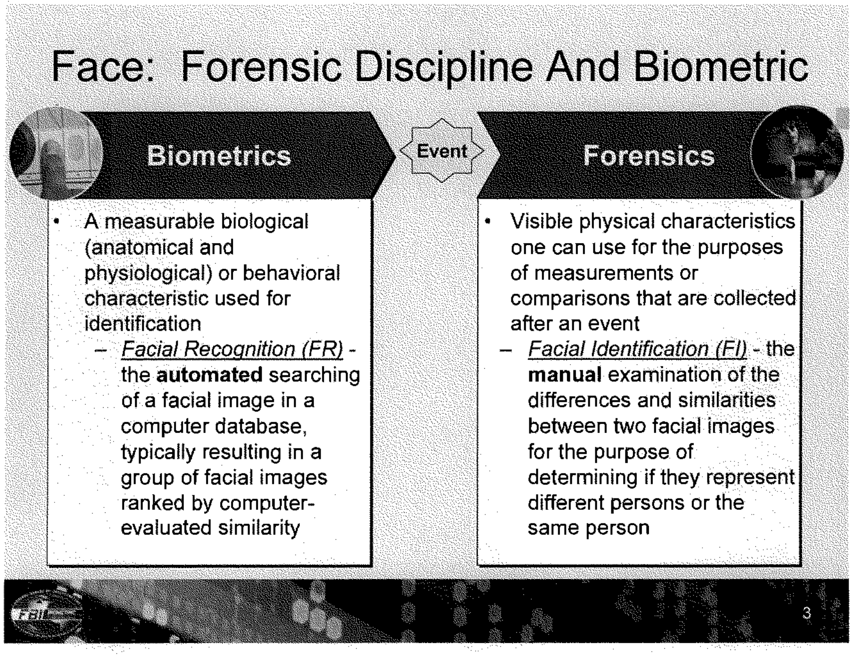


Image Technology in the Forefront

- Unparalleled ease of capturing, storing, copying, and sharing images
- Proliferation of surveillance cameras, expanding global media enterprises, and average citizens with mobile phone still and video camera capabilities
- Unprecedented level of sharing images and videos via the internet and other advanced communication methods
- Photographs and videos depicting victims, suspects, and eyewitnesses are becoming the subject of investigations



Face: Forensic Discipline And Biometric

Biometrics

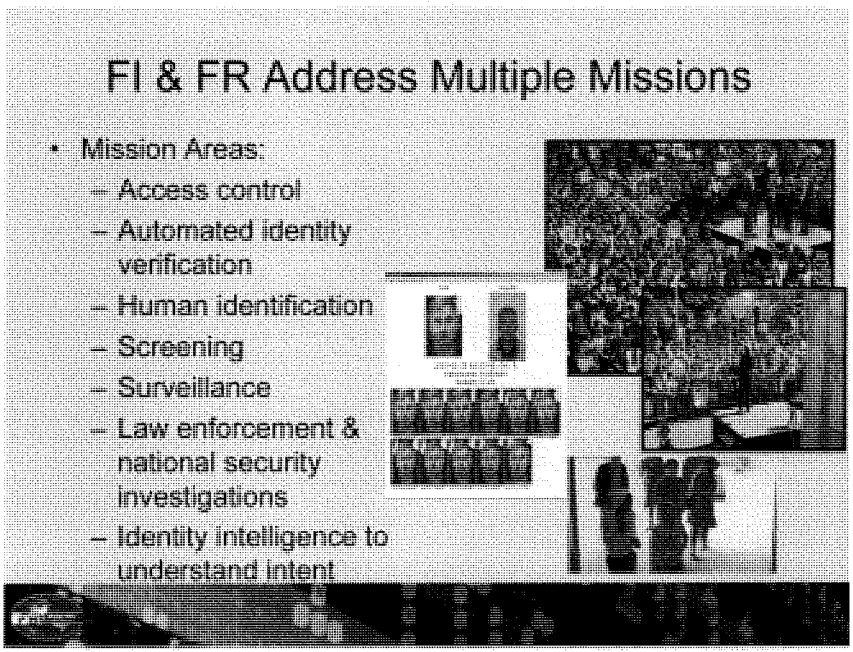
- A measurable biological (anatomical and physiological) or behavioral characteristic used for identification
  - *Facial Recognition (FR)* - the **automated** searching of a facial image in a computer database, typically resulting in a group of facial images ranked by computer-evaluated similarity

Event

Forensics

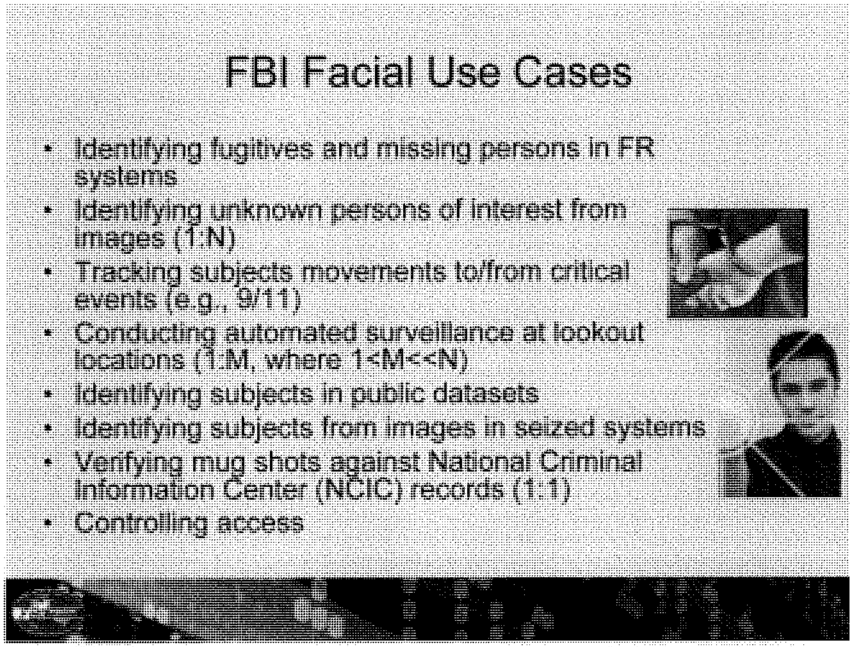
- Visible physical characteristics one can use for the purposes of measurements or comparisons that are collected after an event
  - *Facial Identification (FI)* - the **manual** examination of the differences and similarities between two facial images for the purpose of determining if they represent different persons or the same person

3



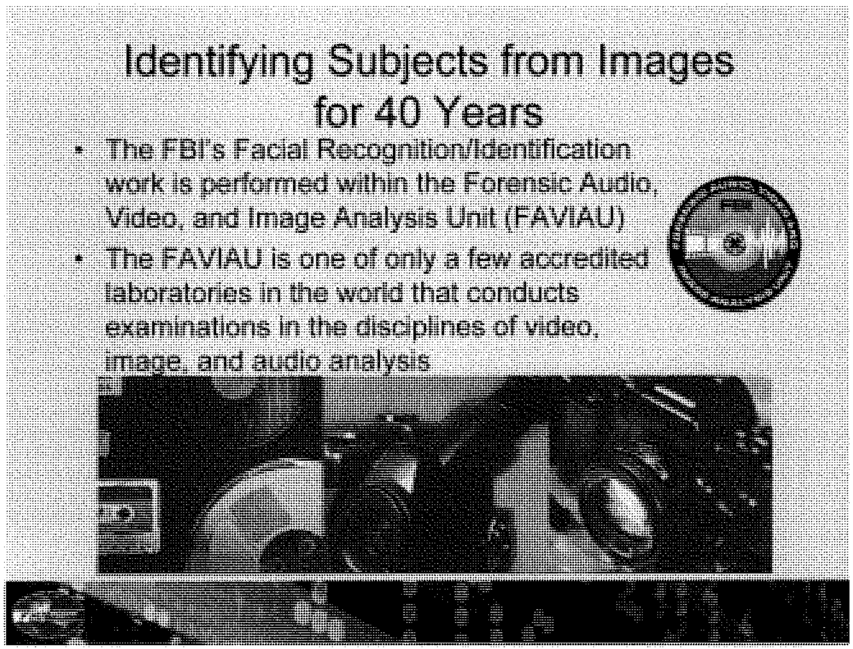
FI & FR Address Multiple Missions

- Mission Areas:
  - – Access control
  - – Automated identity verification
  - – Human identification
  - – Screening
  - – Surveillance
  - – Law enforcement & national security investigations
  - – Identity intelligence to understand intent



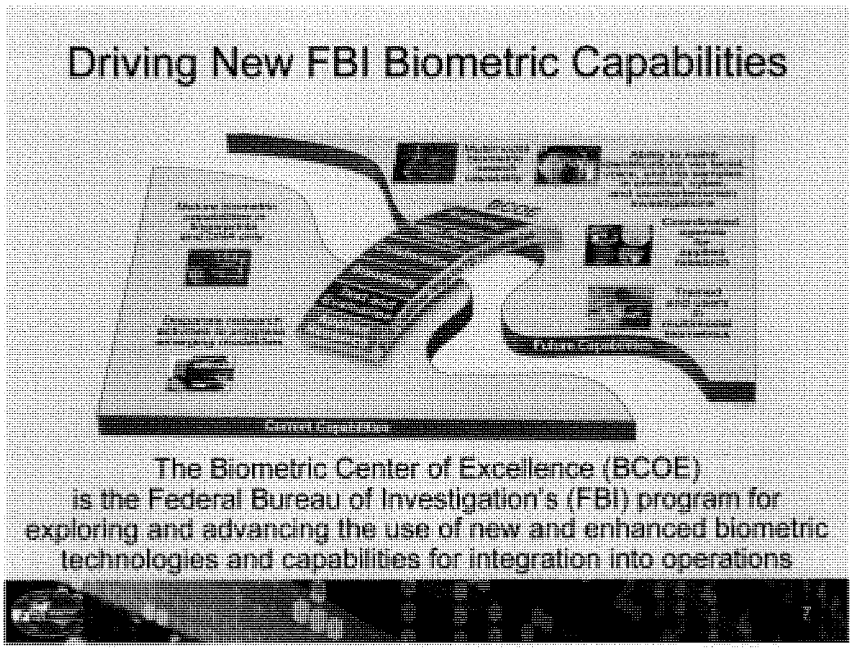
FBI Facial Use Cases

- Identifying fugitives and missing persons in FR systems
- Identifying unknown persons of interest from images (1:N)
- Tracking subjects movements to/from critical events (e.g., 9/11)
- Conducting automated surveillance at lookout locations (1:M, where 1<M<<N)
- Identifying subjects in public datasets
- Identifying subjects from images in seized systems
- Verifying mug shots against National Criminal Information Center (NCIC) records (1:1)
- Controlling access



Identifying Subjects from Images for 40 Years

- The FBI's Facial Recognition/Identification work is performed within the Forensic Audio, Video, and Image Analysis Unit (FAVIAU)
- The FAVIAU is one of only a few accredited laboratories in the world that conducts examinations in the disciplines of video, image, and audio analysis

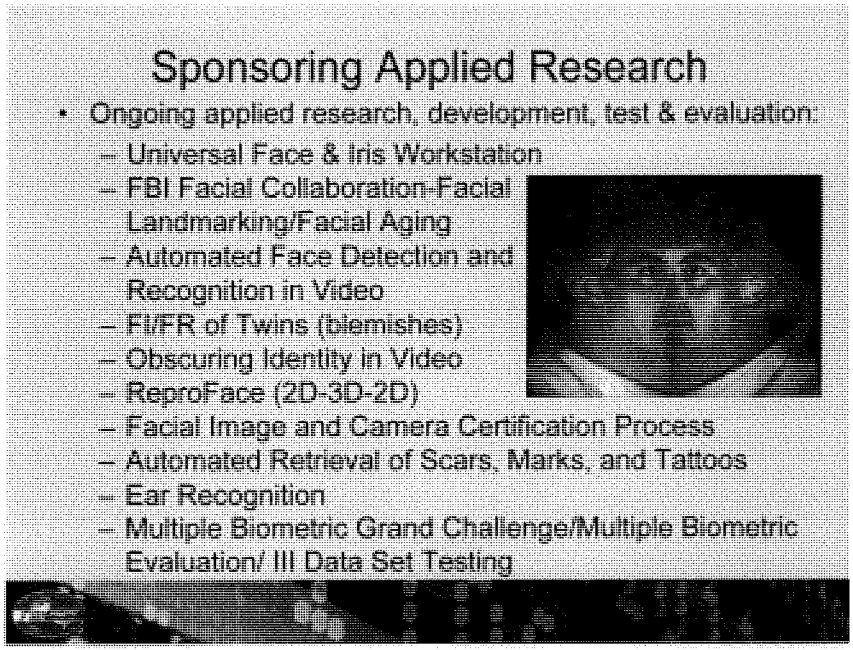


Driving New FBI Biometric Capabilities

BCOE
Future Capabilities
Current Capabilities

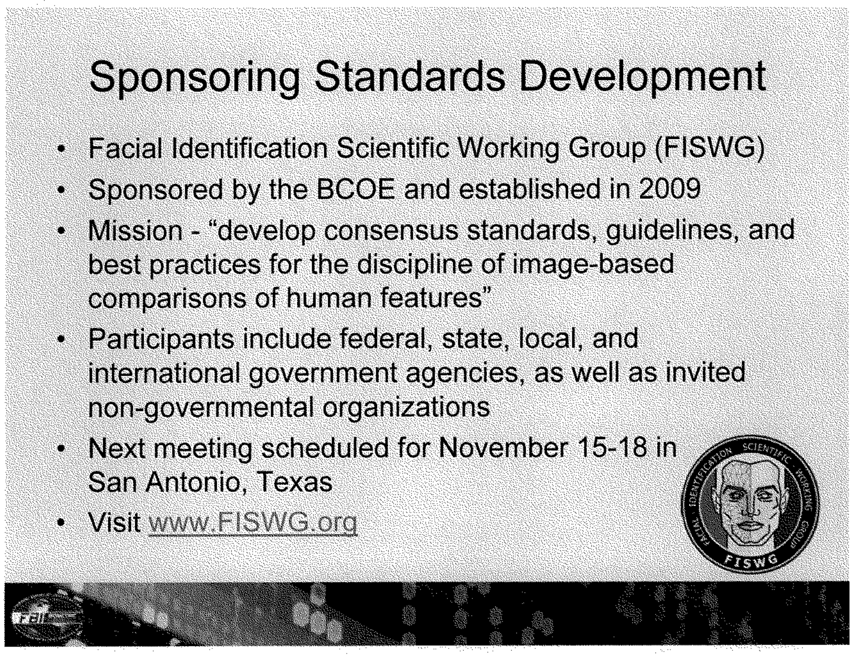
The Biometric Center of Excellence (BCOE)
is the Federal Bureau of Investigation's (FBI) program for
exploring and advancing the use of new and enhanced biometric
technologies and capabilities for integration into operations

7



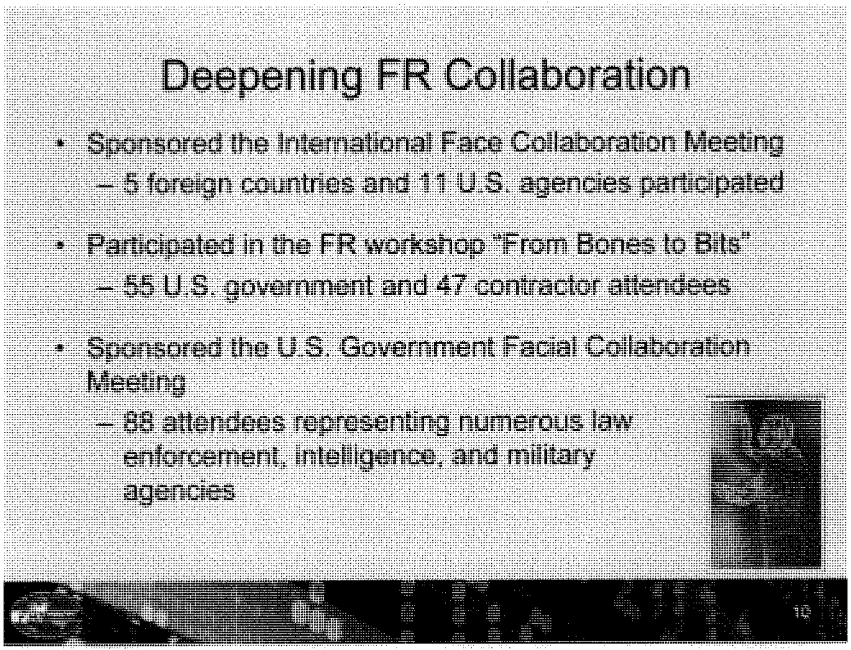
Sponsoring Applied Research

- Ongoing applied research, development, test & evaluation:
  - Universal Face & Iris Workstation
  - FBI Facial Collaboration-Facial Landmarking/Facial Aging
  - Automated Face Detection and Recognition in Video
  - FI/FR of Twins (blemishes)
  - Obscuring Identity in Video
  - ReproFace (2D-3D-2D)
  - Facial Image and Camera Certification Process
  - Automated Retrieval of Scars, Marks, and Tattoos
  - Ear Recognition
  - Multiple Biometric Grand Challenge/Multiple Biometric Evaluation/ III Data Set Testing



Sponsoring Standards Development

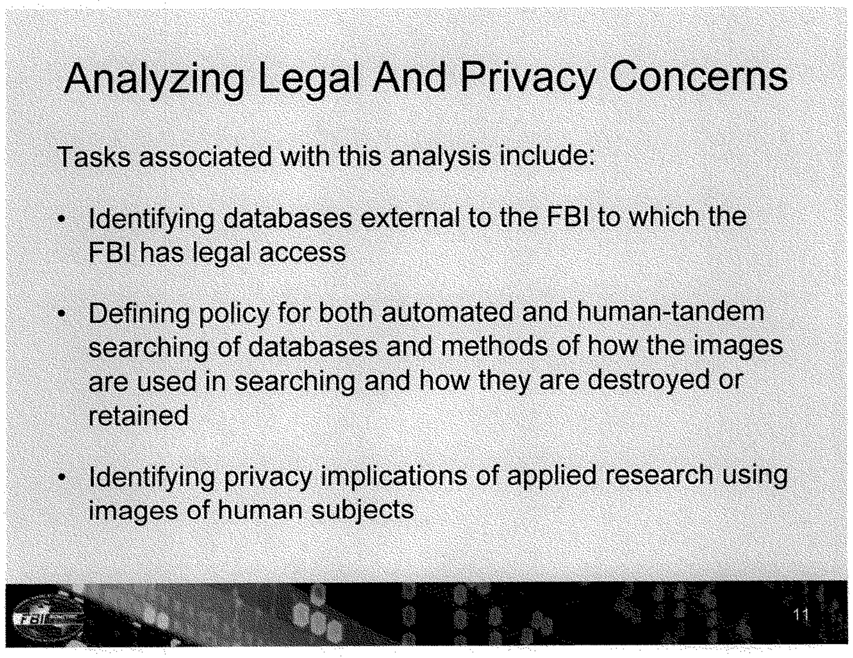
- Facial Identification Scientific Working Group (FISWG)
- Sponsored by the BCOE and established in 2009
- Mission - “develop consensus standards, guidelines, and best practices for the discipline of image-based comparisons of human features”
- Participants include federal, state, local, and international government agencies, as well as invited non-governmental organizations
- Next meeting scheduled for November 15-18 in San Antonio, Texas
- Visit www.FISWG.org



Deepening FR Collaboration

- Sponsored the International Face Collaboration Meeting
  - 5 foreign countries and 11 U.S. agencies participated
- Participated in the FR workshop "From Bones to Bits"
  - 55 U.S. government and 47 contractor attendees
- Sponsored the U.S. Government Facial Collaboration Meeting
  - 88 attendees representing numerous law enforcement, intelligence, and military agencies

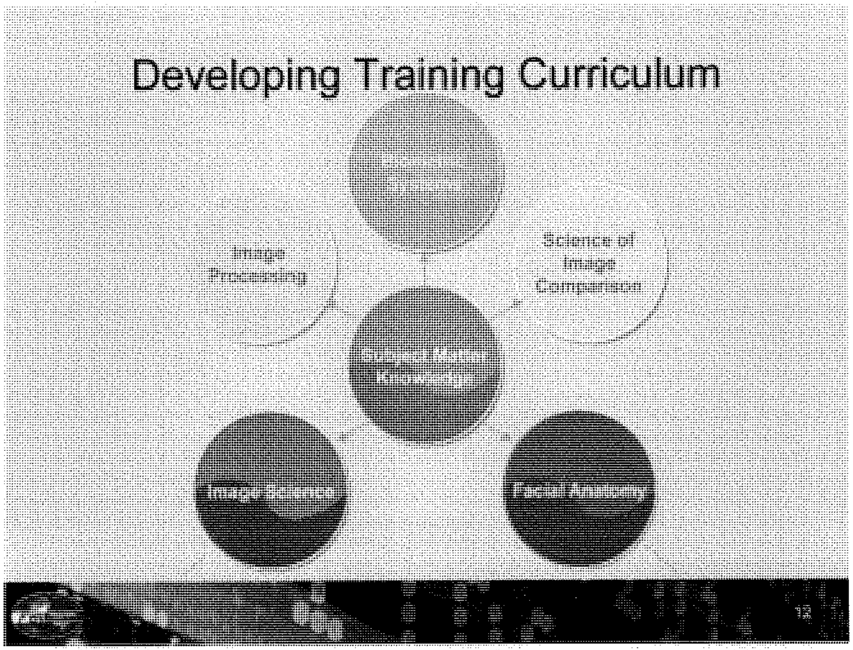
10



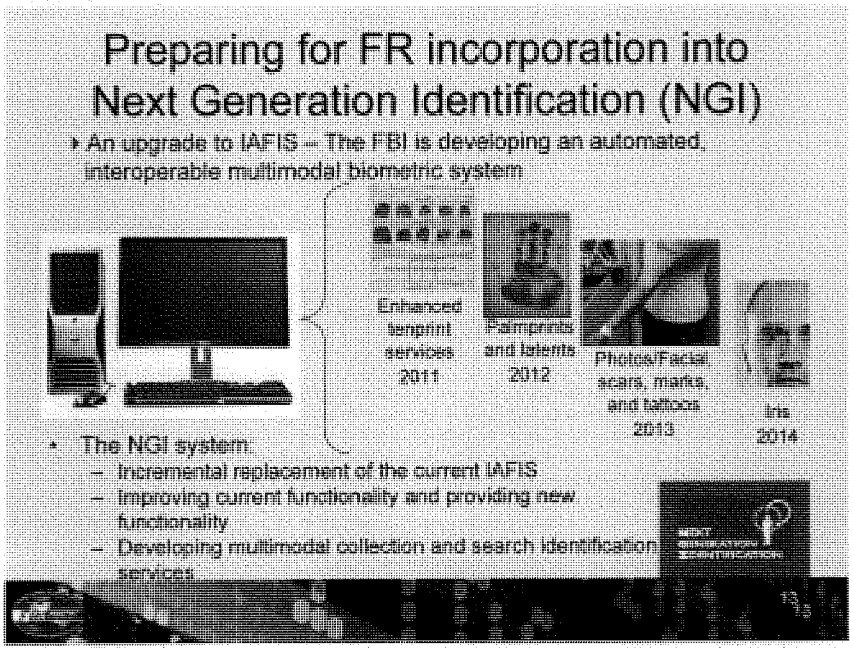
Analyzing Legal And Privacy Concerns

Tasks associated with this analysis include:

- Identifying databases external to the FBI to which the FBI has legal access
- Defining policy for both automated and human-tandem searching of databases and methods of how the images are used in searching and how they are destroyed or retained
- Identifying privacy implications of applied research using images of human subjects



Developing Training Curriculum



Preparing for FR incorporation into Next Generation Identification (NGI)

- An upgrade to IAFIS – The FBI is developing an automated, interoperable multimodal biometric system

Enhanced tenprint services 2011

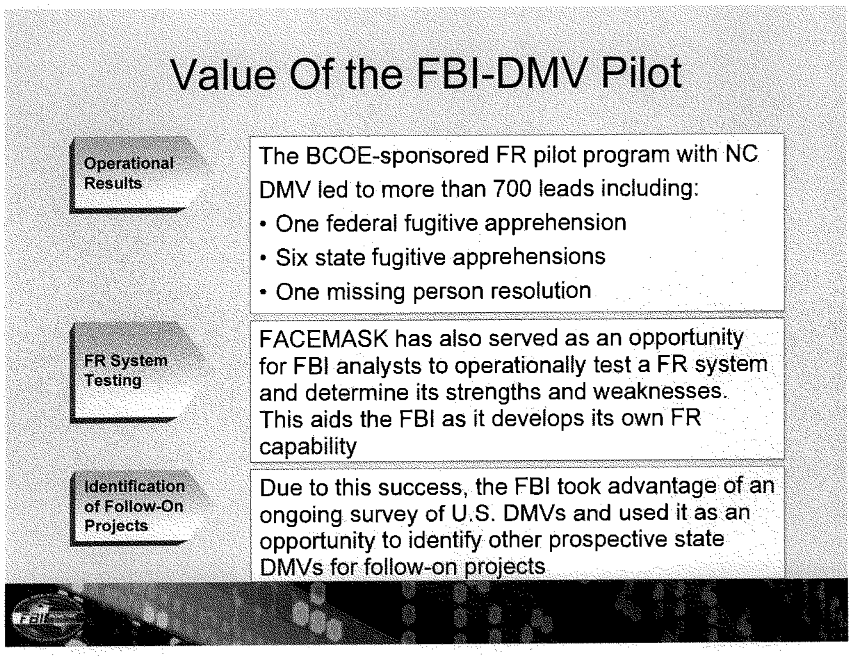
Palmprints and latents 2012

Photos/Facial scars, marks, and tattoos 2013

Iris 2014

- The NGI system:
  - Incremental replacement of the current IAFIS
  - Improving current functionality and providing new functionality
  - Developing multimodal collection and search identification services

13



Value Of the FBI-DMV Pilot

Operational Results

The BCOE-sponsored FR pilot program with NC DMV led to more than 700 leads including:

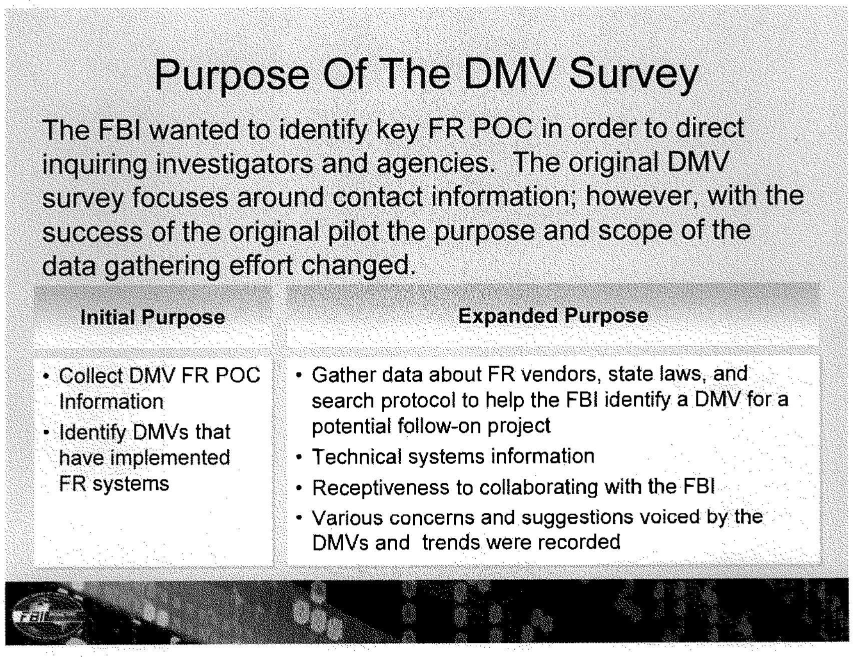
- One federal fugitive apprehension
- Six state fugitive apprehensions
- One missing person resolution

FR System Testing

FACEMASK has also served as an opportunity for FBI analysts to operationally test a FR system and determine its strengths and weaknesses. This aids the FBI as it develops its own FR capability

Identification of Follow-On Projects

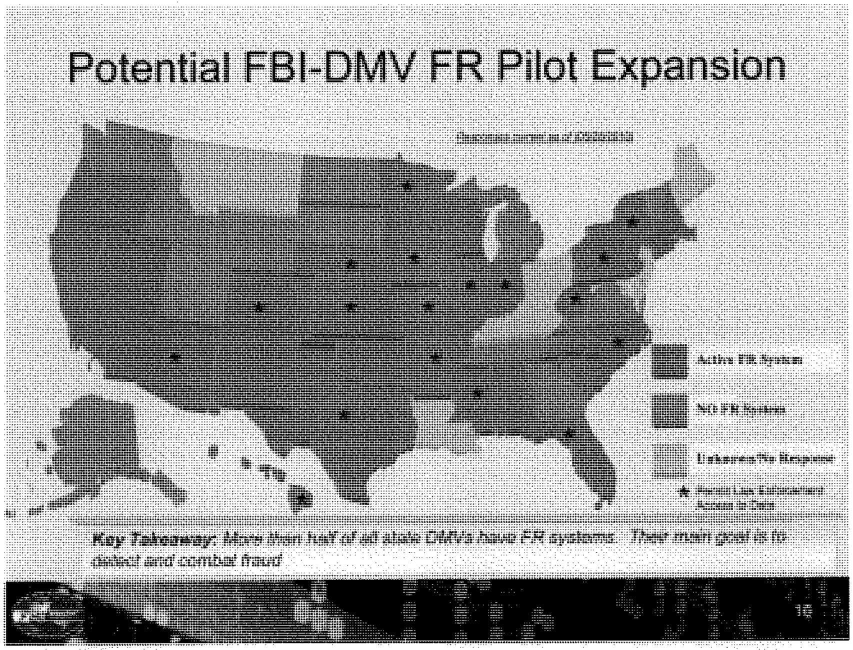
Due to this success, the FBI took advantage of an ongoing survey of U.S. DMVs and used it as an opportunity to identify other prospective state DMVs for follow-on projects



Purpose Of The DMV Survey

The FBI wanted to identify key FR POC in order to direct inquiring investigators and agencies. The original DMV survey focuses around contact information; however, with the success of the original pilot the purpose and scope of the data gathering effort changed.

Initial Purpose	Expanded Purpose
• Collect DMV FR POC Information • Identify DMVs that have implemented FR systems	• Gather data about FR vendors, state laws, and search protocol to help the FBI identify a DMV for a potential follow-on project • Technical systems information • Receptiveness to collaborating with the FBI • Various concerns and suggestions voiced by the DMVs and trends were recorded

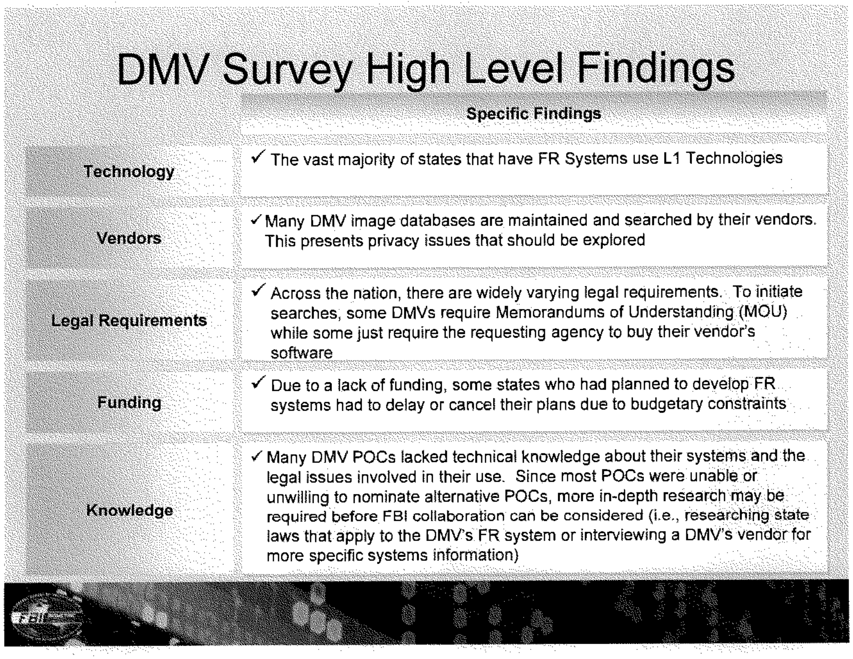


Potential FBI-DMV FR Pilot Expansion

Responses current as of [illegible]

▨	Active FR System
▨	NO FR System
░	Unknown/No Response
★	Permit Law Enforcement Access to Data

Key Takeaway: *More than half of all state DMVs have FR systems. Their main goal is to detect and combat fraud*



DMV Survey High Level Findings

	Specific Findings
Technology	✓ The vast majority of states that have FR Systems use L1 Technologies
Vendors	✓ Many DMV image databases are maintained and searched by their vendors. This presents privacy issues that should be explored
Legal Requirements	✓ Across the nation, there are widely varying legal requirements. To initiate searches, some DMVs require Memorandums of Understanding (MOU) while some just require the requesting agency to buy their vendor's software
Funding	✓ Due to a lack of funding, some states who had planned to develop FR systems had to delay or cancel their plans due to budgetary constraints
Knowledge	✓ Many DMV POCs lacked technical knowledge about their systems and the legal issues involved in their use. Since most POCs were unable or unwilling to nominate alternative POCs, more in-depth research may be required before FBI collaboration can be considered (i.e., researching state laws that apply to the DMV's FR system or interviewing a DMV's vendor for more specific systems information)

Questions / Comments

Contact Information:

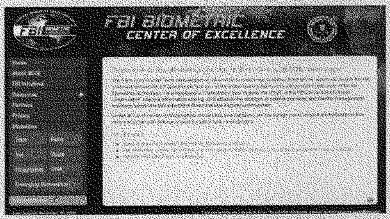
Richard Vorder Bruegge

Email: Richard.VorderBruegge@ic.fbi.gov

Additional Resources:

www.BiometricCoE.gov

Email: BiometricCoE@leo.gov



UNITED STATES PUBLIC LAWS
112th Congress - Second Session
Convening January 04, 2012

Additions and Deletions are not identified in this database.
Vetoed provisions within tabular material are not displayed
Vetoes are indicated by ~~Text~~ ;
stricken material by Text .

PL 112–98 [HR 347]
March 8, 2012

FEDERAL RESTRICTED BUILDINGS AND GROUNDS IMPROVEMENT ACT OF 2011

An Act To correct and simplify the drafting of section 1752 (relating to restricted buildings or grounds) of title 18, United States Code.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

<< 18 USCA § 1 NOTE >>

This Act may be cited as the "**Federal Restricted Buildings** and **Grounds Improvement Act** of **2011**".

SEC. 2. RESTRICTED BUILDING OR GROUNDS.

Section 1752 of title 18, United States Code, is amended to read as follows:

<< 18 USCA § 1752 >>

"§ 1752. Restricted building or grounds

"(a) Whoever--

"(1) knowingly enters or remains in any restricted building or grounds without lawful authority to do so;

"(2) knowingly, and with intent to impede or disrupt the orderly conduct of Government business or official functions, engages in disorderly or disruptive conduct in, or within such proximity to, any restricted building or grounds when, or so that, such conduct, in fact, impedes or disrupts the orderly conduct of Government business or official functions;

"(3) knowingly, and with the intent to impede or disrupt the orderly conduct of Government business or official functions, obstructs or impedes ingress or egress to or from any restricted building or grounds; or

"(4) knowingly engages in any act of physical violence against any person or property in any restricted building or grounds;

or attempts or conspires to do so, shall be punished as provided in subsection (b).

"(b) The punishment for a violation of subsection (a) is--

"(1) a fine under this title or imprisonment for not more than 10 years, or both, if--

"(A) the person, during and in relation to the offense, uses or carries a deadly or dangerous weapon or firearm; or

"(B) the offense results in significant bodily injury as defined by section 2118(e)(3); and

"(2) a fine under this title or imprisonment for not more than one year, or both, in any other case.

"(c) In this section--

***264** "(1) the term 'restricted buildings or grounds' means any posted, cordoned off, or otherwise restricted area--

"(A) of the White House or its grounds, or the Vice President's official residence or its grounds;

"(B) of a building or grounds where the President or other person protected by the Secret Service is or will be temporarily visiting; or

"(C) of a building or grounds so restricted in conjunction with an event designated as a special event of national significance; and

"(2) the term 'other person protected by the Secret Service' means any person whom the United States Secret Service is authorized to protect under section 3056 of this title or by Presidential memorandum, when such person has not declined such protection.".

Approved March 8, 2012.

PL 112-98, 2012 HR 347

END OF DOCUMENT

C

West's **Hawai'i** Revised Statutes Annotated Currentness
Division 5. Crimes and Criminal Proceedings
Title 38. Procedural and Supplementary Provisions
Chapter 852. Obstruction of Ingress or Egress
→→ **§ 852-1. Refusal to provide ingress or egress**

(a) Whenever ingress to or egress from any public or private place is obstructed by any person or persons in such manner as not to leave a free passageway for persons and vehicles lawfully seeking to enter or leave such place, any law enforcement officer shall direct such person or persons to move so as to provide and maintain a free and unobstructed passageway for persons and vehicles lawfully going into or out of such place. It shall be unlawful for any person to refuse or wilfully fail to move as directed by such officer.

(b) As used in this section, "law enforcement officer" means any public servant, whether employed by the State or county, vested by law with a duty to maintain public order, to make arrests for offenses, or to enforce the criminal laws, whether the duty extends to all offenses or is limited to a specific class of offenses.

CREDIT(S)

Laws 1949, Sp. Sess., ch. 9, § 1; R.L. 1955, § 297-1; H.R.S. § 754-1; Laws 1972, ch. 9, § 1; Laws 2002, ch. 144, § 1.

LIBRARY REFERENCES

Disorderly Conduct 🔑 1.
Obstructing Justice 🔑 1.
Westlaw Topic Nos. 129k1; 282k1.
C.J.S. Disorderly Conduct §§ 2 to 3.
C.J.S. Obstructing Justice or Governmental Administration §§ 1, 3 to 14, 16, 18 to 20, 25 to 30, 33, 35 to 36 , 38.

NOTES OF DECISIONS

Constitutional rights 3
Entrapment 4
Federal preemption 2
Right to trial by jury 5
Validity 1

1. Validity

Statute prohibiting the obstruction of ingress to or egress from any public or private place, and making it unlawful to refuse or willfully fail to move so as to provide free and unobstructed passageway when instructed to do so by peace officer, was not void for vagueness under Due Process Clauses and was constitutional on its face; statute gave person of ordinary intelligence an opportunity to know what conduct was prohibited, and it provided sufficiently explicitly standards for those applying it. U.S.C.A. Const.Amend. 14; Const. Art. 1, § 5; HRS § 852-1. State v. Guzman, 1998, 968 P.2d 194, 89 Hawai'i 27, certiorari denied 980 P.2d 998, 91 Hawai'i 124. Constitutional Law 🔑 4509(8); Constitutional Law 🔑 4509(21); Disorderly Conduct 🔑 101; Disorderly Conduct 🔑 108; Disorderly Conduct 🔑 132; Obstructing Justice 🔑 2

2. Federal preemption

National Labor Relations Act does not preempt state statute prohibiting the obstruction of ingress to or egress from any public or private place. National Labor Relations Act, § 1 et seq., as amended, 29 U.S.C.A. § 151 et seq.; HRS § 852-1. State v. Guzman, 1998, 968 P.2d 194, 89 Hawai'i 27, certiorari denied 980 P.2d 998, 91 Hawai'i 124. Disorderly Conduct 🔑 101; Disorderly Conduct 🔑 108; States 🔑 18.55

3. Constitutional rights

Three defendants' conduct of sitting in hole being used by county water supply workers to investigate illegal water line in Hawaiian Home Lands, preventing them from continuing their investigation, was not protected free speech under state or federal constitution, and thus prosecution of defendants for obstructing government operations, which arose from such conduct, was not precluded as matter of law. U.S.C.A. Const.Amend. 1; Const. Art. 1, § 4; HRS §§ 702-222(1)(b), 710-1010(1)(a). State v. Jim, 2004, 97 P.3d 395, 105 Hawai'i 319, as amended, certiorari denied 97 P.3d 1012, 105 Hawai'i 360. Constitutional Law 🔑 1807; Obstructing Justice 🔑 7

Statute prohibiting the obstruction of ingress to or egress from any public or private place did not chill free expression so as to violate Federal and State Constitutions; individuals could continue exercising rights of free expression so long as they did not do so in a manner prohibited by statute. U.S.C.A. Const.Amend. 1; Const. Art. 1, § 4; HRS § 852-1. State v. Guzman, 1998, 968 P.2d 194, 89 Hawai'i 27, certiorari denied 980 P.2d 998, 91 Hawai'i 124. Constitutional Law 🔑 1731; Constitutional Law 🔑 1780; Disorderly Conduct 🔑 101; Disorderly Conduct 🔑 108

4. Entrapment

Picketing hospital security guards who were arrested under statute prohibiting the obstruction of ingress to or egress from any public or private place, after they failed to move from hospital driveway when ordered to do so by police officer, could seek to establish defense of entrapment by estoppel based on alleged prior agreement with other officers concerning picketing procedures; guards would be required to show that, in refusing to obey order, they relied on earlier representations that led them to believe their conduct was lawful, and that such reliance was reasonable. Const. Art. 1, § 5; HRS § 852-1. State v. Guzman, 1998, 968 P.2d 194, 89 Hawai'i 27, certiorari denied 980 P.2d 998, 91 Hawai'i 124. Criminal Law 🔑 37(6.1)

5. Right to trial by jury

Defendant charged with refusing to provide ingress or egress while walking labor picket line was not entitled to jury trial, since offense was presumptively petty; Code statute on grades and classes of offenses overrode non-Code statute defining offense, such that maximum punishment was 30 days in jail, rather than six months. U.S.C.A. Const.Amend. 6; Const. Art. 1, § 13; HRS §§ 701-107, 706-663, 852-1. State v. Emerson, 2006, 129 P.3d 1167, 110 Hawai'i 139, corrected. Jury 🔑 22(2)

Defendant's charge of refusing to provide ingress or egress while walking labor picket line was not extraordinary case in which presumption was overcome that right to jury trial did not attach to such petty offense; there was no such offense at common law, offense was not comparatively grave, and additional penalty of $200 fine was comparatively minor. U.S.C.A. Const.Amend. 6; Const. Art. 1, § 13; HRS §§ 701-107, 706-663, 852-1. State v. Emerson, 2006, 129 P.3d 1167, 110 Hawai'i 139, corrected. Jury 🔑 22(2)

H R S § 852-1, HI ST § 852-1

Current with amendments through Act 129 of the 2012 Regular Session.

END OF DOCUMENT

West's Smith-Hurd Illinois Compiled Statutes Annotated Currentness
Chapter 740. Civil Liabilities
→ Act 14. Biometric Information Privacy Act

→14/1. Short title

§ 1. Short title. This Act may be cited as the Biometric Information Privacy Act.

→14/5. Legislative findings; intent

§ 5. Legislative findings; intent. The General Assembly finds all of the following:

(a) The use of biometrics is growing in the business and security screening sectors and appears to promise streamlined financial transactions and security screenings.

(b) Major national corporations have selected the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions, including finger-scan technologies at grocery stores, gas stations, and school cafeterias.

(c) Biometrics are unlike other unique identifiers that are used to access finances or other sensitive information. For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions.

(d) An overwhelming majority of members of the public are weary of the use of biometrics when such information is tied to finances and other personal information.

(e) Despite limited State law regulating the collection, use, safeguarding, and storage of biometrics, many members of the public are deterred from partaking in biometric identifier-facilitated transactions.

(f) The full ramifications of biometric technology are not fully known.

(g) The public welfare, security, and safety will be served by regulating the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.

→14/10. Definitions

§ 10. Definitions. In this Act:

"Biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color. Biometric identifiers do not include donated organs, tissues, or parts as defined in the Illinois Anatomical Gift Act or blood or serum stored on behalf of recipients or potential recipients of living or cadaveric transplants and obtained or stored by a federally designated organ procurement agency. Biometric identifiers do not include biological materials regulated under the Genetic Information Privacy Act. Biometric identifiers do not include information captured from a patient in a health care setting or information collected, used, or stored for health care treatment, payment, or operations under the federal Health Insurance Portability and Accountability Act of 1996. Biometric identifiers do not include an X-ray, roentgen process, computed tomography, MRI, PET scan, mammography, or other image or film of the human anatomy used to diagnose, prognose, or treat an illness or other medical condition or to further validate scientific testing or screening.

"Biometric information" means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.

"Confidential and sensitive information" means personal information that can be used to uniquely identify an individual or an individual's account or property. Examples of confidential and sensitive information include, but are not limited to, a genetic marker, genetic testing information, a unique identifier number to locate an account or property, an account number, a PIN number, a pass code, a driver's license number, or a social security number.

"Private entity" means any individual, partnership, corporation, limited liability company, association, or other group, however organized. A private entity does not include a State or local government agency. A private entity does not include any court of Illinois, a clerk of the court, or a judge or justice thereof.

"Written release" means informed written consent or, in the context of employment, a release executed by an employee as a condition of employment.

→ **14/15. Retention; collection; disclosure; destruction**

§ 15. Retention; collection; disclosure; destruction.

(a) A private entity in possession of biometric identifiers or biometric information must develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first. Absent a valid warrant or subpoena issued by a court of competent jurisdiction, a private entity in possession of biometric identifiers or biometric information must comply with its established retention schedule and destruction guidelines.

(b) No private entity may collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or biometric information, unless it first:

(1) informs the subject or the subject's legally authorized representative in writing that a biometric identifier or biometric information is being collected or stored;

(2) informs the subject or the subject's legally authorized representative in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and

(3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative.

(c) No private entity in possession of a biometric identifier or biometric information may sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information.

(d) No private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless:

(1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure;

(2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative;

(3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or

(4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction.

(e) A private entity in possession of a biometric identifier or biometric information shall:

(1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and

(2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits, and protects other confidential and sensitive information.

→ 14/20. Right of action

§ 20. Right of action. Any person aggrieved by a violation of this Act shall have a right of action in a State circuit court or as a supplemental claim in federal district court against an offending party. A prevailing party may recover for each violation:

(1) against a private entity that negligently violates a provision of this Act, liquidated damages of $1,000 or actual damages, whichever is greater;

(2) against a private entity that intentionally or recklessly violates a provision of this Act, liquidated damages of $5,000 or actual damages, whichever is greater;

(3) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses; and

(4) other relief, including an injunction, as the State or federal court may deem appropriate.

→ 14/25. Construction

§ 25. Construction.

(a) Nothing in this Act shall be construed to impact the admission or discovery of biometric identifiers and biometric information in any action of any kind in any court, or before any tribunal, board, agency, or person.

(b) Nothing in this Act shall be construed to conflict with the X-Ray Retention Act, the federal Health Insurance Portability and Accountability Act of 1996 and the rules promulgated under either Act.

(c) Nothing in this Act shall be deemed to apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 and the rules promulgated thereunder.

(d) Nothing in this Act shall be construed to conflict with the Private Detective, Private Alarm, Private Security, Fingerprint Vendor, and Locksmith Act of 2004 and the rules promulgated thereunder.

(e) Nothing in this Act shall be construed to apply to a contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government.

→14/30. Biometric Information Privacy Study Committee

§ 30. Biometric Information Privacy Study Committee.

(a) The Department of Human Services, in conjunction with Central Management Services, subject to appropriation or other funds made available for this purpose, shall create the Biometric Information Privacy Study Committee, hereafter referred to as the Committee. The Department of Human Services, in conjunction with Central Management Services, shall provide staff and administrative support to the Committee. The Committee shall examine (i) current policies, procedures, and practices used by State and local governments to protect an individual against unauthorized disclosure of his or her biometric identifiers and biometric information when State or local government requires the individual to provide his or her biometric identifiers to an officer or agency of the State or local government; (ii) issues related to the collection, destruction, security, and ramifications of biometric identifiers, biometric information, and biometric technology; and (iii) technical and procedural changes necessary in order to implement and enforce reasonable, uniform biometric safeguards by State and local government agencies.

(b) The Committee shall hold such public hearings as it deems necessary and present a report of its findings and recommendations to the General Assembly before January 1, 2009. The Committee may begin to conduct business upon appointment of a majority of its members. All appointments shall be completed by 4 months prior to the release of the Committee's final report. The Committee shall meet at least twice and at other times at the call of the chair and may conduct meetings by telecommunication, where possible, in order to minimize travel expenses. The Committee shall consist of 27 members appointed as follows:

(1) 2 members appointed by the President of the Senate;

(2) 2 members appointed by the Minority Leader of the Senate;

(3) 2 members appointed by the Speaker of the House of Representatives;

(4) 2 members appointed by the Minority Leader of the House of Representatives;

(5) One member representing the Office of the Governor, appointed by the Governor;

(6) One member, who shall serve as the chairperson of the Committee, representing the Office of the Attorney General, appointed by the Attorney General;

(7) One member representing the Office of the Secretary of the State, appointed by the Secretary of State;

(8) One member from each of the following State agencies appointed by their respective heads: Department of Corrections, Department of Public Health, Department of Human Services, Central Management Services, Illinois Commerce Commission, Illinois State Police, Department of Revenue;

(9) One member appointed by the chairperson of the Committee, representing the interests of the City of Chicago;

(10) 2 members appointed by the chairperson of the Committee, representing the interests of other municipalities;

(11) 2 members appointed by the chairperson of the Committee, representing the interests of public hospitals; and

(12) 4 public members appointed by the chairperson of the Committee, representing the interests of the civil liberties community, the electronic privacy community, and government employees.

(c) This Section is repealed January 1, 2009.

➡14/99. Effective date

§ 99. Effective date. This Act takes effect upon becoming law.

END OF DOCUMENT

MD Code, Criminal Law, § 10-201

Formerly cited as MDCODE Art. 27, § 121

C

West's Annotated Code of Maryland Currentness
Criminal Law (Refs & Annos)
Title 10. Crimes Against Public Health, Conduct, and Sensibilities
Subtitle 2. Disturbing the Peace, Disorderly Conduct, and Related Crimes
→→ **§ 10-201. Disturbing the public peace and disorderly conduct**

Definitions

(a)(1) In this section the following words have the meanings indicated.

(2)(i) "**Public conveyance**" means a conveyance to which the public or a portion of the public has access to and a right to use for transportation.

(ii) "**Public conveyance**" includes an airplane, vessel, bus, railway car, school vehicle, and subway car.

(3)(i) "Public place" means a place to which the public or a portion of the public has access and a right to resort for business, dwelling, entertainment, or other lawful purpose.

(ii) "Public place" includes:

1. a restaurant, shop, shopping center, store, tavern, or other place of business;

2. a public building;

3. a public parking lot;

4. a public street, sidewalk, or right-of-way;

5. a public park or other public grounds;

6. the common areas of a building containing four or more separate dwelling units, including a corridor, elevator, lobby, and stairwell;

7. a hotel or motel;

8. a place used for public resort or amusement, including an amusement park, golf course, race track, sports arena, swimming pool, and theater;

9. an institution of elementary, secondary, or higher education;

10. a place of public worship;

11. a place or building used for entering or exiting a **public conveyance**, including an airport terminal, bus station, dock, railway station, subway station, and wharf; and

12. the parking areas, sidewalks, and other grounds and structures that are part of a public place.

Construction of section

(b) For purposes of a prosecution under this section, a **public conveyance** or a public place need not be devoted solely to public use.

Prohibited

(c)(1) A person may not willfully and without lawful purpose obstruct or hinder the free passage of another in a public place or on a **public conveyance**.

(2) A person may not willfully act in a disorderly manner that disturbs the public peace.

(3) A person may not willfully fail to obey a reasonable and lawful order that a law enforcement officer makes to prevent a disturbance to the public peace.

(4) A person who enters the land or premises of another, whether an owner or lessee, or a beach adjacent to residential riparian property, may not willfully:

(i) disturb the peace of persons on the land, premises, or beach by making an unreasonably loud noise; or

(ii) act in a disorderly manner.

(5) A person from any location may not, by making an unreasonably loud noise, willfully disturb the peace of

another:

(i) on the other's land or premises;

(ii) in a public place; or

(iii) on a **public conveyance**.

(6) In Worcester County, a person may not build a bonfire or allow a bonfire to burn on a beach or other property between 1 a.m. and 5 a.m.

Penalty

(d) A person who violates this section is guilty of a misdemeanor and on conviction is subject to imprisonment not exceeding 60 days or a fine not exceeding $500 or both.

CREDIT(S)

Added by Acts 2002, c. 26, § 2, eff. Oct. 1, 2002.

Formerly Art. 27, § 121.

LEGISLATIVE NOTES

Revisor's Note (Acts 2002, c. 26):

> This section is new language derived without substantive change from former Art. 27, § 121.
>
> Subsection (b) of this section is revised as a construction provision for clarity.
>
> In subsection (a)(2)(i) and (3)(i) of this section, the former references to the "general" public are deleted as unnecessary.
>
> In subsection (a)(2)(ii) of this section, the former reference to a "boat" is deleted as included in the comprehensive reference to a "vessel".
>
> Also in subsection (a)(2)(ii) of this section, the former reference to a "school bus" is deleted in light of the comprehensive reference to a "school vehicle".
>
> In subsection (a)(3)(ii)12 of this section, the former reference to parking "lots" is deleted as included in the reference to "parking areas".

Formerly cited as MDCODE Art. 27, § 121

In subsection (c)(5) of this section, the former phrase "in a place of business" is deleted as included in the definition of "public place".

Defined term: "Person" § 1-101

HISTORICAL AND STATUTORY NOTES

Derivation:

Former Art. 27, § 121, related to obstructing or hindering free passage in a public place or on a **public conveyance**, repealed by Acts 2002, c. 26, § 1.

LIBRARY REFERENCES

Breach of The Peace 🔑 1, 14.
Westlaw Key Number Searches: 62k1; 62k14.
C.J.S. Breach of the Peace §§ 2 to 5, 13.

RESEARCH REFERENCES

ALR Library

52 ALR 6th 125, Validity, Construction, and Application of State Statutes and Municipal Ordinances Proscribing Failure or Refusal to Obey Police Officer's Order to Move On, or Disperse, on Street, as Disorderly Conduct.

9 ALR 3rd 203, Modern Status of Doctrine of Res Judicata in Criminal Cases.

Encyclopedias

Maryland Law Encyclopedia Amusements § 10, Civil Penalties and Criminal Offenses.

Maryland Law Encyclopedia Criminal Law § 40, Several Offenses in Same Act or Transaction.

Maryland Law Encyclopedia Highways § 38, Common Law and Statutory Offenses.

NOTES OF DECISIONS

Admissibility of evidence 12
Arrest 7
Collateral estoppel 9.6
Construction and application 2
Double jeopardy 9.5
Fighting words 6

1. Validity

Disorderly conduct conviction based on advocacy of unpopular ideas would violate Constitution. Code Md.1957, art. 27, § 123; Code Md.Supp. art. 27, § 123(c); U.S.C.A.Const. Amends. 1, 14. Bachellar v. Maryland, 1970, 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Constitutional Law 🔑 1812

Statute making it unlawful for anyone to "wilfully disturb any neighborhood in [any Maryland] city, town or county by loud and unseemly noises" was not unconstitutionally overbroad. U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md. 436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Constitutional Law 🔑 1840; Disorderly Conduct 🔑 101; Disorderly Conduct 🔑 110

Statute making it unlawful for anyone to "wilfully disturb any neighborhood in [any Maryland] city, town or county by loud and unseemly noises," as construed to regulate only volume and not content of speech, was sufficiently narrowly tailored. U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md. 436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Constitutional Law 🔑 1840; Disorderly Conduct 🔑 101; Disorderly Conduct 🔑 110

Statute prohibiting residential picketing, even if peaceful, orderly, quiet, and nonthreatening and on public property and without obstruction of persons or traffic, violates First and Fourteenth Amendments. Code 1957, art. 27, § 580A; U.S.C.A.Const. Amends. 1, 14. State v. Schuller, 1977, 372 A.2d 1076, 280 Md. 305. Constitutional Law 🔑 1852; Constitutional Law 🔑 4071; Disorderly Conduct 🔑 101; Disorderly Conduct 🔑 111

2. Construction and application

Words "loud and unseemly" in statute making it unlawful for anyone to "wilfully disturb any neighborhood in [any Maryland] city, town or county by loud and unseemly noises," construed to proscribe speech so unreasonably loud as to unreasonably intrude on privacy of captive audience, were not vague. U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md. 436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Disorderly Conduct 🔑 101; Disorderly Conduct 🔑 110

Word "unseemly" in statute proscribing wilfully disturbing any neighborhood in any city, town or county by "loud and unseemly noises" would be construed in content-neutral fashion as directly modifying volume level of "loud." U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md. 436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Constitutional Law 🔑 1840

Statute prohibiting disorderly conduct upon any public street is sufficiently definite, in conjunction with previous judicial constructions, to inform man of ordinary intelligence of nature of activity proscribed, and was not unconstitutional as applied to defendants who refused to comply with thrice repeated request by police that defendants remove themselves from sidewalk upon which they were sitting and lying. Code 1957, art. 27, § 123; U.S.C.A.Const. Amends. 1, 14. Bacheller v. State, 1968, 240 A.2d 623, 3 Md.App. 626, certiorari denied 251 Md. 747, certiorari granted 90 S.Ct. 109, 396 U.S. 816, 24 L.Ed.2d 68, reversed 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Constitutional Law 🔑 4509(8); Disorderly Conduct 🔑 101; Disorderly Conduct 🔑 132

3. Nature and elements of offense

Failure to obey a lawful police order designed to protect the public peace may amount to disorderly conduct under Maryland law, although to be guilty of disorderly conduct on this basis, there must be a sufficient nexus between the police command and the probability of disorderly conduct. Md.Code 1957, Art. 27, § 121(b)(3). White v. Maryland Transp. Authority, 2001, 151 F.Supp.2d 651. Disorderly Conduct 🔑 132

For purposes of disorderly conduct under Maryland law, public must be present for its peace to be threatened. Md.Code 1957, Art. 27, § 121(b)(3). White v. Maryland Transp. Authority, 2001, 151 F.Supp.2d 651. Disorderly Conduct 🔑 106

Failure to obey policeman's command to move on when not to do so may endanger public peace amounts to "disorderly conduct." Code 1957, Art. 27, § 121(b)(2). Dziekonski v. State, 1999, 732 A.2d 367, 127 Md.App. 191. Disorderly Conduct 🔑 132

Carnival constituted "public resort or amusement," within meaning of disorderly conduct statute. Code 1957, Art. 27, § 123. Briggs v. State, 1992, 599 A.2d 1221, 90 Md.App. 60. Disorderly Conduct 🔑 107

Defendant violated disorderly conduct statute by shouting, grabbing back money that he lost at carnival's dicing booth, and slamming dice into table; firemen operating dicing game were moved to seek police assistance in persuading defendant to leave. Code 1957, Art. 27, § 123; U.S.C.A. Const.Amend. 1. Briggs v. State, 1992, 599 A.2d 1221, 90 Md.App. 60. Disorderly Conduct 🔑 110; Disorderly Conduct 🔑 128

Police officers reasonably told defendant to move along from carnival, and therefore his failure to obey constituted disorderly conduct; defendant had been shouting, grabbing back money he lost at dicing table, and slamming dice into table. Code 1957, Art. 27, § 123; U.S.C.A. Const.Amend. 1. Briggs v. State, 1992, 599 A.2d 1221, 90 Md.App. 60. Disorderly Conduct 🔑 132

Even if police officers unlawfully demanded that defendant leave carnival, his response to their order constituted disorderly conduct, where defendant, in addition to physically resisting officers' efforts to take him into custody, threatened officers, and incited crowd sufficiently to cause officers to fear the crowd would "take him away" from them. Code 1957, Art. 27, § 123; U.S.C.A. Const.Amend. 1. Briggs v. State, 1992, 599 A.2d 1221, 90 Md.App. 60. Disorderly Conduct 🔑 134

Probationer's response to police officer's statement that she enter police car or she would be arrested, that probationer did not "give a fuck," did not amount to "profanity" or "obscene language", within meaning of "disorderly conduct" statutes, and thus could not serve as basis for finding violation of probation condition prohibiting disorderly conduct. Code 1957, Art. 27, §§ 121, 122. Baynard v. State, 1990, 569 A.2d 652, 318 Md. 531. Disorderly Conduct 🔑 131; Sentencing And Punishment 🔑 2004

Probationer's response to police officer's statement that she enter police car or she would be arrested, that she did not "give a fuck," could not be seen as effort to incite police officer, and thus did not fall within proscribed conduct of disorderly conduct statutes, and could not serve as basis for finding violation of probation condition prohibiting disorderly conduct, as "vulgar noun" was not directed at officer, but merely expressed probationer's state of mind. Code 1957, Art. 27, §§ 121, 122, 123. Baynard v. State, 1990, 569 A.2d 652, 318 Md. 531. Disorderly Conduct 🔑 133; Sentencing And Punishment 🔑 2004

Antiabortion protester, whose unamplified shouting disturbed local residents, and who continued to shout after being warned to lower his voice by police officer whose action was based on complaints from members of the captive audience, was properly convicted of disturbing the peace. U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md. 436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Disorderly Conduct 🔑 111; Disorderly Conduct 🔑 132

Police may act under statute making it unlawful for anyone to "wilfully disturb a neighborhood in [any Maryland] city, town or county by loud and unseemly noises" only upon receipt of complaint from affected citizen upon basis of which officer reasonably believes statute has been violated. U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md. 436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Criminal Law 🔑 1224(1)

Properly construed, statute making it unlawful for anyone to "wilfully disturb a neighborhood in [any Maryland] city, town or county by loud and unseemly noises" could be enforced to limit protected speech only to extent speaker's actions were wilful, volume clearly exceeded what was necessary to address passersby, and noise was actually disruptive to "captive" audience in the neighborhood. U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md. 436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Disorderly Conduct 🔑 106; Disorderly Conduct 🔑 110

Application of statute making it unlawful for anyone to "wilfully disturb any neighborhood in [any Maryland] city, town or county by loud and unseemly noise" ordinarily requires prior warning by police authority, so that speaker may be aware that further communication at the offensive volume level may subject the individual to prosecution. U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md.

436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Disorderly Conduct 🔑 110; Disorderly Conduct 🔑 132

Defendant's constitutionally protected oral response to unlawful police conduct was insufficient to sustain disorderly conduct conviction because defendant did not "willfully disturb" anyone nor did his speech qualify as a "loud and unseemly noise." Code 1957, Art. 27, § 121; U.S.C.A.Const.Amend. 1. Diehl v. State, 1982, 451 A.2d 115, 294 Md. 466, certiorari denied 103 S.Ct. 1798, 460 U.S. 1098, 76 L.Ed.2d 363. Disorderly Conduct 🔑 131

A person standing on a county highway making loud and unseemly noises and profanely cursing and swearing would not be guilty of disorderly conduct unless he was within the hearing of others passing by or along the highway, but it would not be necessary that the State prove such other persons in fact heard the noises; it would be sufficient if they were passing by or along the highway so that reasonably they may have heard them. Code 1957, art. 27, § 121. In re Nawrocki, 1972, 289 A.2d 846, 15 Md.App. 252, certiorari denied 266 Md. 741. Disorderly Conduct 🔑 105; Disorderly Conduct 🔑 110

The "obscene language" prohibited by disorderly conduct statute means obscene in the constitutional sense, and the profanely cursing or swearing prohibited by statutes, and the "saying" aspect of the gist of the crime of disorderly conduct, means "fighting words". Code 1957, art. 27, §§ 121-123. In re Nawrocki, 1972, 289 A.2d 846, 15 Md.App. 252, certiorari denied 266 Md. 741. Disorderly Conduct 🔑 109; Disorderly Conduct 🔑 127

"Breach of the peace" signifies disorderly, dangerous conduct disruptive of public peace. Great Atlantic & Pacific Tea Co. v. Paul, 1970, 261 A.2d 731, 256 Md. 643. Disorderly Conduct 🔑 104

The usual shoplifting incident does not constitute "breach of the peace". Great Atlantic & Pacific Tea Co. v. Paul, 1970, 261 A.2d 731, 256 Md. 643. Disorderly Conduct 🔑 140; Larceny 🔑 21

Conduct of defendant who implored crowd of from 400 to 450 whites to "burn out" Negro family was not constitutionally protected and sustained his conviction of disorderly conduct. U.S.C.A.Const. Amends. 1, 14; Code 1957, art. 27, § 123. Luthardt v. State, 1969, 251 A.2d 40, 6 Md.App. 251, certiorari denied 255 Md. 742. Disorderly Conduct 🔑 111

Merely because there was no evidence that defendant personally muttered any obscenities, shouted any insulting epithets, or uttered any fighting words during his participation in march, did not insulate him from conviction for disorderly conduct, where record clearly disclosed that he was integral part of disorderly group of persons espousing racial hatred and counseling violent action. U.S.C.A.Const. Amends. 1, 14; Code 1957, art. 27, § 123. Luthardt v. State, 1969, 251 A.2d 40, 6 Md.App. 251, certiorari denied 255 Md. 742. Disorderly Conduct 🔑 111

Where defendant and leader of march exhorted crowd by means of loudspeaker installed in vehicle to attend "rally" and "burn out the savages" because "tomorrow may be too late", defendant's subsequent presence among marchers established not only his identity with their announced objectives, but also fact of his voluntary involvement with their disorderly activities. U.S.C.A.Const. Amends. 1, 14; Code 1957, art. 27, § 123. Luthardt v. State, 1969, 251 A.2d 40, 6 Md.App. 251, certiorari denied 255 Md. 742. Disorderly Conduct 🔑 111

"Breach of the peace" includes not only violent acts but words likely to produce violence in others. Lynch v. State, 1967, 236 A.2d 45, 2 Md.App. 546, certiorari denied 249 Md. 732, certiorari denied 249 Md. 733, certiorari denied 89 S.Ct. 236, 393 U.S. 915, 21 L.Ed.2d 200. Disorderly Conduct 🔑 127; Disorderly Conduct 🔑 128

Fact that defendant may have been standing on the steps of the restaurant rather than on the public sidewalk at time police officer in an attempt to prevent a disturbance of the public peace ordered teenagers gather in front of restaurant to disperse did not take defendant's conduct out of terms of statute making disorderly conduct a crime since disorderly conduct is prohibited not only upon any public street but in any store during business hours. Code 1957, art. 27, § 123. McIntyre v. State, 1967, 232 A.2d 279, 1 Md.App. 586, certiorari denied 248 Md. 733. Disorderly Conduct 🔑 107; Disorderly Conduct 🔑 141

To constitute a "breach of peace," it is necessary to show an affray, actual violence, or conduct tending to or provocative of violence by others. Wanzer v. State, 1953, 97 A.2d 914, 202 Md. 601. Disorderly Conduct 🔑 127

4. Freedom of speech

Public expression of ideas may not be prohibited merely because ideas are themselves offensive to some of their hearers, or simply because bystanders object to peaceful and orderly demonstrations. U.S.C.A.Const. Amends. 1 , 14. Bachellar v. Maryland, 1970, 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Constitutional Law 🔑 1490; Constitutional Law 🔑 1845

Disorderly conduct convictions resting on a finding that accused sat or lay across a public sidewalk with intent of fully blocking passage along it, or that they refused to obey police commands to stop obstructing the sidewalk in this manner and move on would not violate Constitution. Code Md.1957, art. 27, § 123; Code Md.Supp. art. 27, § 123(c); U.S.C.A.Const. Amends. 1, 14. Bachellar v. Maryland, 1970, 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Disorderly Conduct 🔑 108; Disorderly Conduct 🔑 132

Police officer's order to defendant to keep her mouth quiet, given after defendant, a former hospital employee, repeatedly stated "fuck you, asshole," to officer while inside hospital, was lawful, such that subsequent arrest for disorderly conduct based on defendant's continued yelling did not violate First Amendment; orders were mainly directed at volume, rather than content, of defendant's speech, officer had compelling interest in maintaining peace and quiet in environs of hospital, and defendant had other means of expressing her discontent with hospital or officer. Polk v. State, 2003, 835 A.2d 575, 378 Md. 1, certiorari denied 124 S.Ct. 1691, 541 U.S. 951, 158 L.Ed.2d 382. Arrest 🔑 63.4(15); Constitutional Law 🔑 1795

If police officers unlawfully demanded that defendant depart from carnival, his abusive language directed at officers would be constitutionally protected. U.S.C.A. Const.Amend. 1. Briggs v. State, 1992, 599 A.2d 1221, 90 Md.App. 60. Constitutional Law 🔑 1814

Defendant's repeated utterance of unspecified obscenities while standing in dicing booth at carnival was constitutionally protected speech, and therefore such speech was not in violation of disorderly conduct statute; remarks were not addressed to any particular person. Code 1957, Art. 27, § 123; U.S.C.A. Const.Amend. 1. Briggs v. State, 1992, 599 A.2d 1221, 90 Md.App. 60. Constitutional Law 🔑 2190; Disorderly Conduct 🔑 109

Use of offensive expletive does not, by itself, deprive speech of protection, but rather court must examine context in which words were uttered. U.S.C.A. Const.Amend. 1. Briggs v. State, 1992, 599 A.2d 1221, 90 Md.App. 60. Constitutional Law 🔑 1559

Evaluating whether language violates disorderly conduct statute involves determining if, under circumstances, speech was within ambit of constitutionally protected free expression. Code 1957, Art. 27, § 123; U.S.C.A. Const.Amend. 1. Briggs v. State, 1992, 599 A.2d 1221, 90 Md.App. 60. Constitutional Law 🔑 1812; Disorderly Conduct 🔑 109

Statute making it unlawful for anyone to "wilfully disturb any neighborhood in [any Maryland] city, town or county by loud and unseemly noises" went no further than to afford content-neutral protection to the captive auditor who could not avoid continuing, unreasonably loud and disruptive communications emanating from the street. U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md. 436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Constitutional Law 🔑 1840

If State is able to prove that, under the circumstances, the human voice is so unreasonably loud as to be unreasonably intrusive on captive audience, that is enough to find application of antinoise law constitutional; artificial amplification is not a constitutional sine qua non. U.S.C.A. Const.Amend. 1; Code 1957, Art. 27, § 121. Eanes v. State, 1990, 569 A.2d 604, 318 Md. 436, certiorari denied 110 S.Ct. 3218, 496 U.S. 938, 110 L.Ed.2d 665. Constitutional Law 🔑 1840

Disorderly conduct statutes punish spoken words, but they cannot apply to speech, although vulgar or offensive, that is protected by the First and Fourteenth Amendments. Code 1957, art. 27, §§ 121-123; U.S.C.A.Const. Amends. 1, 14. In re Nawrocki, 1972, 289 A.2d 846, 15 Md.App. 252, certiorari denied 266 Md. 741. Constitutional Law 🔑 1812; Constitutional Law 🔑 4509(8)

Whether constitutional guarantee of freedom of speech is applicable depends upon whether words are used in such circumstances and are of such nature as to create clear and present danger. Bacheller v. State, 1968, 240 A.2d 623, 3 Md.App. 626, certiorari denied 251 Md. 747, certiorari granted 90 S.Ct. 109, 396 U.S. 816, 24 L.Ed.2d 68, reversed 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Constitutional Law 🔑 1529

Constitutional protection afforded particular form of conduct is more limited than that afforded pure forms of expression such as the verbalized or printed word. U.S.C.A.Const. Amends. 1, 14. Bacheller v. State, 1968, 240 A.2d 623, 3 Md.App. 626, certiorari denied 251 Md. 747, certiorari granted 90 S.Ct. 109, 396 U.S. 816, 24 L.Ed.2d 68, reversed 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Constitutional Law 🔑 1497

It is substance rather than form of communication to which constitutional right of free speech attaches, and regulation of form of communication is constitutional where same arises from legitimate state interest and not for sole purpose of censoring the underlying thought or idea. Bacheller v. State, 1968, 240 A.2d 623, 3 Md.App. 626, certiorari denied 251 Md. 747, certiorari granted 90 S.Ct. 109, 396 U.S. 816, 24 L.Ed.2d 68, reversed 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Constitutional Law 🔑 1490; Constitutional Law 🔑 1504

Although protections afforded by First and Fourteenth Amendments encompass spectrum of application with regard to freedom of speech that includes the less pure nonverbal freedom of speech, freedom of even the pure forms of speech is by no means absolute. U.S.C.A.Const. Amends. 1, 14. Bacheller v. State, 1968, 240 A.2d 623, 3 Md.App. 626, certiorari denied 251 Md. 747, certiorari granted 90 S.Ct. 109, 396 U.S. 816, 24 L.Ed.2d 68, reversed 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Constitutional Law 🔑 1490; Constitutional Law 🔑 4034

5. Obscenity

Regardless of how insulting, in the absence of any aggressive action constituting an assault or incitement, an obscene gesture by defendant, after he complied with officer's command for him to step back, furnished no basis upon which to arrest for failure to obey a lawful order made to prevent a disturbance to the public peace. Lamb v. State, 2001, 786 A.2d 783, 141 Md.App. 610. Arrest 🔑 63.4(15)

Defendant, who said "Fuck you" to police officer in response to unlawful police conduct, did not "profanely curse or swear" nor "use obscene language" such as would sustain his disorderly conduct conviction since the language did not import an imprecation of divine vengeance or imply divine condemnation or irreverance toward God or holy things nor was intended to, nor did excite, sexual desire in the police officer. Code 1957, Art. 27, § 121. Diehl v. State, 1982, 451 A.2d 115, 294 Md. 466, certiorari denied 103 S.Ct. 1798, 460 U.S. 1098, 76 L.Ed.2d 363. Obscenity 🔑 4

6. Fighting words

Defendant's conduct in saying "fuck you, cops" and "fuck you, motherfucking cops," and in continuing to shout obscenities at police officers as they escorted him from carnival, did not involve "fighting words" which would fall outside constitutional protection, and could not provide probable cause to arrest defendant for disorderly conduct; police officers were theoretically noninciteable, and no evidence suggested that officers were aroused by such language. Code 1957, Art. 27, § 123; U.S.C.A. Const.Amend. 1. Briggs v. State, 1992, 599 A.2d 1221, 90 Md.App. 60. Arrest 🔑 63.4(5); Constitutional Law 🔑 1814

7. Arrest

Under Maryland law, police officer had probable cause to arrest store patron for disorderly conduct, where patron failed to obey lawful order to leave marked-off crime scene in store's parking lot, even though officer allegedly issued order in rude, unprofessional, and overly aggressive manner. Carter v. Jess, 2001, 179 F.Supp.2d 534. Arrest 🔑 63.4(15)

In order to initiate prosecution for failure to obey a police officer's reasonable and lawful order to prevent a disturbance to the public peace, a police officer does not have to arrest an individual immediately after the first disobedience of a lawful order, nor does the officer have to arrest the individual at the scene. Spry v. State, 2007, 914 A.2d 1182, 396 Md. 682. Obstructing Justice 🔑 7

8. Permits

State police officers' order to pro-life demonstrators to obtain permit for demonstrating their pro-life stance through posters and signs on state highway or leave county was neither reasonable nor lawful, and thus charge of failure to obey reasonable and lawful order under Maryland law did not constitute basis for probable cause to arrest demonstrators; permit requirement did not exist, and order to leave county was clearly unconstitutional. Swagler v. Sheridan, 2011, 2011 WL 2746649. Arrest🔑 63.4(5); Arrest🔑 63.4(17)

Mayor and city council were without authority to grant permit allowing private individual to obstruct public street, thus denying public full use to which they were entitled, to gain access to beach and accordingly, order requiring that parking structure erected in bed of public street adjacent to oceanfront lot be abated as public nuisance was proper. Code 1957, art. 23A, § 2(23); art. 27, § 121. Caine v. Cantrell, 1977, 369 A.2d 56, 279 Md. 392. Municipal Corporations🔑 692

9. Jurisdiction

Prosecutions for violations of statute defining offense of disturbing the peace were within the exclusive original jurisdiction of the district court because offenses charged were statutory misdemeanors as to which maximum penalty authorized for confinement was less than three years. Code 1957, art. 27, § 121; Code, Courts and Judicial Proceedings, §§ 4-301, 4-302, 4-302(c). Howard v. State, 1976, 359 A.2d 568, 32 Md.App. 75. Criminal Law 🔑 94

Even if disturbing the peace charge against wife had been properly consolidated in the district court with disturbing the peace charges against her husband and even though husband was entitled to jury trial in circuit court on disturbing the peace charges because he was also charged with assault and battery and obstructing a police officer, district court was not thereby divested of its exclusive original jurisdiction over case against wife, in view of fact that wife was not entitled to jury trial for charge of disturbing the peace since penalty for that offense did not permit imprisonment for a period in excess of three months. Code 1957, art. 27, § 121; Code, Courts and Judicial Proceedings, §§ 4-302, 4-302(d, e); Maryland Rules, Rule 734. Howard v. State, 1976, 359 A.2d 568, 32 Md.App. 75. Criminal Law 🔑 102

Defendants charged with disturbing the peace could not deprive district court of its exclusive original jurisdiction over those cases merely by demanding jury trial as to those cases. Code, Courts and Judicial Proceedings, § 4-302(d)(1); Code 1957, art. 27, § 121. Howard v. State, 1976, 359 A.2d 568, 32 Md.App. 75. Criminal Law 🔑 102

Where defendant was charged with disturbing the peace, assault and battery, and hindering a police officer in the execution of the officer's duty, all charges arising out of same circumstances, and where defendant made timely demand for jury trial as to charges of assault and battery and hindering the police officer, circuit court properly acquired jurisdiction over all of the offenses with which defendant was charged, even though defendant would have been within exclusive jurisdiction of district court and would not have been entitled to jury trial if he had been charged merely with disturbing the peace. Code 1957, art. 27, § 121; Code, Courts and Judicial Proceedings, §§ 4-301, 4-302, 4-302(e). Howard v. State, 1976, 359 A.2d 568, 32 Md.App. 75. Criminal Law 🔑 102

9.5. Double jeopardy

Defendant's earlier acquittal, in District Court, on charges of disorderly conduct, possession of drugs (not marijuana), and possession of PCP (phencyclidine) with intent to distribute, relating to items found in search of vehicle parked outside defendant's home and defendant's encounter with police during the search, did not preclude, under double jeopardy principles, prosecution in Circuit Court pursuant to a subsequent indictment for possession of regulated firearms after conviction for disqualifying crime, possession of short-barreled shotgun, possession of bulletproof body armor after having previously been convicted of crime of violence or drug trafficking, and possession of drug paraphernalia, relating to items found in search of home; charges for which defendant was acquitted in District Court required proof of a fact for which the offenses charged in the subsequent indictment did not require proof. State v. Long, 2008, 954 A.2d 1083, 405 Md. 527. Double Jeopardy 🔑 146

9.6. Collateral estoppel

Acquittal of defendant, in District Court, on charges of disorderly conduct, possession of drugs (not marijuana), and possession of PCP (phencyclidine) with intent to distribute, based on District Court's determinations that search of vehicle parked outside of defendant's home was illegal, that defendant did not possess drugs found in vehicle because they were not within his reach, and that defendant's conduct towards police officers constituted mere curiosity regarding what officers were doing around the vehicle, did not collaterally estop the State from prosecuting defendant, in Circuit Court, for possession of regulated firearms after conviction for disqualifying crime, possession of short-barreled shotgun, possession of bulletproof body armor after having previously been convicted of crime of violence or drug trafficking, and possession of drug paraphernalia, relating to items found in search of defendant's home; District Court had not decided the legality of search of home, and acquittals were not based on State's failure to prove any fact that would be an essential element of a crime charged in Circuit Court. State v. Long, 2008, 954 A.2d 1083, 405 Md. 527. Judgment 🔑 751

10. Indictment and information

Indictment which charged that defendants "unlawfully did conspire, combine, confederate and agree together and with each other unlawfully, riotously and tumultuously to assemble and gather together to disturb the peace" would not be quashed as too vague. Code Supp.1947, art. 27, § 128. Winkler v. State, 1949, 69 A.2d 674, 194

Md. 1, certiorari denied 70 S.Ct. 621, 339 U.S. 919, 94 L.Ed. 1343. Indictment And Information 🔑 71.4(3)

Where state abandoned indictments charging defendants with engaging in interracial tennis matches in violation of rules of city park board and proceeded on subsequent indictments charging conspiracy to disturb the peace, proof that park board rule was illegal as depriving defendants of their civil rights under First and Fourteenth Amendments, if established, would not show that trial was so unfair as to amount to denial of due process under Fourteenth Amendment, so as to authorize Court of Appeals to examine evidence to determine its legal sufficiency to support the criminal charges. Code Supp.1947, art. 27, § 128; Const.Md. art. 15, § 5; U.S.C.A.Const. Amends. 1, 14. Winkler v. State, 1949, 69 A.2d 674, 194 Md. 1, certiorari denied 70 S.Ct. 621, 339 U.S. 919, 94 L.Ed. 1343. Criminal Law 🔑 260.11(5)

Trial court, by permitting state to proceed on subsequent indictments charging riot and conspiracy to promote disorder rather than on earlier indictments for violations of rules of city park board, did not abuse its discretion. Winkler v. State, 1949, 69 A.2d 674, 194 Md. 1, certiorari denied 70 S.Ct. 621, 339 U.S. 919, 94 L.Ed. 1343. Criminal Law 🔑 618

11. Joint or separate trials of codefendants

Wife, who was charged with disturbing the peace, had no absolute right, constitutional or otherwise, to be tried jointly with her husband, who was charged with disturbing the peace, assault and battery, and hindering a police officer in the execution of the officer's duty and whose voluntary action divested the district court, which had exclusive original jurisdiction, of its jurisdiction over him. Code 1957, art. 27, § 121; Code, Courts and Judicial Proceedings, §§ 4-301, 4-302. Howard v. State, 1976, 359 A.2d 568, 32 Md.App. 75. Criminal Law 🔑 622.7(1)

12. Admissibility of evidence

Fact that defendants had entered recruiting station demanding that posters protesting policy in Vietnam conflict be displayed inside and had been removed by United States Marshal was proper and relevant background to charge of disorderly conduct arising from defendants' refusal to leave sidewalk in front of recruiting station when thrice told to leave by police officer. Code 1957, art. 27, § 123. Bacheller v. State, 1968, 240 A.2d 623, 3 Md.App. 626, certiorari denied 251 Md. 747, certiorari granted 90 S.Ct. 109, 396 U.S. 816, 24 L.Ed.2d 68, reversed 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Criminal Law 🔑 345

13. Weight and sufficiency of evidence

Findings of disorderly conduct as to each charged juvenile were supported by sufficient evidence, in delinquency proceeding arising from altercation on mass transit bus; evidence established that a group of juveniles conspired to assault one or both victims on the bus, eyewitness saw bus "rocking" violently, bus driver reported that a group of juveniles on the bus "went crazy" and that a "riot broke out," and interior of bus was damaged during the attacks. In re Lavar D., 2009, 985 A.2d 102, 189 Md.App. 526, certiorari denied 995 A.2d 297, 414 Md. 331. Infants🔑 2640(1)

Evidence did not support defendant's conviction for willful failure to obey the lawful order of an officer; although officer ordered defendant to step away, he never issued an order for defendant to leave the scene, defendant withdrew from the public sidewalk to his parent's property, there was no evidence of a gathering crowd during the confrontation, and hence, there could be neither a disturbance of the public peace nor an obstruction of the free passage of pedestrians or others in a public place or on a **public conveyance**. Lamb v. State, 2001, 786 A.2d 783, 141 Md.App. 610. Obstructing Justice🔑 16

Circuit court did not have sufficient evidentiary basis for finding the probationer had made willful disturbance by making loud and unseemly noise, within meaning of disorderly conduct statute, and thus evidence did not support finding that probationer had violated condition of probation; evidence did not show how loudly probationer was speaking, did not show whether her speech or actions were disturbing anybody, and officer's testimony only described probationer as victim of disorderly conduct, not as perpetrator of it. Code 1957, Art. 27, § 121. Baynard v. State, 1990, 569 A.2d 652, 318 Md. 531. Sentencing And Punishment🔑 2021

Statement of officer that juvenile was "using profane language" was a conclusion, and in absence of evidence setting out the language the officer concluded was profane there was not enough for trier of fact to determine that the language was "profane" within ambit of disorderly conduct statutes. Code 1957, art. 27, §§ 121-123. In re Nawrocki, 1972, 289 A.2d 846, 15 Md.App. 252, certiorari denied 266 Md. 741. Disorderly Conduct🔑 148

If evidence was sufficient to show that juvenile was guilty of the crime of disorderly conduct, this alone would support the finding of delinquency whether or not he resisted arrest, but if the evidence was not sufficient to establish that juvenile was guilty of disorderly conduct, then he would not be guilty of resisting arrest because his arrest would be illegal. Code 1957, art. 27, §§ 121-123. In re Nawrocki, 1972, 289 A.2d 846, 15 Md.App. 252, certiorari denied 266 Md. 741. Infants🔑 2640(1); Obstructing Justice🔑 3

Evidence was sufficient to support defendant's conviction of disorderly conduct. Code 1957, art. 27, § 123. McIntyre v. State, 1967, 232 A.2d 279, 1 Md.App. 586, certiorari denied 248 Md. 733. Disorderly Conduct🔑 148

Finding that "sit down" orders which defendant admittedly refused to obey were meant to preserve public peace, as required to support defendant's conviction under Maryland law of willfully failing to obey a reasonable and lawful order issued by law enforcement officer to prevent disturbance to public peace, was sufficiently supported by evidence; incident occurred in public area of military base, in area through which members of public were passing, and where defendant was engaged in excited exchange with officers issuing orders. U.S. v. Lee, 2011, 432 Fed.Appx. 232, 2011 WL 2109909, Unreported. Disorderly Conduct🔑 132

14. Instructions

In prosecution of defendant for assaulting officer in connection with officer's unlawful arrest of juveniles for possessing alcohol, trial court, in addition to providing the elements of assault, should have instructed jury, in weighing evidence, to determine whether the initial force applied to prevent the arrests of juveniles was reasonable, and court should then have instructed the jury to determine whether the force employed by defendant was unreasonable, i.e., more than the force necessary to repel officer's attempt to grab him and, thereafter, to subdue him. Lamb v. State, 2001, 786 A.2d 783, 141 Md.App. 610. Assault And Battery 🔑 96(2)

Instruction requested by defendant, in prosecution for, inter alia, disturbing neighborhood and for acting in a disorderly manner, stating, inter alia, that jury must consider character testimony offered by defendant with all other evidence offered, and that the character testimony could in and of itself create doubt in minds of jury sufficient to cause it to find defendant not guilty of each and every count, was properly refused where such testimony was not relevant to demonstrate that it was unlikely that defendant would commit crimes with which he was charged. Code 1957, art. 27, §§ 121, 123, 123(c). Hallengren v. State, 1972, 286 A.2d 213, 14 Md.App. 43. Criminal Law 🔑 776(5)

Where evidence clearly established that defendants' arrests and charges of disorderly conduct resulted from their refusal to cease obstruction of sidewalk and resultant public disturbance, refusal to instruct jury that defendants had constitutional right to express their political beliefs and that jury could not convict on basis of disagreement with defendants' expressed views did not violate defendants' rights under First and Fourteenth Amendments. U.S.C.A.Const. Amends. 1, 14. Bacheller v. State, 1968, 240 A.2d 623, 3 Md.App. 626, certiorari denied 251 Md. 747, certiorari granted 90 S.Ct. 109, 396 U.S. 816, 24 L.Ed.2d 68, reversed 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Constitutional Law 🔑 4637

15. Verdict

Acquittal of defendant on charge of assault and inciting a riot was not inconsistent with conviction on charges of, inter alia, disturbing neighborhood by loud and unseemly noises, and of acting in a disorderly manner to the disturbance of the public peace upon a designated public street. Code 1957, art. 27, §§ 121, 123. Hallengren v. State, 1972, 286 A.2d 213, 14 Md.App. 43. Criminal Law 🔑 878(4)

An acquittal on count of indictment charging disorderly conduct does not necessarily invalidate conviction of assault charged in another count of same indictment. Williams v. State, 1954, 102 A.2d 714, 204 Md. 55. Criminal Law 🔑 878(3)

Where prosecutions under two indictments charging respectively disturbance of public peace and disorderly conduct, and assault, were tried together but not formally consolidated and docket entries in each case were separate, the cases were so distinct that there should be separate verdicts as to each indictment or at least a verdict touching upon each indictment. Glickman v. State, 1948, 60 A.2d 216, 190 Md. 516. Criminal Law 🔑 876.5

16. Review

Where it could not be determined whether convictions for disorderly conduct rested on constitutional or on unconstitutional grounds, convictions must be set aside. U.S.C.A.Const. Amends. 1, 14. Bachellar v. Maryland, 1970, 90 S.Ct. 1312, 397 U.S. 564, 25 L.Ed.2d 570, 52 O.O.2d 200. Criminal Law 🔑 1186.1

Trial court's finding on defendant's motion for judgment of acquittal in prosecution for disorderly conduct that police officer's orders to defendant were aimed, in the main, at volume of defendant's speech rather than its content was not clearly erroneous based on evidence in the record and thus would be accorded deference on appeal. Polk v. State, 2003, 835 A.2d 575, 378 Md. 1, certiorari denied 124 S.Ct. 1691, 541 U.S. 951, 158 L.Ed.2d 382. Disorderly Conduct 🔑 149

Where defendant charged with disorderly conduct and disturbing public peace asked for a jury trial upon appearance before a justice of the peace after arrest upon a warrant, and was thereafter convicted by criminal court of Baltimore City, criminal court was not acting as an appeal court of special limited jurisdiction, but as a trial court, and defendant was entitled to appeal from its decision to the Court of Appeals. Code Pub.Loc.Laws 1930, art. 4, §§ 632, 632A; Code 1939, art. 5, §§ 2, 86; art. 27, §§ 128, 131; art. 52, § 13; Code Supp.1943, art. 52, §§ 13, 13A, as amended by Laws 1945, c. 845. Brack v. State, 1947, 51 A.2d 171, 187 Md. 542. Criminal Law 🔑 1022

MD Code, Criminal Law, § 10-**201**, MD CRIM LAW § 10-**201**

The statutes and Constitution are current through all chapters of the 2012 Regular Session and 2012 First Special Session of the General Assembly, effective through July 1, 2012.

END OF DOCUMENT

C

Michigan Compiled Laws Annotated Currentness
Chapter 117. Home Rule Cities
Home Rule City Act (Refs & Annos)
→→ **117.3. Mandatory charter provisions**

Sec. 3. Each city charter shall provide for all of the following:

(a) The election of a mayor, who shall be the chief executive officer of the city, and of a body vested with legislative power, and for the election or appointment of a clerk, a treasurer, an assessor or board of assessors, a board of review, and other officers considered necessary. The city charter may provide for the selection of the mayor by the legislative body. Elections may be by a partisan, nonpartisan, or preferential ballot, or by any other legal method of voting. Notwithstanding another law or charter provision to the contrary, a city having a 1970 official population of more than 150,000, whose charter provides for terms of office of less than 4 years, and in which the term of office for the mayor and the governing body are of the same length, may provide by **ordinance** for a term of office of up to 4 years for mayor and other elected city officials. The **ordinance** shall provide that the **ordinance** shall take effect 60 days after it is enacted unless within the 60 days a petition is submitted to the city clerk signed by not less than 10% of the registered electors of the city requesting that the question of approval of the **ordinance** be submitted to the electors at the next regular election or a special election called for the purpose of approving or disapproving the **ordinance**.

(b) The nomination of elective officers by partisan or nonpartisan primary, by petition, or by convention.

(c) The time, manner, and means of holding elections and the registration of electors, subject to section 26 [FN1] and other applicable requirements of law.

(d) The qualifications, duties, and compensation of the city's officers. If the city has an appointed chief administrative officer, the legislative body of the city may enter into an employment contract with the chief administrative officer extending beyond the terms of the members of the legislative body unless the employment contract is prohibited by the city charter. An employment contract with a chief administrative officer shall be in writing and shall specify the compensation to be paid to the chief administrative officer, any procedure for changing the compensation, any fringe benefits, and other conditions of employment. The contract shall state if the chief administrative officer serves at the pleasure of the legislative body, and the contract may provide for severance pay or other benefits in the event the chief administrative officer's employment is terminated at the pleasure of the legislative body.

(e) The establishment of 1 or more wards, and if the members of the city's legislative body are chosen by wards, for equal representation for each ward in the legislative body.

(f) That the subjects of taxation for municipal purposes are the same as for state, county, and school purposes under the general law.

(g) The annual laying and collecting taxes in a sum, except as otherwise provided by law, not to exceed 2% of the taxable value of the real and personal property in the city. Unless the charter provides for a different tax rate limitation, the governing body of a city may levy and collect taxes for municipal purposes in a sum not to exceed 1% of the taxable value of the real and personal property in the city. As used in this subdivision, "taxable value" is that value determined under section 27a of the general property tax act, 1893 PA 206, MCL 211.27a.

(h) An annual appropriation of money for municipal purposes.

(i) The levy, collection, and return of state, county, and school taxes in conformance with the general laws of this state, except that the preparation of the assessment roll, the meeting of the board of review, and the confirmation of the assessment roll may be at the times provided in the city charter.

(j) The public peace and health and for the safety of persons and property. In providing for the public peace, health, and safety, a city may expend funds or enter into contracts with a private organization, the federal or state government, a county, village, or township, or another city for services considered necessary by the legislative body. Public peace, health, and safety services may include the operation of child guidance and community mental health clinics, the prevention, counseling, and treatment of developmental disabilities, the prevention of drug abuse, and the counseling and treatment of drug abusers.

(k) Adopting, continuing, amending, and repealing the city **ordinances** and for the publication of each **ordinance** before it becomes operative. Whether or not provided in its charter, instead of publishing a true copy of an **ordinance** before it becomes operative, the city may publish a summary of the **ordinance**. If the city publishes a summary of the **ordinance**, the city shall include in the publication the designation of a location in the city where a true copy of the **ordinance** can be inspected or obtained. A charter provision to the contrary notwithstanding, a city may adopt an **ordinance** punishable by imprisonment for not more than 93 days or a fine of not more than $500.00, or both, if the violation substantially corresponds to a violation of state law that is a misdemeanor for which the maximum period of imprisonment is 93 days. Whether or not provided in its charter, a city may adopt a provision of a state statute for which the maximum period of imprisonment is 93 days or the **Michigan** vehicle code, 1949 PA 300, MCL 257.1 to 257.923. Except as otherwise provided under the Stille-DeRossett-Hale single state construction code act, 1972 PA 230, MCL 125.1501 to 125.1531, a city may adopt a law, code, or rule that has been promulgated and adopted by an authorized agency of this state pertaining to fire, fire hazards, fire prevention, or fire waste, and a fire prevention code, plumbing code, heating code, electrical code, building code, refrigeration machinery code, piping code, boiler code, boiler operation code, elevator machinery code, an international property maintenance code, or a code pertaining to flammable liquids and gases or hazardous chemicals, that has been promulgated or adopted by this state, by a department, board, or other agency of this state, or by an organization or association that is organized and conducted for the purpose of developing the code, by reference to the law, code, or rule in an adopting **ordinance** and without publishing the law, code, or rule in full. The law, code, or rule shall be clearly identified in the **ordinance** and its purpose shall be published with the adopting **ordinance**. Printed copies of the law, code, or rule shall be kept in the office of the city clerk, available for inspection by, and distribution to, the public at all times. The publication shall contain a notice stating that a complete copy of the law, code, or rule is made available to the public at the office of the city clerk in compliance with state law requiring that records of public bodies be made available to the general public. Except as otherwise provided in this subdivision, a city shall not enforce a provision adopted by reference for which the maximum period of imprisonment is greater than 93 days. A city may adopt section 625(1)(c) of the **Michigan** vehicle code, 1949 PA 300, MCL 257.625, by reference in an adopting **ordinance** and shall provide that a violation of that **ordinance** is punishable by 1 or more of the following:

(*i*) Community service for not more than 360 hours.

(*ii*) Imprisonment for not more than 180 days.

(*iii*) A fine of not less than $200.00 or more than $700.00.

(*l*) That the business of the legislative body shall be conducted at a public meeting held in compliance with the open meetings act, 1976 PA 267, MCL 15.261 to 15.275. All records of the municipality shall be made available to the general public in compliance with the freedom of information act, 1976 PA 442, MCL 15.231 to 15.246.

(m) Keeping in the English language a written or printed journal of each session of the legislative body.

(n) A system of accounts that conforms to a uniform system of accounts as required by law.

CREDIT(S)

Amended by P.A.1991, No. 182, § 1, Imd. Eff. Dec. 27, 1991; P.A.1993, No. 207, § 1, Imd. Eff. Oct. 19, 1993; P.A.1999, No. 256, Imd. Eff. Dec. 28, 1999; P.A.1999, No. 260, Eff. Dec. 29, 1999; P.A.2002, No. 201, Imd. Eff. April 29, 2002; P.A.2003, No. 303, Eff. Jan. 1, 2005; P.A.2004, No. 541, Imd. Eff. Jan. 3, 2005; P.A.2012, No. 7, Imd. Eff. Feb. 15, 2012.

[FN1] M.C.L.A. § 117.26.

HISTORICAL AND STATUTORY NOTES

Source:

P.A.1909, No. 279, § 3, Eff. Sept. 1, 1909.

C.L.1915, § 3006.

P.A.1929, No. 126, Eff. Aug. 28, 1929.

C.L.1929, § 2230.

P.A.1947, No. 344, Eff. Oct. 11, 1947.

P.A.1948, 1st Ex.Sess., No. 44, Eff. Aug. 20, 1948.

C.L.1948, § 117.3.

P.A.1949, No. 43, § 1, Eff. Sept. 23, 1949.

P.A.1960, No. 14, § 1, Imd. Eff. April 13, 1960.

P.A.1967, No. 43, § 1, Eff. Nov. 2, 1967.

C.L.1970, § 117.3.

P.A.1973, No. 81, § 1, Imd. Eff. July 31, 1973.

P.A.1977, No. 204, § 1, Imd. Eff. Nov. 17, 1977.

P.A.1978, No. 241, § 1, Imd. Eff. June 15, 1978.

P.A.1979, No. 59, § 1, Imd. Eff. July 18, 1979.

The 1991 amendment, in subd. (g), in the second sentence inserted "the municipal finance act,"; in subd. (k), inserted the second and third sentences, and in the fourth sentence substituted "that have been" for "which have been", "that has been" for "which have been", and "that is" for "which is"; in subd. (*l*), in the first sentence inserted "the open meetings act,", and in the second sentence inserted "the freedom of information act,"; and, in subd. (n), substituted "that" for "which".

The 1993 amendment, in subd. (a), in the second sentence substituted "The city charter may provide" for "Provision may be made", and in the fourth sentence deleted "and" following "more than 150,000,", inserted "by **ordinance**", and deleted ", by **ordinance**" following "elected city officials"; in subd. (d), added the second to fourth sentences; in subd. (e), substituted "are chosen" for "be chosen"; in subd. (j), in the second sentence inserted "or" preceding "township"; in subd. (k), in the fourth sentence deleted "or" preceding "by a department"; and, in subd. (l), in the first sentence substituted "business that" for "business which".

P.A.1999, No. 260, enacting § 1, provides:

"Enacting section 1. This amendatory act does not take effect unless all of the following bills of the 90th Legislature are enacted into law:

"(a) Senate Bill No. 831.

"(b) Senate Bill No. 832.

"(c) Senate Bill No. 833.

"(d) Senate Bill No. 855.

"(e) Senate Bill No. 856."

Senate Bill Nos. 831, 832, and 833, were enacted as P.A.1999, Nos. 258, 257, and 259, respectively, and were approved and filed December 28, 1999; Senate Bill Nos. 855 and 856, were enacted as P.A.1999, Nos. 266 and 267, respectively, and were approved December 28, 1999 and filed December 29, 1999.

P.A.1999, No. 260, was ordered to take immediate effect, and was approved and filed December 28, 1999.

P.A.2003, No. 303, enacting §§ 1 and 2, provide:

"Enacting section 1. This amendatory act takes effect January 1, 2005.

"Enacting section 2. This amendatory act does not take effect unless all of the following bills of the 92nd Legislature are enacted into law:

"(a) Senate Bill No. 877.

"(b) House Bill No. 4820.

"(c) House Bill No. 4822.

"(d) House Bill No. 4823.

"(e) House Bill No. 4824.

"(f) House Bill No. 4826.

"(g) House Bill No. 4827.

"(h) House Bill No. 4828."

Senate Bill No. 877 was enacted as P.A.2003, No. 298, and was approved and filed January 8, 2004, eff. January 1, 2005.

House Bill No. 4820 was enacted as P.A.2003, No. 299, and was approved and filed January 8, 2004, eff. January 1, 2005.

House Bill No. 4822 was enacted as P.A.2003, No. 300, and was approved and filed January 8, 2004, eff. January 1, 2005.

House Bill No. 4823 was enacted as P.A.2003, No. 301, and was approved and filed January 8, 2004, eff. January 1, 2005.

House Bill No. 4824 was enacted as P.A.2003, No. 302, and was approved and filed January 8, 2004.

House Bill No. 4826 was enacted as P.A.2003, No. 304, and was approved and filed January 8, 2004, eff. January 1, 2005.

House Bill No. 4827 was enacted as P.A.2003, No. 305, and was approved and filed January 8, 2004, eff. January 1, 2005.

House Bill No. 4828 was enacted as P.A.2003, No. 306, and was approved and filed January 8, 2004, eff. January 1, 2005.

P.A.2003, No. 303, was not ordered to take immediate effect, and was approved and filed January 8, 2004.

CONSTITUTIONAL PROVISIONS

Article 7, § 21, provides:

"The legislature shall provide by general laws for the incorporation of cities and villages. Such laws shall limit their rate of ad valorem property taxation for municipal purposes, and restrict the powers of cities and villages to borrow money and contract debts. Each city and village is granted power to levy other taxes for public purposes, subject to limitations and prohibitions provided by this constitution or by law."

Article 7, § 22, provides:

"Under general laws the electors of each city and village shall have the power and authority to frame, adopt and amend its charter, and to amend an existing charter of the city or village heretofore granted or enacted by the legislature for the government of the city or village. Each such city and village shall have power to adopt resolutions and **ordinances** relating to its municipal concerns, property and government, subject to the constitution and law. No enumeration of powers granted to cities and villages in this constitution shall limit or restrict the general grant of authority conferred by this section."

CROSS REFERENCES

Amendment of charter, procedure, see § 117.21 et seq.
Apportionment of wards, see § 117.27a.
Charter townships, see § 42.1 et seq.
City property purchased on installment plan, see § 123.721 et seq.
Compensation,
  Fourth class city officers, see § 87.1 et seq.
  Village officers, see § 64.21.
Division of wards into precincts, see § 168.656.
Elections,
  City offices, see § 168.321 et seq.
  Rules and procedures, see Const. Art. 2, § 1 et seq.
Liberal construction of law concerning cities, see Const. Art. 7, § 34.
Loan of credit, see Const. Art. 7, § 26.
Municipal joint endeavors, property tax levies, voting, limitations, see § 124.117.
Prohibited taxes, see § 141.91.
Rate of taxation, see § 117.5.
Reproduction of records, see § 691.1101 et seq.
Uniform city income tax **ordinance**, see § 141.601 et seq.

LAW REVIEW AND JOURNAL COMMENTARIES

Administrative processes and review in tax matters. Benjamin Krawood, 11 Wayne L.Rev. 512 (1965).

Commercial transaction and contracts: Annual survey of **Michigan** law June 2002-May 2003. Geoffrey C. Rapp, 50 Wayne L.Rev. 383 (2004).

Constitutional validity of curfew **ordinance**. 55 Mich.L.Rev. 1026 (1957).

Delegation of municipality's power to patrol highways. 54 Mich.L.Rev. 1016 (1956).

Due process; knowledge of law required for conviction under criminal registration **ordinance**. 56 Mich.L.Rev. 1008 (1958).

Elections, cities and villages, at-large elections, representation of minorities. Leon H. Weaver, 49 U.Det.J.Urb.L. 134 (1971).

Environmental Law: Annual Survey of **Michigan** Law 1996. Leonard F. Charla, 43 Wayne L.Rev. 909 (1997).

Government law: Annual survey of **Michigan** law June 2002-May 2003. Michael P. Doerr, 50 Wayne L.Rev. 637 (2004).

The handbill **ordinances**. James K. Lindsay, 39 Mich.L.Rev. 561 (1941).

Home rule legislation. Robert E. Jacobson. 14 Mich.L.Rev. 281 (1916).

Local government: Annual survey of **Michigan** law 1974. Jerold Lax, 21 Wayne L.Rev. 577 (1975).

Local government: Public transportation. Solomon Bienenfeld, 13 Wayne L.Rev. 241 (1966).

Residency requirement for municipal employees. Avern Cohn and Norman Hyman, 19 Wayne L.Rev. 522 (1973).

Status of city manager--executive or legislative? 38 Mich.L.Rev. 261 (1939).

Use of standard of average assessment levels affecting uniformity of treatment. Burns Stanley and Edward Tunstall, 13 Wayne L.Rev. 146 (1966).

LIBRARY REFERENCES

Municipal Corporations 🔑 40, 64.5, 65, 67(1), 73, 105, 110, 129, 149(2), 228, 885.
Westlaw Topic No. 268.
C.J.S. Municipal Corporations §§ 122, 140 to 141, 143, 180 to 184, 190, 247 to 251, 277 to 284, 331, 350 to 351, 353 to 354, 361 to 363, 367, 902, 1628.

RESEARCH REFERENCES

ALR Library

35 ALR 883, Power of City Under Freeholders' Charter Over Taxes.

163 ALR 1435, Validity and Construction of Legislation Conferring Personal Immunity on Public Officers or Employees for Acts in Course of Duty.

106 ALR 1202, Home Rule Charter as Affecting Power of Legislature in Respect of Municipal Taxation.

53 ALR 41, Personal Liability of Peace Officer or His Bond for Negligence Causing Damage to Property.

Encyclopedias

Mich. Civ. Jur. Constitutional Law § 80, Police and Fire Departments.

Mich. Civ. Jur. Fires § 2, Authority of Municipalities.

Mich. Civ. Jur. Municipal Corporations § 9, Home-Rule or Freeholders' Charters.

Mich. Civ. Jur. Municipal Corporations § 23, Wards or Other Divisions of Municipalities.

Mich. Civ. Jur. Municipal Corporations § 51, Councilmen, Aldermen, Commissioners, and Supervisors.

Mich. Civ. Jur. Municipal Corporations § 177, Minutes and Records--Generally.

Mich. Civ. Jur. Municipal Corporations § 194, Publication and Notice.

Mich. Civ. Jur. Municipal Corporations § 232, Powers Under Home Rule Act.

Mich. Civ. Jur. Municipal Corporations § 274, Fixing Penalties and Punishment.

Mich. Civ. Jur. Municipal Corporations § 293, Fire Protection.

Mich. Civ. Jur. Municipal Corporations § 337, Fiscal Year.

Mich. Civ. Jur. Taxes § 28, Discretion of Municipality.

Mich. Civ. Jur. Taxes § 184, Municipal Tax.

Mich. Civ. Jur. Taxes § 196, Statutory Provisions.

Treatises and Practice Aids

Gillespie MI Crim. Law & Proc. § 116:1, Authority of Municipalities.

NOTES OF DECISIONS

1. In general

Courts will give rational construction to city charters and language employed will be given its plain meaning, and no words will be treated as surplusage. City of Sterling Heights v. General Emp. Civil Service Commission of City of Sterling Heights (1978) 265 N.W.2d 88, 81 Mich.App. 221. Municipal Corporations 🔑 58

"Permissible charter provisions" within meaning of §§ 117.4i and 117.4j of the Home Rule Cities Act are those subjects that city may, if it desires, include in its charter, and are to be distinguished from mandatory charter provisions such as those required by § 117.3. Detroit Police Officers Ass'n v. City of Detroit (1974) 214 N.W.2d 803, 391 **Mich**. 44. Municipal Corporations 🔑 65

City's past construction of provision of this section limiting tax revenues as being an all-inclusive limitation on aggregate tax revenues did not preclude Supreme Court from giving section a different construction. Dooley v. City of Detroit (1963) 121 N.W.2d 724, 370 **Mich**. 194. Statutes 🔑 219(10)

The word "qualifications" as used in this section making it mandatory that each city charter provide for qualifications of its officers, includes qualifications to be elected to office and also qualifications to hold the office. Doyle v. City of Dearborn (1963) 121 N.W.2d 473, 370 **Mich**. 236. Municipal Corporations 🔑 138

C.L.1929, § 2228 et seq., recognized power of city to levy taxes, and contemplated power to make all reasonable provisions for collection thereof. City of Detroit v. Safety Inv. Corp. (1939) 285 N.W. 42, 288 **Mich**. 511. Municipal Corporations 🔑 978(1)

Under P.A.1909, No. 279, which provided for home rule by municipal corporations, there was a general grant of rights and powers subject only to certain enumerated restrictions instead of, as formerly, a grant of enumerated rights and powers definitely specified. City of Pontiac v. Ducharme (1936) 270 N.W. 754, 278 **Mich**. 474. Municipal Corporations 🔑 65

Provisions of Home Rule Act (P.A.1909, No. 279) designating what each city charter shall provide were mandatory. City Commission of Jackson v. Hirschman (1931) 235 N.W. 265, 253 **Mich**. 596. Municipal Corporations 🔑 11

Home Rule Act (P.A.1909, No. 279) should have been construed liberally and in a home rule spirit. City Commission of Jackson v. Hirschman (1931) 235 N.W. 265, 253 **Mich**. 596. Municipal Corporations 🔑 65

2. Federal antitrust laws

Anticompetitive effects were the logical and foreseeable result of city's broad authority under **Michigan** Home Rule City Act, and **Michigan** Constitution, to bid out public contracts for maintenance of city prisons, and thus, city was immune from federal antitrust laws, pursuant to state action doctrine, with respect to Sherman Act claims asserted by unsuccessful bidders on contract to provide pay telephone service in city prison. **Michigan** Paytel Joint Venture v. City of Detroit, C.A.6 (**Mich**.)2002, 287 F.3d 527. Antitrust And Trade Regulation 🔑 903

3. Charters--In general

Charter restriction making it unlawful for any elective official to hold any position on another public payroll did not offend either the state constitution or § 117.3(d) and was valid. Doyle v. City of Dearborn (1963) 121 N.W.2d 473, 370 **Mich**. 236. Municipal Corporations 🔑 124(3)

Charter provisions of municipal corporations come into being by legislative enactment as well as by adoption by local electors. Council of City of Saginaw v. Board of Trustees of Policemen and Firemen Retirement System of City of Saginaw (1948) 32 N.W.2d 899, 321 **Mich**. 641. Municipal Corporations 🔑 8

Charter of the city or village is subject to the Constitution and general laws of this state. City of Hazel Park v. Municipal Finance Commission (1947) 27 N.W.2d 106, 317 **Mich**. 582.

Under provision in charter of home rule city requiring all municipal contracts involving an expenditure of $500 or more to be let upon competitive bidding, a proposed contract for purchase of electricity by city could be awarded only upon competitive bids therefor. Hunt v. Fenlon (1946) 21 N.W.2d 906, 313 **Mich**. 644. Municipal Corporations 🔑 236

Provision in home rule city charter that, subject to the limitations of the general laws, the city should have power to regulate the gas rate in the city did not give city power to fix ex parte gas rate, since such power was vested in State Public Service Commission under general law which supplanted any contravening charter provision. City of Jackson v. Consumers Power Co. (1945) 20 N.W.2d 265, 312 **Mich**. 437. Gas 🔑 14.2

Provision of proposed home rule charter for election of officers at special charter election was constitutional and valid as against contention that it provided for election of persons to office before it had been determined that offices should be created. Streat v. Vermilya (1934) 255 N.W. 604, 268 **Mich.** 1. Municipal Corporations 🔑 124(2)

Provision in city charter amendment setting fiscal year ahead six months, providing for temporary tax levy to bridge six months' gap, did not render charter amendment invalid. City Commission of Jackson v. Hirschman (1931) 235 N.W. 265, 253 **Mich.** 596. Municipal Corporations 🔑 46

In home rule city adopting charter under § 117.1 et seq., charter which prescribed filing of petitions as method for nomination of candidates was controlling, and, without charter amendment, there would be no authority for holding either a primary election or party caucus. Op.Atty.Gen.1957-58, No. 3216, p. 61.

4. ---- Nature of charters

A city "charter" is the "organic law" of the city and is considered as other organic acts are considered. Sykes v. City of Battle Creek (1939) 286 N.W. 117, 288 **Mich.** 660. Municipal Corporations 🔑 8

Within range of Constitution and Home Rule Act (P.A.1909, No. 279) for cities, electors might have made "charter," which was organic law of city, and to have been considered as other organic acts were considered. Streat v. Vermilya (1934) 255 N.W. 604, 268 **Mich.** 1. Municipal Corporations 🔑 44

A city charter defines its municipal rights and obligations not otherwise legally granted or imposed. Common Council of City of Jackson v. Harrington (1910) 125 N.W. 383, 160 **Mich.** 550. Municipal Corporations 🔑 8

A city charter and powers it assumes to grant, so far as it is not plainly unconstitutional, must be construed as conferring only such power over the subjects referred to as will enable the city to keep order, and suppress mischief, in accordance with the limitations and conditions required by the rights of the people themselves, as secured by the principles of law, which cannot be less careful of private rights under a Constitution than under the common law. In re Frazee (1886) 30 N.W. 72, 63 **Mich.** 396, 6 Am.St.Rep. 310. Municipal Corporations 🔑 589

5. ---- Amendment, charters

Where petitions for special election to amend city charter are in proper form, they are presumed to be valid and to have been completed in accordance with circulator's affidavit, but, on showing by city clerk of sufficient magnitude tending to rebut presumption, presumption will disappear, and compliance of petitions with § 117.24 must be affirmatively shown. Grosse Pointe Farms Fire Fighters Ass'n v. Caputo (1968) 157 N.W.2d 695, 11 Mich.App. 112. Municipal Corporations 🔑 46

Amendment to charter of City of Dearborn for which voters voted at election, which provided for election of a Municipal Judge and Associate Municipal Judge for six-year terms, and which authorized salary for Associate Municipal Judge which was less than salary previously provided for each of two Municipal Judges provided for by charter, provided for a bona fide abolition of one Municipal Judge to take effect immediately upon passage of such amendment rather than unconstitutional reduction in salary, term, duties and authority of office of Municipal Judge. Millard v. Guy (1952) 55 N.W.2d 210, 334 **Mich.** 694. Judges 🔑 2; Judges 🔑 22(7)

6. ---- Construction, charters

If a charter provision is ambiguous it must still be interpreted in a manner consistent with reason and with a goal of determining the purpose and intent of the framers and public. Detroit Fire Fighters Ass'n v. City of Detroit (1983) 339 N.W.2d 230, 127 Mich.App. 673. Municipal Corporations 🔑 58

When language of a charter provision is unambiguous and specific it is controlling; in such a case, it is presumed that framers of charter, and people of city involved, intended that provision be construed as it reads. Detroit Fire Fighters Ass'n v. City of Detroit (1983) 339 N.W.2d 230, 127 Mich.App. 673. Municipal Corporations 🔑 58

In construing provisions of the fundamental law of the city, the general rules recognized in cases involving the interpretation of statutes are applicable. Brady v. City of Detroit (1958) 91 N.W.2d 257, 353 **Mich.** 243. Municipal Corporations 🔑 58

In construing provisions of the fundamental law of the city, the inquiry is directed to ascertaining the intention of the people in the adoption of their charter. Brady v. City of Detroit (1958) 91 N.W.2d 257, 353 **Mich.** 243. Municipal Corporations 🔑 58

Provisions of the charter pertaining to a given subject must be construed together and, if possible, harmonized, and it may not be assumed that the adoption of conflicting provisions was intended. Brady v. City of Detroit (1958) 91 N.W.2d 257, 353 **Mich.** 243. Municipal Corporations 🔑 58

Presumption existed that charter provisions were drafted with care. Utica State Sav. Bank v. Village of Oak Park (1937) 273 N.W. 271, 279 **Mich.** 568. Municipal Corporations 🔑 58

Rule or doctrine of ejusdem generis is only a rule of construction to be used as an aid in ascertaining the intent of the enacting body, regardless of whether it be a statutory provision or a charter provision. Utica State Sav. Bank v. Village of Oak Park (1937) 273 N.W. 271, 279 **Mich.** 568. Municipal Corporations 🔑 58; Statutes 🔑 194

If the language used is plain, the rule of ejusdem generis cannot be applied in construing city charter. Utica State Sav. Bank v. Village of Oak Park (1937) 273 N.W. 271, 279 **Mich.** 568. Municipal Corporations 🔑 58

City charter must be construed as intended to create corporation resembling general class into which it is introduced. Veldman v. City of Grand Rapids (1936) 265 N.W. 790, 275 **Mich.** 100. Municipal Corporations 🔑 58

Municipal charter should be given force according to language and purpose, and exceptions should be permitted only on sound distinctions. Northrup v. City of Jackson (1935) 262 N.W. 641, 273 **Mich.** 20. Municipal Corporations 🔑 58

A charter must be considered in its entirety. City of Lansing v. Jenison (1918) 167 N.W. 947, 201 **Mich.** 491. Municipal Corporations 🔑 58

It is not in the power of the Legislature to deprive any of the people of the enjoyment of equal privileges under the law, or to give cities any tyrannical powers; all charters, laws, and regulations, to be valid for any purpose, must be capable of construction, and must be construed in conformity to constitutional principles, and in harmony with the general laws of the land; and any by-law which violates any of the recognized principles of legal and equal rights is necessarily void so far as it does so, and void entirely if it cannot be reasonably applied according to its terms. In re Frazee (1886) 30 N.W. 72, 63 **Mich.** 396, 6 Am.St.Rep. 310. Municipal Corporations 🔑 111(1)

City charters must be rationally construed as intended to create corporations which shall resemble in their essential character the class into which they are introduced. Torrent v. City of Muskegon (1881) 10 N.W. 132, 47 **Mich.** 115, 41 Am.Rep. 715. Municipal Corporations 🔑 58

7. ---- Conflicting charter provisions

Where two provisions of city charter apparently conflict, they will be construed so as to give effect to both, if that can be done without violence to language used. Hanley v. Ingalls (1926) 209 N.W. 920, 235 **Mich.** 700. Municipal Corporations 🔑 58

8. ---- Statutes conflicting with charters

Provisions of charter of city in **Michigan** cannot vitiate rights bestowed by an act of **Michigan** Legislature. Martz v. Consumers Power Co., E.D.Mich.1951, 101 F.Supp. 853. Municipal Corporations 🔑 8

Battle Creek charter provision, requiring written notice of tort claim to be served within 60 days after occurrence of injury or wrong, was void for contravening state statutes setting up three-year statute of limitations for such claims. Marks v. City of Battle Creek (1959) 99 N.W.2d 587, 358 **Mich.** 114. Municipal Corporations 🔑 79

Municipal charter provisions or **ordinances** must not contravene a statutory enactment. City of Grand Haven v. Grocer's Co-op. Dairy Co. (1951) 48 N.W.2d 362, 330 **Mich.** 694. Municipal Corporations 🔑 46; Municipal Corporations 🔑 111(2)

General statutory provision authorizing municipal library board of directors to acquire library building was not abrogated by home-rule charter providing that library should remain property of municipal corporation, hence city commission acted without authority in selling library building since title was in library board. Bostedor v.

City of Eaton Rapids (1935) 263 N.W. 416, 273 **Mich**. 426. Municipal Corporations 🔑 225(3)

Limitation in provision of city charter requiring as condition to suit against city presentment of claim to city commission within six months after cause of action arose was void in so far as it fixes limitation period as contravening general statutes of limitations. Northrup v. City of Jackson (1935) 262 N.W. 641, 273 **Mich**. 20. Municipal Corporations 🔑 79

P.A.1925, No. 273, entitled "an Act to regulate issue of bonds, or other obligations, by municipalities, * * * provide method of payment * * * and prescribe duties of municipal officers and * * * state treasurer," construed as applicable to cities under home rule charter, was not unconstitutional as not showing by its title that Home Rule Act (P.A.1909, No. 279), limiting tax rate was thereby modified. Simonton v. City of Pontiac (1934) 255 N.W. 608, 268 **Mich**. 11. Statutes 🔑 120(4)

A statute should not be so construed as to render city charter unworkable, seriously impair conduct of municipal business, or result in litigation or absurdity in government, if another construction be fairly possible. Kelly v. Laing (1932) 242 N.W. 891, 259 **Mich**. 212. Statutes 🔑 181(2)

Detroit City Charter, tit. 9, c. 2, entitled "Minimum Wage," and declaring an eight-hour service day for city employees and a minimum wage, and requiring contractors doing work for the city to observe such hours and rates, and a city **ordinance** of similar import, were ultra vires as an attempt to exercise police power over matters of state concern, and to fix a public policy over matters not purely local. Attorney General v. City of Detroit (1923) 196 N.W. 391, 225 **Mich**. 631. Municipal Corporations 🔑 590

A city charter providing for a city manager was not unconstitutional under Const.1908, Art. 8, §§ 20, 21 (see, now, Const. Art. 7, §§ 21, 22) or invalid in its entirety, whether or not the power of the manager conflicted with P.A.1909, No. 279, § 3. Kopczynski v. Schriber (1917) 161 N.W. 238, 194 **Mich**. 553. Statutes 🔑 64(4)

The term of office of a justice of the peace of Bay City, a "home rule" city, expired in the month of April rather than July 4th, since the term of office was so prescribed by Local Act No. 636 of 1907 and the city charter neither of which were in conflict with the home rule cities act (P.A.1909, No. 279). Op.Atty.Gen.1949-50, No. 1214, p. 568.

Where provisions of city charter relative to primary elections are inconsistent with state law, charter provisions control. Op.Atty.Gen. 1928-30, p. 746.

9. ---- **Ordinances** conflicting with charters

In the event of a conflict, the requirements of the charter as adopted by the people of the municipality are controlling over conflicting **ordinances**. Brady v. City of Detroit (1958) 91 N.W.2d 257, 353 **Mich**. 243. Municipal Corporations 🔑 111(1)

Proposed **ordinance** that no city official, employee, officer, or agent shall expend, disburse or commit any public funds, revenues or income of city, regardless of source, for acquisition, development, maintenance or operation of off-street parking of automobiles, other than those owned by city, was void because it would prohibit city officials from disbursing or committing funds of city for purposes expressly authorized by both city charter and state law. Stolorow v. City of Pontiac (1954) 63 N.W.2d 611, 339 **Mich**. 199. Municipal Corporations 🔑 267

A home rule city cannot pass **ordinances** that are contrary to the charter of the city. Thiesen v. Parker (1948) 31 N.W.2d 806, 320 **Mich**. 446.

The charter of a city is fundamental law thereof, and all city **ordinances** in conflict with or violating mandates of charter are void. Hubbard v. Board of Trustees of Retirement System (1946) 23 N.W.2d 186, 315 **Mich**. 18. Municipal Corporations 🔑 111(1)

The charter of a city is the fundamental law thereof and all **ordinances** of the city which are in conflict therewith or violative of its mandates are void. Quandt v. Schwass (1938) 282 N.W. 206, 286 **Mich**. 433. Municipal Corporations 🔑 111(1)

That local acts creating board of poor commissioners and office of city physician were not designated as parts of, or amendments to, city charter, did not except them from amendment by the people. Pryzbylowski v. Board of Poor Com'rs (1915) 154 N.W. 117, 188 **Mich**. 270. Municipal Corporations 🔑 46

10. **Ordinances**--In general

Distinction between zoning and regulatory **ordinances** cannot be predicated on whether purpose of **ordinance** is to promote the general good, since both may have common purpose of promoting public good. People v. Strobridge (1983) 339 N.W.2d 531, 127 Mich.App. 705. Zoning And Planning 🔑 1000

City, like township, has power to adopt **ordinances** for promotion of public welfare and power to establish zoning districts. People v. Strobridge (1983) 339 N.W.2d 531, 127 Mich.App. 705. Zoning And Planning 🔑 1017

Ordinance violations constitute criminal acts. City of Detroit v. Recorder's Court Traffic and **Ordinance** Judge (1981) 304 N.W.2d 829, 104 Mich.App. 214. Municipal Corporations 🔑 630

Size and scope of matters involved are not proper yardsticks for determining whether city action requires adoption of an **ordinance** or whether action can be authorized by resolution of city commission; the difference lies in the nature of the act, not its impact. Rollingwood Homeowners Corp. v. City of Flint (1971) 191 N.W.2d 325, 386 **Mich**. 258. Municipal Corporations 🔑 85

The difference between municipal **ordinances** and resolutions is in what the actions do rather than in the manner in which they are passed; "resolutions" are for implementing ministerial functions of government for short-term purposes while "**ordinances**" are for establishing more permanent influences on the community itself. Parr v.

Fulton (1968) 158 N.W.2d 35, 9 Mich.App. 719. Municipal Corporations 🔑 85; Municipal Corporations 🔑 105

Labeling a resolution an **ordinance** does not make it so. Parr v. Fulton (1968) 158 N.W.2d 35, 9 Mich.App. 719. Municipal Corporations 🔑 85; Municipal Corporations 🔑 105

Under **ordinance** making it unlawful to display or advertise for sale contraceptive devices or prophylactic rubber goods of similar character, and making sale of such articles unlawful except when sale was made by a bona fide druggist or a licensed physician, question of whether right to make sales, so far as pharmacists were concerned, should be limited to those operating or employed in drug stores of kind designated in **ordinance**, was for determination of body passing **ordinance**, provided that method adopted was not arbitrary or discriminatory. People v. Pennock (1940) 293 N.W. 759, 294 **Mich.** 578. Municipal Corporations 🔑 63.15(3)

In **ordinances** enacted under police power and designed to preserve property values, esthetics may be an incident but may not be the moving factor. Wolverine Sign Works v. City of Bloomfield Hills (1937) 271 N.W. 823, 279 **Mich.** 205. Zoning And Planning 🔑 1050

Under Home Rule Charter Law (P.A.1909, No. 279), city had the power to pass **ordinance** regulating, restricting, and limiting number and location of oil and gasoline filling stations and enforcing specific taxes thereon. Fletcher Oil Co. v. Bay City (1929) 226 N.W. 248, 247 **Mich.** 572.

A city incorporating or desiring a general revision of its charter, under (P.A.1909, No. 279), providing for the incorporation of new cities and the revision of charters of existing cities, must include in its charter the compulsory provisions of § 3, enumerating the compulsory provisions of every city charter, and the restrictive provisions of § 5, defining and limiting the power of cities. Kuhn v. Common Council of City of Detroit (1911) 129 N.W. 879, 164 **Mich.** 369. Municipal Corporations 🔑 46

Detroit City Charter, par. 170, confers the power to regulate the use of the highways and public grounds within the city; § 186 authorizes the city to license and regulate draymen, truckmen, and drivers of carriages and vehicles of every description used and employed for hire; by **ordinance** the mayor was authorized to grant licenses to any person of good character to drive or use any vehicle for carting stone, bricks, and mortar, etc., or rubbish, upon payment of a license charge and the execution of a bond to the city to indemnify it against loss or damage by the dumping of such vehicles, and no person was to engage in such business without a license; the defendant owning and operating its own teams in its business of dealing in brick, plaster, and building material, and its team and driver were complained against for a violation of the **ordinance**; the **ordinance** was passed under § 186 of the charter, and was aimed at the regulation of a business, and the business of the defendant, being no different from the use made of the streets by any business man, was not what the **ordinance** was designed to regulate. People v. C.H. Little Co. (1910) 128 N.W. 767, 163 **Mich.** 444. Licenses 🔑 14(1)

On a prosecution for violating an **ordinance** regulating the disposition of the garbage of a city, evidence showing that the purpose of the council in adopting the **ordinance** was fraudulent and to create a monopoly of the garbage business in the hands of one concern was inadmissible. People v. Gardner (1906) 106 N.W. 541, 143 **Mich.** 104. Municipal Corporations 🔑 111(7)

A township, city or village has the power to adopt an **ordinance** regulating well construction, provided that the requirements of the **ordinance** are not less restrictive than the administrative rule requirements set forth in 1994 AACS, R 325.1601 et seq. Op.Atty.Gen. 1996, No. 6898, 1996 WL 221569.

11. ---- Enacting requirements, **ordinances**

Constitutional provisions as to titles of laws do not apply to city **ordinances**. Hughes v. City of Detroit (1922) 187 N.W. 530, 217 **Mich.** 567; People v. Hanrahan (1889) 42 N.W. 1124, 75 **Mich.** 611.

Ordinance having but one general object, that of consolidating city's two tracts of land for enlarged airport, was not objectionable as embracing more than one object. Clayton & Lambert Mfg. Co. v. City of Detroit, E.D.Mich.1929, 34 F.2d 303. Municipal Corporations 🔑 111(1)

Statute allowing cities to adopt by reference any fire, plumbing, heating, building, or other code promulgated by an authorized agency of state, and any code pertaining to flammable liquids and gases, and other chemicals, which has been promulgated by state agency or organization or association that is organized for purposes of developing code, did not authorize city to adopt by reference property maintenance code established by national organization. Ewing v. City of Detroit (1999) 604 N.W.2d 787, 237 Mich.App. 696, appeal denied 618 N.W.2d 766, 463 **Mich.** 888. Municipal Corporations 🔑 599

Ordinance imposing fee for waste collection was not a pure revenue measure subject to method of enactment different from **ordinance** in exercise of police power. Alexander v. City of Detroit (1973) 205 N.W.2d 819, 45 Mich.App. 7, reversed on other grounds 219 N.W.2d 41, 392 **Mich.** 30. Municipal Corporations 🔑 106(1)

Classification of objects to which municipal **ordinance** may be applicable must be based on natural distinguishing characteristics and must bear a reasonable relation to object of the **ordinance**. Beauty Built Const. Corp. v. City of Warren (1965) 134 N.W.2d 214, 375 **Mich.** 229. Municipal Corporations 🔑 111(3)

Where common council, in passing **ordinance**, declared **ordinance** to be necessary for preservation of public peace, health, and safety, although such declaration was not conclusive of power to enact, it was indicative of purpose of **ordinance**. People v. Pennock (1940) 293 N.W. 759, 294 **Mich.** 578. Municipal Corporations 🔑 595; Municipal Corporations 🔑 596; Municipal Corporations 🔑 597

All by-laws and **ordinances** of any home rule city relating to its municipal concerns must be subject to Constitution and general laws of state. Hudson Motor Car Co. v. City of Detroit (1937) 275 N.W. 770, 282 **Mich.** 69. Municipal Corporations 🔑 111(2)

Regulatory **ordinance** should specify standard for guidance of official who passes on application for permit.

Hoyt Bros. v. City of Grand Rapids (1932) 245 N.W. 509, 260 **Mich**. 447. Municipal Corporations 🔑 591

The omission from the title of a city **ordinance** of the provision therein contained, imposing a penalty for its violation, does not invalidate the **ordinance**, in view of a previous decision that the constitutional provisions relating to the title of laws do not apply to **ordinances**. Melconian v. City of Grand Rapids (1922) 188 N.W. 521, 218 **Mich**. 397. Municipal Corporations 🔑 112(3)

The state is in no way concerned in the question of the irregular enactment of city **ordinances**. People ex rel. Kunze v. Ft. Wayne & E. Ry. Co. (1892) 52 N.W. 1010, 92 **Mich**. 522. Municipal Corporations 🔑 121

The constitution, relating to the title of laws, does not apply to city **ordinances**; and an **ordinance** of the City of Detroit, entitled "An **ordinance** relative to the manufacture and selling of bread," is not objectionable on the ground that matters contained within the body of the **ordinance** are not within the title. People v. Wagner (1891) 49 N.W. 609, 86 **Mich**. 594, 24 Am.St.Rep. 141. Municipal Corporations 🔑 112(3)

The omission from an **ordinance** of the enacting clause will not render it void, in the absence of any provision of the statute to that effect. People v. Murray (1885) 24 N.W. 118, 57 **Mich**. 396. Municipal Corporations 🔑 105

A home rule city may adopt an **ordinance** incorporating a state act by reference without publication of the entire act, where the **ordinance** otherwise complies with the requirements of this section, or where the Legislature has delegated to home rule cities the power to do so by law. Op.Atty.Gen. 1989, No. 6575, p. 70, 1989 WL 445948.

12. ---- Publication, **ordinances**

Statute allowing cities to adopt by reference any fire, plumbing, heating, building, or other code promulgated by an authorized agency of state, and any code pertaining to flammable liquids and gases, and other chemicals, which has been promulgated by state agency or organization or association that is organized for purposes of developing code, did not authorize city to adopt by reference property maintenance code established by national organization. Ewing v. City of Detroit (1999) 604 N.W.2d 787, 237 Mich.App. 696, appeal denied 618 N.W.2d 766, 463 **Mich**. 888. Municipal Corporations 🔑 599

Ordinance approved May 29 and published June 3, 5 and 6 was published "immediately" within charter provision. Red Star Motor Drivers' Ass'n v. City of Detroit (1928) 221 N.W. 622, 244 **Mich**. 480. Municipal Corporations 🔑 110

Publication of **ordinance** on newspaper, printing news of courts, legal notices, and proceedings held compliance with charter requiring publication in newspaper. Red Star Motor Drivers' Ass'n v. City of Detroit (1928) 221 N.W. 622, 244 **Mich**. 480. Municipal Corporations 🔑 110

Publication of **ordinance** of the city of Detroit, No. 600A, as passed, containing a reference to a so-called

"Building Code" of the city by title, held insufficient to comply with the charter of Detroit City Charter, c. 1, tit. 3, § 20. L.A. Thompson Scenic Ry. Co. v. McCabe (1920) 178 N.W. 662, 211 **Mich.** 133. Municipal Corporations 🔑 110

A municipal **ordinance** is not invalid because not published, where the charter did not require publication. Vernakes v. City of South Haven (1915) 152 N.W. 919, 186 **Mich.** 595. Municipal Corporations 🔑 110

Under a city charter providing that no **ordinance** shall take effect unless published at least one week in the official paper of the city, the publication is sufficient if the **ordinance** is published as often as such paper is issued; the fact that the paper has no Monday issue is immaterial. Richter v. Harper (1893) 54 N.W. 768, 95 **Mich.** 221. Municipal Corporations 🔑 110

Term "publish" refers to act of making information known to the general public, as distinguished from "print" which properly refers to the mechanical process whereby the impression of words are stamped upon paper; "circulate" is synonymous with "publish" and refers to the passing from one person or place to another person or place. Op.Atty.Gen.1975, No. 4891, p. 177.

As in the case of legal notices, municipalities must publish **ordinances** in a "qualified" newspaper published within their municipality, and quoted term refers to compliance with the statutory requirements; fourth class cities and villages have the added obligation of publishing their **ordinances** in a newspaper which is printed within the municipality. Op.Atty.Gen.1975, No. 4891, p. 177.

13. ---- Statutes conflicting with **ordinances**

In absence of specific statutory or charter power in municipality, **ordinance** contravening state law is void. City of Grand Haven v. Grocer's Co-op. Dairy Co. (1951) 48 N.W.2d 362, 330 **Mich.** 694; National Amusement Co. v. Johnson (1935) 259 N.W. 342, 270 **Mich.** 613.

Ordinance requiring inspection before homeowner could sell his one or two-family residence was not preempted by state housing code [§ 333.12201 et seq. (repealed)]. Butcher v. City of Detroit (1984) 347 N.W.2d 702, 131 Mich.App. 698. Municipal Corporations 🔑 592(1)

Where provision of **ordinance** had been found invalid because in conflict with state statute, constitutionality of **ordinance** would not be determined. City of Grand Haven v. Grocer's Co-op. Dairy Co. (1951) 48 N.W.2d 362, 330 **Mich.** 694. Municipal Corporations 🔑 121

In absence of specific statutory or charter power in municipality, provisions of **ordinance** contravening state law are void. Richards v. City of Pontiac (1943) 9 N.W.2d 885, 305 **Mich.** 666. Municipal Corporations 🔑 592(1)

Generally, existence of state law on same subject as municipal **ordinance** relating to Sunday observance does not invalidate **ordinance**, if city has authority, either express or implied, to legislate on such subject, and its legislation is not in conflict with statute, but **ordinance** prohibiting that which statute permits is void. Builders Ass'n (of Metropolitan Detroit) v. City of Detroit (1940) 294 N.W. 677, 295 **Mich**. 272. Municipal Corporations 🔑 592(1)

City cannot without express authority suppress what Legislature permits. National Amusement Co. v. Johnson (1935) 259 N.W. 342, 270 **Mich**. 613. Municipal Corporations 🔑 591

A municipality may not, in performance of its functions as agent for a state, declare a public policy applicable to matters of state concern. Attorney General v. City of Detroit (1923) 196 N.W. 391, 225 **Mich**. 631. Municipal Corporations 🔑 590

A city has no power to pass **ordinances** to preserve private property from encroachment; that protection must be enforced under the laws of the state. Horn v. People (1872) 26 **Mich**. 221. Municipal Corporations 🔑 599

14. ---- Construction, **ordinances**

The rules governing the construction of statutes are applicable to **ordinances**. Fink v. City of Detroit (1983) 333 N.W.2d 376, 124 Mich.App. 44. Municipal Corporations 🔑 120

Where an **ordinance** is open to two constructions, one of which is legal and the other illegal, the legal construction will, if possible, be adopted, notwithstanding it is not the most obvious or natural construction. Quandt v. Schwass (1938) 282 N.W. 206, 286 **Mich**. 433. Municipal Corporations 🔑 120

Ordinance prohibiting auction sales of linen, laces, etc., except by merchants in business in city for one year and certain others, was not prohibitive, but merely regulatory. Saigh v. Common Council of City of Petoskey (1930) 231 N.W. 107, 251 **Mich**. 77. Auctions And Auctioneers 🔑 2

City **ordinances** conferring grants are to be construed liberally in favor of the public. Traverse City Gas Co. v. City of Traverse City (1902) 89 N.W. 574, 130 **Mich**. 17. Municipal Corporations 🔑 120

The fact that an **ordinance** covers matters which the city has no power to control is no reason why it should not be enforced as to those which it may control; the unauthorized provisions do not invalidate the whole **ordinance** , if they can be separated from the rest of the **ordinance** without so mutilating it as to render it inoperative. People v. Armstrong (1889) 41 N.W. 275, 73 **Mich**. 288, 16 Am.St.Rep. 578. Municipal Corporations 🔑 111(4)

15. ---- Reasonableness, **ordinances**

Classification of objects to which municipal **ordinances** may be made applicable must be based on natural characteristics and bear reasonable relation to object of **ordinance**. Alexander v. City of Detroit (1973) 205 N.W.2d 819, 45 Mich.App. 7, reversed on other grounds 219 N.W.2d 41, 392 **Mich**. 30. Municipal Corporations 🔑

625

Whether regulatory **ordinance** is unreasonable must be determined as question of law and not as question of policy. Red Star Motor Drivers' Ass'n v. City of Detroit (1926) 208 N.W. 602, 234 **Mich**. 398, stay granted 210 N.W. 496, 236 **Mich**. 422, error dismissed 48 S.Ct. 27, 275 U.S. 486, 72 L.Ed. 386. Municipal Corporations 🔑 63.20

Compiled **Ordinance** of Detroit 1912, p. 600, c. 245, § 19a, requiring all street cars, when signaled, to stop at every intersection, is not unreasonable. People v. Detroit United Ry. (1919) 173 N.W. 396, 207 **Mich**. 143. Street Railroads 🔑 74

To render **ordinances** reasonable, they must tend in some degree to the accomplishment of the object for which the corporation was created and its powers conferred. People v. Armstrong (1889) 41 N.W. 275, 73 **Mich**. 288, 16 Am.St.Rep. 578. Municipal Corporations 🔑 111(3)

Where an **ordinance** was a valid exercise of the power granted the city, and the act of granting the power was itself constitutional, there could be no question as to the reasonableness of the **ordinance**. People v. Armstrong (1889) 41 N.W. 275, 73 **Mich**. 288, 16 Am.St.Rep. 578. Municipal Corporations 🔑 111(3)

Where the power to legislate on a given subject is conferred, and the mode of its exercise is not prescribed, then the **ordinance** passed in pursuance thereof must be a reasonable exercise of the power, or it will be pronounced invalid. People v. Armstrong (1889) 41 N.W. 275, 73 **Mich**. 288, 16 Am.St.Rep. 578. Municipal Corporations 🔑 111(3)

16. ---- Validity, **ordinances**

Ordinance requiring valid certificate of approval or valid inspection report from city before person could sell or transfer one or two-family residential structure in city and also authorizing inspection fee did not amount to unconstitutional taking of property without due process under U.S.C.A. Const. Amend. 14. Butcher v. City of Detroit (1984) 347 N.W.2d 702, 131 Mich.App. 698. Eminent Domain 🔑 2.10(1)

Municipal **ordinance** designed to regulate distribution of contraceptive products and devices in general and prophylactic rubber goods specifically, and "any sex inciting device or contrivance" was not invalid as conflicting with state regulatory scheme. Kalita v. City of Detroit (1975) 226 N.W.2d 699, 57 Mich.App. 696. Municipal Corporations 🔑 592(1)

Where activity sought to be prohibited by municipal **ordinance** was of an indelicate nature, failure to graphically outline the conduct regulated did not cause **ordinance** to be unconstitutionally vague or overbroad under M.C.L.A. Art. 1, § 17 or U.S.C.A. Const. Amend. 14. Kalita v. City of Detroit (1975) 226 N.W.2d 699, 57 Mich.App. 696. Municipal Corporations 🔑 594(2)

Municipal **ordinance** primarily designed to regulate distribution of contraceptive products and devices in general and prophylactic rubber goods specifically properly included "any sex inciting device or contrivance"; quoted phrase derived added certitude from its inclusion among other products and was not unconstitutionally vague or overbroad under M.C.L.A. Const. Art. 1, § 17 or U.S.C.A. Const. Amend. 14. Kalita v. City of Detroit (1975) 226 N.W.2d 699, 57 Mich.App. 696. Municipal Corporations 🔑 594(2)

Mere fact that municipal **ordinance** authorizes imposition of greater penalty than does statute does not necessarily invalidate the **ordinance**. Kalita v. City of Detroit (1975) 226 N.W.2d 699, 57 Mich.App. 696. Municipal Corporations 🔑 592(3)

Generally, local regulation in addition to state law does not constitute conflict therewith where statute has not preempted field and state law can work effectively despite local intervention. Kalita v. City of Detroit (1975) 226 N.W.2d 699, 57 Mich.App. 696. Municipal Corporations 🔑 592(1)

Fact that **ordinance** has been held to be constitutional does not foreclose continued consideration of constitutional challenges to **ordinance**, in that **ordinance** may be constitutional on its face and yet work a deprivation of due process as it is applied in a particular situation. Detroit Police Lieutenants and Sergeants Ass'n v. City of Detroit (1974) 224 N.W.2d 728, 56 Mich.App. 617. Municipal Corporations 🔑 121

Ordinance, which made it unlawful for any person to make, continue or cause to be made or continued any loud, "unnecessary" or unusual noise or any noise which either "annoys", disturbs, injures or endangers the comfort, repose, health, peace or safety of others was unconstitutionally vague under U.S.C.A. Const. Amend. 1. **United Pentecostal Church** v. Steendam (1974) 214 N.W.2d 866, 51 Mich.App. 323. Municipal Corporations 🔑 594(2)

A municipality has a legitimate objective in protection of its citizens from those noises which may affect their health, morals, and safety. **United Pentecostal Church** v. Steendam (1974) 214 N.W.2d 866, 51 Mich.App. 323 . Municipal Corporations 🔑 595; Municipal Corporations 🔑 597; Municipal Corporations 🔑 598

Where activity to be regulated is safeguarded by U.S.C.A.Const. Amend. 1, standard of permissible statutory vagueness becomes more strict. **United Pentecostal Church** v. Steendam (1974) 214 N.W.2d 866, 51 Mich.App. 323. Statutes 🔑 47

Plaintiffs, not city have burden on issue of validity of **ordinance**. Alexander v. City of Detroit (1973) 205 N.W.2d 819, 45 Mich.App. 7, reversed on other grounds 219 N.W.2d 41, 392 **Mich**. 30. Municipal Corporations 🔑 122.1(2)

Municipal regulations which require that licensee's business premises comply with health, safety, and fire laws and which provide means for inspection to assure compliance would be deemed reasonable. Soof v. City of Highland Park (1971) 186 N.W.2d 361, 30 Mich.App. 400. Licenses 🔑 7(1)

Ordinance prohibiting loitering and defining loitering as act of standing or idling in or about any street, sidewalk, over-pass or public place so as to hinder or impede or tend to hinder or impede passage of pedestrians or vehicles is not unconstitutionally broad or vague. People of City of Detroit v. Ritchey (1970) 181 N.W.2d 87, 25 Mich.App. 98. Municipal Corporations 🔑 594(2); Municipal Corporations 🔑 703(1); Municipal Corporations 🔑 704

Portions of Detroit **ordinance** prohibiting wrongfully ogling, annoying, or improperly and wrongfully molesting by gesture are valid and binding upon any person who clearly expresses intent, by overt action or foul talk, to interfere with or abuse other persons or culpably offend their dignity or sensibilities. People v. Wilson (1969) 173 N.W.2d 252, 19 Mich.App. 595. Municipal Corporations 🔑 631(1)

Prosecution under **ordinance** prohibiting loitering on street or sidewalk so as to obstruct free and uninterrupted passage of public did not deny any constitutionally protected rights of defendant who sat in street and blocked traffic in order to protest and to assemble in favor of fair housing legislation. People v. Deutsch (1969) 172 N.W.2d 392, 19 Mich.App. 74. Constitutional Law 🔑 1431

Ordinance prohibiting any person from loitering on street or sidewalk or conducting himself in any public place so as to obstruct free and uninterrupted passage of public was enacted to protect public safety and was within police powers of the city. People v. Deutsch (1969) 172 N.W.2d 392, 19 Mich.App. 74. Municipal Corporations 🔑 703(3)

It is not beyond power of municipality to control means and extent of manner of dissemination of ideas on city streets; however, when used for ordinary purposes, right of regulating streets and sidewalks should be sparingly exercised. People v. Deutsch (1969) 172 N.W.2d 392, 19 Mich.App. 74. Municipal Corporations 🔑 703(1)

Ordinance prohibiting loitering and defining loitering as the act of standing or idling in or about any street, sidewalk, overpass or public place so as to hinder or impede or tend to hinder or impede passage of pedestrians or vehicles is not unconstitutionally broad or vague under M.C.L.A. Const. Art. 1, § 17 or U.S.C.A. Const. Amend. 14. People v. Wedlow (1969) 169 N.W.2d 145, 17 Mich.App. 134. Municipal Corporations 🔑 594(2) ; Municipal Corporations 🔑 703(1); Municipal Corporations 🔑 704

Ordinance prohibiting loitering, having been enacted to protect public safety was within police power of municipality. People v. Wedlow (1969) 169 N.W.2d 145, 17 Mich.App. 134. Municipal Corporations 🔑 595

Legislative body can make even innocent acts unlawful if these acts have tendency to affect or endanger public in connection with health, safety, morals or general welfare. People v. Wedlow (1969) 169 N.W.2d 145, 17 Mich.App. 134. Criminal Law 🔑 3

An **ordinance** making it unlawful for a known prostitute to repeatedly stop or attempt to stop any pedestrian in any public place and defining a known prostitute as any female convicted of prostitution within two years of her arrest was unconstitutional for violation of the privilege against self-incrimination, and the right to remain silent under M.C.L.A. Const. Art. 1, § 17 and U.S.C.A. Const. Amend. 5, in view of fact that it did not permit any defense in that once it was shown that the accused committed the forbidden act of waving, or other proscribed acts, and that she had previously been convicted of a similar offense within the prescribed time period, the violation was proved. City of Detroit v. Bowden (1967) 149 N.W.2d 771, 6 Mich.App. 514. Criminal Law 🔑 393(1)

Ordinance making it unlawful for a known prostitute to repeatedly stop or attempt to stop any pedestrian or motor vehicle operator by hailing, whistling, waving of arms, or any other bodily gesture, in any public place, was void for vagueness. City of Detroit v. Bowden (1967) 149 N.W.2d 771, 6 Mich.App. 514. Municipal Corporations 🔑 111(1)

Ordinance proscribing certain activity by a known prostitute or panderer, and defining a known prostitute or panderer as a person convicted of prostitution, pandering or other crimes within two years from date of arrest for violation of the **ordinance** created a conclusive presumption that one convicted of one of the listed crimes within two years prior to arrest was a "known prostitute or panderer," and thereby stripped a defendant of all defense because of a prior conviction, and was thus unconstitutional for failure to meet test of due process under both M.C.L.A.Const. Art. 1, § 17 and U.S.C.A.Const. Amend. 5. City of Detroit v. Bowden (1967) 149 N.W.2d 771, 6 Mich.App. 514. Constitutional Law 🔑 4509(23); Prostitution 🔑 14

Regulations may result to some extent practically in the taking of property or the restricting of its uses and yet not be deemed confiscatory or unreasonable and courts will not hold laws, **ordinances**, or regulations adopted under sanction of law to be unconstitutional unless they are clearly unreasonable, destructive, or confiscatory. Patchak v. Lansing Tp. (1960) 105 N.W.2d 406, 361 **Mich.** 489. Constitutional Law 🔑 1007; Municipal Corporations 🔑 122.1(2); Zoning And Planning 🔑 1035

In absence of clear evidence to the contrary, court will assume that city council has acted upon facts within its possession which justify classification made as reasonable and proper. People's Appliance & Furniture, Inc. v. City of Flint (1959) 99 N.W.2d 522, 358 **Mich.** 34. Municipal Corporations 🔑 122.1(2)

It is not judicial function to determine wisdom or lack of wisdom of city legislative body in adopting certain **ordinances** but only to determine whether the **ordinance** is constitutional. People's Appliance & Furniture, Inc. v. City of Flint (1959) 99 N.W.2d 522, 358 **Mich.** 34. Municipal Corporations 🔑 63.10

Reduction of tax claim to lien and execution without any judicial proceedings whatsoever is not objectionable as violation of due process. State of Ohio, Dept. of Taxation v. Kleitch Bros., Inc. (1959) 98 N.W.2d 636, 357 **Mich.** 504. Constitutional Law 🔑 4138(2)

While it is within the province of the courts to pass upon the validity of statutes and **ordinances**, courts may not legislate or undertake to compel legislative bodies to do so one way or another. Randall v. Township Bd. of Meridian Tp., Ingham County (1955) 70 N.W.2d 728, 342 **Mich.** 605. Constitutional Law 🔑 2473; Municipal Corporations 🔑 63.1

A city **ordinance** prohibiting sale of certain commodities does not constitute class legislation if it applies with equal force to all situated in a like business. People v. Krotkiewicz (1938) 282 N.W. 852, 286 **Mich.** 644. Sunday 🔑 2

Ordinance authorizing city manager to grant or withhold permits for soliciting funds for charitable purposes, on determination whether charity is "worthy" and applicants are "fit and responsible," was void. Hoyt Bros. v. City of Grand Rapids (1932) 245 N.W. 509, 260 **Mich.** 447. Municipal Corporations 🔑 591

The motives of members of a council in voting for an **ordinance** may not be inquired into for purpose of determining validity of the **ordinance**. People v. Gardner (1906) 106 N.W. 541, 143 **Mich.** 104. Municipal Corporations 🔑 111(7)

P.A.1865, which established a police government for the city of Detroit, created a board composed of resident freeholders of the city and conferred upon them powers and duties of a local nature; the **Michigan** liquor law, (Laws 1887, § 33), which extended the jurisdiction of the board within the county, but outside of the city limits, without changing the general character and duties of the board as a city board, and provided for the payment of the extra police force by the county, was invalid. Metropolitan Police Board v. Board of Auditors of Wayne County (1888) 36 N.W. 743, 68 **Mich.** 576. Municipal Corporations 🔑 66

Summary process to enforce payment by a delinquent or defaulting tax collector was not so unusual or unknown in this or other states when our Constitution was proposed and adopted as to be by implication excluded from "due process of law." Weimer v. Bunbury (1874) 30 **Mich.** 201. Constitutional Law 🔑 4135

17. ---- Partial invalidity, **ordinances**

An **ordinance** may be valid in part and void in part, and the valid part may be carried into effect, if what remains after the invalid part is eliminated contains the essential elements of a complete **ordinance**. Johnson v. Common Council of City of Bessemer (1906) 106 N.W. 852, 143 **Mich.** 313; City of Detroit v. Ft. Wayne & B.I. Ry. Co. (1893) 54 N.W. 958, 95 **Mich.** 456, 35 Am.St.Rep. 580.

Invalid phrase "any other lewd immoral act" was severable from city **ordinance** making it unlawful to accost, solicit or invite another in any public place or in or from any building or vehicle to commit or afford an opportunity to commit fornication or prostitution or any other lewd immoral act and, on finding that it was overly broad, would be severed without effecting validity of remainder of **ordinance**. Morgan v. City of Detroit, E.D.Mich.1975, 389 F.Supp. 922. Municipal Corporations 🔑 111(4)

If unconstitutional language can be deleted from city **ordinance** and still leave **ordinance** complete and operative, then such remainder of **ordinance** may be permitted to stand. Eastwood Park Amusement Co. v. City of East Detroit (1950) 43 N.W.2d 851, 328 **Mich.** 272. Municipal Corporations 🔑 111(4)

In licensing **ordinance**, provisions requiring license as prerequisite to operation of amusement park, forbidding licensees to permit gambling at park, for revocation of license for violation of **ordinance**, and for refusal of license on grounds of violation of state laws or city **ordinances** were severable from rest of **ordinance** and complete and operative in and of themselves, and, hence, valid and enforceable even though other sections of **ordinance** were unconstitutional. Eastwood Park Amusement Co. v. City of East Detroit (1950) 43 N.W.2d 851, 328 **Mich.** 272. Municipal Corporations 🔑 111(4)

If unconstitutional language can be deleted from a city **ordinance** and still leave **ordinance** complete and operative, then such remainder of the **ordinance** may be permitted to stand, even though there is no severability clause in **ordinance**. Eastwood Park Amusement Co. v. Stark (1949) 38 N.W.2d 77, 325 **Mich.** 60. Municipal Corporations 🔑 111(4)

Where city **ordinance** dealing with licensing of places of entertainment was complete and operative after deletion of invalid provisions relating to revocation of licenses of places of entertainment by mayor, remainder was valid and would be permitted to stand. Eastwood Park Amusement Co. v. Stark (1949) 38 N.W.2d 77, 325 **Mich.** 60. Municipal Corporations 🔑 111(4)

Ordinance licensing sale of food and imposing sanitary regulations was not invalid in toto because of invalid provisions governing suspension or revocation of licenses; such provisions being severable, especially in view of severability clause. Ritter v. City of Pontiac (1936) 267 N.W. 641, 276 **Mich.** 416. Municipal Corporations 🔑 111(4)

An **ordinance** is not entirely void because it contains an illegal provision. Goldstein v. City of Hamtramck (1924) 198 N.W. 962, 227 **Mich.** 263. Municipal Corporations 🔑 111(4)

18. ---- Presumption of validity, **ordinances**

Same rule of construction as to constitutional validity applies to both **ordinances** and statutes, as well as same presumptions. Tower Realty v. City of East Detroit, C.A.6 (**Mich.**)1952, 196 F.2d 710. Constitutional Law 🔑 990; Municipal Corporations 🔑 111(1); Municipal Corporations 🔑 122.1(2)

A statute or **ordinance** will be presumed to be constitutional unless contrary clearly appears, and in case of doubt, every possible presumption not clearly inconsistent with language and subject matter is to be made in favor of constitutionality. Tower Realty v. City of East Detroit, C.A.6 (**Mich.**)1952, 196 F.2d 710. Constitutional Law 🔑 996; Constitutional Law 🔑 1002; Municipal Corporations 🔑 122.1(2)

Ordinance which is patently unconstitutional is not afforded benefit of presumed validity. Bristow v. City of Woodhaven (1971) 192 N.W.2d 322, 35 Mich.App. 205. Municipal Corporations 🔑 122.1(2)

Ordinance will be presumed to be constitutional unless the contrary clearly appears. People v. Deutsch (1969) 172 N.W.2d 392, 19 Mich.App. 74. Constitutional Law 🔑 996

Rule that a statute will be presumed to be constitutional unless the contrary clearly applies, is applicable with equal force to municipal **ordinances**. Watnick v. City of Detroit (1962) 113 N.W.2d 876, 365 **Mich**. 600. Municipal Corporations 🔑 122.1(2)

A presumption prevails in favor of reasonableness and validity in all particulars of a municipal **ordinance**, unless contrary is shown by competent evidence, or appears on face of the enactment. Brown v. Shelby Tp., Macomb County (1960) 103 N.W.2d 612, 360 **Mich**. 299. Municipal Corporations 🔑 122.1(2)

The constitutionality of an **ordinance** of a home rule city will be presumed unless fatal defects are shown. Mutchall v. City of Kalamazoo (1948) 35 N.W.2d 245, 323 **Mich**. 215. Municipal Corporations 🔑 122.1(2)

A presumption prevails in favor of the reasonableness and validity of a municipal **ordinance**, unless the contrary is shown by competent evidence, or appears on the face of the **ordinance**. Fass v. City of Highland Park (1948) 32 N.W.2d 375, 321 **Mich**. 156. Municipal Corporations 🔑 122.1(2)

A presumption prevails in favor of the reasonableness and validity of a municipal **ordinance**, unless contrary is shown by competent evidence or appears on the face of the enactment. Portage Tp. v. Full Salvation Union (1947) 29 N.W.2d 297, 318 **Mich**. 693, appeal dismissed 68 S.Ct. 735, 333 U.S. 851, 92 L.Ed. 1133, rehearing denied 68 S.Ct. 1336, 334 U.S. 830, 92 L.Ed. 1757. Municipal Corporations 🔑 122.1(2)

Every intendment is in favor of the constitutionality of an **ordinance** and party attacking the validity thereof has the burden of showing that it has no real or substantial relation to public health, morals, safety or general welfare. Portage Tp. v. Full Salvation Union (1947) 29 N.W.2d 297, 318 **Mich**. 693, appeal dismissed 68 S.Ct. 735, 333 U.S. 851, 92 L.Ed. 1133, rehearing denied 68 S.Ct. 1336, 334 U.S. 830, 92 L.Ed. 1757. Municipal Corporations 🔑 122.1(2)

The same presumption of constitutionality applies to a city **ordinance** as to a state statute. People v. Sell (1945) 17 N.W.2d 193, 310 **Mich**. 305. Municipal Corporations 🔑 122.1(2)

Every intendment is in favor of constitutionality of an **ordinance**, and person alleging unconstitutionality thereof has burden of showing that **ordinance** has no real or substantial relation to public health, morals, safety or general welfare. People v. Scrafano (1943) 12 N.W.2d 325, 307 **Mich**. 655. Municipal Corporations 🔑 122.1(2)

As respects presumption of constitutionality, rule applicable to a city **ordinance** is the same as that applied to statutes passed by Legislature. Cady v. City of Detroit (1939) 286 N.W. 805, 289 **Mich**. 499, appeal dismissed 60 S.Ct. 470, 309 U.S. 620, 84 L.Ed. 984. Municipal Corporations 🔑 122.1(2)

Every intendment is in favor of the constitutionality of an **ordinance** under police power, and party attacking **ordinance** has burden of showing that **ordinance** has no substantial relation to public health, morals, safety, or general welfare. Austin v. Older (1938) 278 N.W. 727, 283 **Mich**. 667. Municipal Corporations 🔑 120; Municipal Corporations 🔑 122.1(2)

City licensing and regulation **ordinances** are primarily presumed to be reasonable, but if the inherent character of their provisions appear to be unreasonable, the courts must declare such provisions void. People v. Gibbs (1915) 152 N.W. 1053, 186 **Mich**. 127, Am.Ann.Cas. 1917B,830. Municipal Corporations 🔑 63(2)

19. ---- Proof as to validity of **ordinances**

Person asserting unconstitutionality of **ordinance** has burden of overcoming presumption of constitutionality. People v. Deutsch (1969) 172 N.W.2d 392, 19 Mich.App. 74. Municipal Corporations 🔑 122.1(2)

Duly passed **ordinance** is presumed constitutionally valid, and burden of overcoming presumption is on the defendant. People v. Wedlow (1969) 169 N.W.2d 145, 17 Mich.App. 134. Municipal Corporations 🔑 122.1(2)

As a duly passed legislative act, an **ordinance** is presumed constitutionally valid, and those who seek to defeat it bear the burden of proving that, when tested by constitutional standards, judicial scrutiny will find that the presumption has been overcome. City of Detroit v. Bowden (1967) 149 N.W.2d 771, 6 Mich.App. 514. Municipal Corporations 🔑 122.1(2)

Plaintiffs did not sustain burden of overcoming presumption of validity of municipal **ordinances** defining encroachments on public rights-of-way, providing penalties for violation and prohibiting display of goods, wares or signs of any description on any public property. Elias Bros., Inc. v. City of Hazel Park (1965) 133 N.W.2d 206, 1 Mich.App. 30. Municipal Corporations 🔑 122.1(2)

Generally, presumption prevails in favor of reasonableness and validity in all particulars of municipal **ordinance** , unless contrary is shown by competent evidence, or appears on the face of the enactment. Elias Bros., Inc. v. City of Hazel Park (1965) 133 N.W.2d 206, 1 Mich.App. 30. Municipal Corporations 🔑 122.1(2)

One claiming that a city **ordinance** is arbitrary, unreasonable or discriminatory has burden of so showing. **Michigan** Towing Ass'n v. City of Detroit (1963) 122 N.W.2d 709, 370 **Mich**. 440. Municipal Corporations 🔑 122.1(2)

Every intendment is in favor of constitutionality of an **ordinance** and plaintiff has burden of showing that it has no real or substantial relation to public health, morals, safety, or general welfare, and zoning **ordinances** are constitutional in principle as a valid exercise of the police power. Brown v. Shelby Tp., Macomb County (1960) 103 N.W.2d 612, 360 **Mich**. 299. Municipal Corporations 🔑 120; Municipal Corporations 🔑 122.1(2); Zoning And Planning 🔑 1039

Presumption of validity attaches to **ordinance** adopted and one assailing it has burden of establishing that it is void unless invalidity is such as to appear on face of enactment. Brown v. Shelby Tp., Macomb County (1960)

103 N.W.2d 612, 360 **Mich.** 299. Municipal Corporations 🔑 122.1(2)

Every intendment is in favor of the constitutionality of an **ordinance** under police power, and party attacking **ordinance** has burden of showing that **ordinance** has no substantial relation to public health, morals, safety, or general welfare. Austin v. Older (1938) 278 N.W. 727, 283 **Mich.** 667. Municipal Corporations 🔑 120; Municipal Corporations 🔑 122.1(2)

One asserting the invalidity of a municipal **ordinance** must establish the invalidity, and the court must, if it can consistently do so, give to the **ordinance** such a reasonable construction as will sustain it. Building Commission of City of Detroit v. Kunin (1914) 148 N.W. 207, 181 **Mich.** 604, Am.Ann.Cas. 1916C,959. Municipal Corporations 🔑 122.1(2)

20. ---- Licensing **ordinances**

Despite § 338.751 et seq. which constitutes a comprehensive cosmetology statute, municipality can enact an **ordinance** providing for concurrent local licensing, regulation, and inspection of practice of cosmetology. Op.Atty.Gen.1967, No. 4581, p. 95.

21. ---- Penal **ordinances**, generally

In order to satisfy U.S.C.A. Const. Amend. 14 due process requirements with respect to vagueness, a criminal **ordinance** must give a person of average intelligence fair notice that his contemplated conduct is forbidden by the statute and be narrowly drawn so as not to encourage arbitrary and erratic arrests. Morgan v. City of Detroit, E.D.Mich.1975, 389 F.Supp. 922. Constitutional Law 🔑 4506

In determining whether an **ordinance** is unconstitutionally vague courts traditionally look to the common-law background for interpretation of broad terms. Morgan v. City of Detroit, E.D.Mich.1975, 389 F.Supp. 922. Constitutional Law 🔑 4506

Issue of whether **ordinance** prohibiting keeping more than three dogs on "premises" zoned residential was void for vagueness was not properly before court since defendant did not raise issue below concerning his alleged lease of part of land to his son and since defendant's conviction did not rest on reading "premises" to include entire parcel of land but was based on officer's finding six dogs in one pen behind defendant's premises. People v. Strobridge (1983) 339 N.W.2d 531, 127 Mich.App. 705. Criminal Law 🔑 1030(2)

Fact that determination of question of reasonableness may, on occasion, be required is not sufficient to render **ordinance** too vague to establish practical guide to permissible conduct. People of Dearborn Heights v. Bellock (1969) 169 N.W.2d 347, 17 Mich.App. 163. Municipal Corporations 🔑 111(1)

Requisite of definiteness of penal **ordinance** demands no more than reasonable degree of certainty. People of Dearborn Heights v. Bellock (1969) 169 N.W.2d 347, 17 Mich.App. 163. Municipal Corporations 🔑 594(2)

Penal **ordinance** must have ascertainable standard of guilt and its terms must be sufficiently explicit to inform those who are subject to it as to what conduct on their part will render them liable to its penalties and to guide judges and juries in fair administration of **ordinance** without resort to speculation and conjecture. People of Dearborn Heights v. Bellock (1969) 169 N.W.2d 347, 17 Mich.App. 163. Municipal Corporations 🔑 594(2)

22. ---- Prostitution, **ordinances**

Prostitution is not a problem requiring a statewide regulatory scheme preempting municipal regulation. City of Detroit v. Recorder's Court Traffic and **Ordinance** Judge (1981) 304 N.W.2d 829, 104 Mich.App. 214. Municipal Corporations 🔑 592(1)

23. ---- Breach of the peace, **ordinances**

To be within proscription of breach of peace **ordinance**, disturbance must be outside ordinary course of human conduct and violations of **ordinance** must be restricted to intentional, unreasonable disturbances. People of Dearborn Heights v. Bellock (1969) 169 N.W.2d 347, 17 Mich.App. 163. Disorderly Conduct 🔑 104; Disorderly Conduct 🔑 106

Ordinance making it an offense for anyone to make or assist in making any noise, disturbance, trouble or improper diversion by which peace and good order of city are disturbed was not void on its face or unconstitutionally vague or uncertain when applied to defendant who was the only adult at premises from which loud music was emanating and adjacent to which there were broken beer bottles. People of Dearborn Heights v. Bellock (1969) 169 N.W.2d 347, 17 Mich.App. 163. Municipal Corporations 🔑 594(2); Municipal Corporations 🔑 596

Ordinance making it an offense for any person to make or assist in making any noise, disturbance, trouble or improper diversion, by which peace and good order of city are disturbed may reasonably be construed to proscribe offensive parties without interfering with exercise of constitutionally protected rights. People of Dearborn Heights v. Bellock (1969) 169 N.W.2d 347, 17 Mich.App. 163. Municipal Corporations 🔑 596

24. ---- Enforcement, **ordinances**

Generally, estoppel will not operate to bar enforcement of an **ordinance**, absent exceptional circumstances. Detroit Police Lieutenants and Sergeants Ass'n v. City of Detroit (1974) 224 N.W.2d 728, 56 Mich.App. 617. Estoppel 🔑 62.4

25. ---- Violations, **ordinances**

Defendant could be convicted of violation of Detroit **ordinance** prohibiting ogling, annoying, and molesting by gesture on evidence that he had invited 14-year-old girl into his automobile, offering to "do it" to her and stating that he would "get" her after church. People v. Wilson (1969) 173 N.W.2d 252, 19 Mich.App. 595. Municipal Corporations 🔑 640

Sentence to 50 days in jail, one year's probation, and $150 fine, was within maximum provided by **ordinance** prohibiting ogling, annoying, or molesting by gesture, and exercise of discretion would be sustained. People v. Wilson (1969) 173 N.W.2d 252, 19 Mich.App. 595. Municipal Corporations 🔑 643

26. Powers of cities--In general

Michigan Home Rule City Act authorizes charter cities to exercise any power, enumerated or not, that advances the interests of the city. In re Wilcox, C.A.6 (**Mich.**)2000, 233 F.3d 899, rehearing and suggestion for rehearing en banc denied, certiorari denied 121 S.Ct. 2550, 533 U.S. 929, 150 L.Ed.2d 717. Municipal Corporations 🔑 65

Michigan cities are empowered to enact any **ordinance** or charter provision deemed necessary for the public interest, as long as the enactment is not contrary to or preempted by the state constitution or state laws. In re Wilcox, C.A.6 (**Mich.**)2000, 233 F.3d 899, rehearing and suggestion for rehearing en banc denied, certiorari denied 121 S.Ct. 2550, 533 U.S. 929, 150 L.Ed.2d 717. Municipal Corporations 🔑 64

School districts and other municipal corporations are creations of the state, and except as provided by the state, they have no existence, no functions, no rights and no powers. East Jackson Public Schools v. State (1984) 348 N.W.2d 303, 133 Mich.App. 132. Municipal Corporations 🔑 54; Municipal Corporations 🔑 57; Schools 🔑 21; Schools 🔑 55

City had authority to collect inspection fee pursuant to **ordinance** requiring inspection for sale or transfer of one or two-family residence. Butcher v. City of Detroit (1984) 347 N.W.2d 702, 131 Mich.App. 698. Municipal Corporations 🔑 595

Even though home rule city did not have power concurrent with legislature and in fact needed at least statutory authorization to pass **ordinance** requiring inspection for one and two-family dwellings before sale or transfer, city generally had power to impose such requirement. Butcher v. City of Detroit (1984) 347 N.W.2d 702, 131 Mich.App. 698. Municipal Corporations 🔑 595

In the adoption of rules pursuant to charter authority, the Civil Service Commission is bound by the provisions creating it and defining its powers and duties and in the adoption of **ordinances** the council is likewise limited. Brady v. City of Detroit (1958) 91 N.W.2d 257, 353 **Mich.** 243. Municipal Corporations 🔑 111(1); Municipal Corporations 🔑 216(2)

Under the Home Rule amendment, powers possessed by the city under previous charter of city of Detroit were carried over into the new charter. 1426 Woodward Ave. Corp. v. Wolff (1945) 20 N.W.2d 217, 312 **Mich.** 352. Municipal Corporations 🔑 65

Under C.L.1929, § 2228 et seq., providing for home rule by municipal corporations, there was a general grant of rights and powers subject only to certain enumerated restrictions instead of, as formerly, a grant of enumerated rights and powers definitely specified. City of Pontiac v. Ducharme (1936) 270 N.W. 754, 278 **Mich**. 474. Municipal Corporations 🔑 65

Action of city commissioners in exercising judgment and discretion legally conferred on them is conclusive. Veldman v. City of Grand Rapids (1936) 265 N.W. 790, 275 **Mich**. 100. Municipal Corporations 🔑 63.5

City council and electors each exercise part or the whole of municipal powers when it is so provided by law, and each has only such powers as are conferred by law. City of Niles v. **Michigan** Gas & Elec. Co. (1935) 262 N.W. 900, 273 **Mich**. 255. Municipal Corporations 🔑 60

City under Home Rule Act (P.A.1909, No. 279) has implied power to incorporate in its charter a provision changing fiscal year. City Commission of Jackson v. Hirschman (1931) 235 N.W. 265, 253 **Mich**. 596. Municipal Corporations 🔑 46

While the Legislature of the state functions under broad constitutional limitations, the common council of the city of Detroit must act strictly within its charter powers. L.A. Thompson Scenic Ry. Co. v. McCabe (1920) 178 N.W. 662, 211 **Mich**. 133. Municipal Corporations 🔑 60

27. ---- Source, powers of cities

City of Grand Rapids, under provisions of home rule act (P.A.1909, No. 279) and city charter adopted pursuant thereto, had power to regulate restaurants and other public places of like character including power to revoke licenses if reasonably pertinent to proper regulation. Prawdzik v. City of Grand Rapids (1946) 21 N.W.2d 168, 313 **Mich**. 376. Licenses 🔑 5.5; Municipal Corporations 🔑 611

Municipalities must find their powers in statute, either directly or by charter authorized by general law. City of Niles v. **Michigan** Gas & Elec. Co. (1935) 262 N.W. 900, 273 **Mich**. 255. Municipal Corporations 🔑 57

Municipal corporations are created by law, and all their powers are derived from the statutes creating them, and all their liabilities are thereby imposed. School Dist. of City of Saginaw, East Side, v. School Dist. No. 6 of Buena Vista Tp. (1925) 204 N.W. 737, 231 **Mich**. 664. Municipal Corporations 🔑 69

The citizens of a municipality cannot confer upon the common council functions not left with them by the charter. Torrent v. City of Muskegon (1881) 10 N.W. 132, 47 **Mich**. 115, 41 Am.Rep. 715. Municipal Corporations 🔑 60

28. ---- Limitations, powers of cities

One dealing with the officers of a municipality is bound at his peril to take notice of the limitations upon their power and authority. Schneider v. City of Ann Arbor (1917) 162 N.W. 110, 195 **Mich**. 599; Moore v. City of Detroit (1911) 129 N.W. 715, 164 **Mich**. 543; Rens v. City of Grand Rapids (1889) 41 N.W. 263, 73 **Mich**. 237.

Municipalities have broad discretion in deciding whether to provide particular services to populace and in determining amount and character of service and parties to be served. Alexander v. City of Detroit (1973) 205 N.W.2d 819, 45 Mich.App. 7, reversed on other grounds 219 N.W.2d 41, 392 **Mich.** 30. Municipal Corporations 🔑 57

Constitutionally ordained powers of home rule cities cannot be allowed to be wholly thwarted by failure of Legislature to comply with its own duty to impose limitations on such powers by general law. Dooley v. City of Detroit (1963) 121 N.W.2d 724, 370 **Mich.** 194. Municipal Corporations 🔑 65

Provision of Home Rule Act (§ 117.1 et seq.) giving cities the right to determine the time and manner of nominating and electing judges did not give cities the right to establish qualifications for the office of judge contrary to the qualifications established by the Legislature, and therefore Local Acts of 1895, No. 429, requiring judge of the Recorder's Court of Cadillac to be a qualified attorney was not deleted by electorate's amendment to its city charter deleting such requirement for the judgeship. People ex rel. Wexford County Prosecuting Attorney v. Kearney (1956) 77 N.W.2d 115, 345 **Mich.** 680. Judges 🔑 4

In determining whether an **ordinance** or resolution involves an unconstitutional delegation of legislative power to property owners or other individuals, a distinction is made between **ordinances** or regulations which leave enactment of law to individuals and those prohibitory in character but which permit the prohibition to be modified with the consent of the persons who are to be most affected by such modification, and if such consent is used for no greater purpose than to waive a restriction which legislative authority itself has created and, in which creation, it has made provision for waiver, such consent is generally regarded as being within constitutional limitations. People v. Gottlieb (1953) 59 N.W.2d 289, 337 **Mich.** 276. Municipal Corporations 🔑 591

A city may not prohibit that which is permitted by the state. People v. McDaniel (1942) 5 N.W.2d 667, 303 **Mich.** 90. Municipal Corporations 🔑 592(1)

Persons contracting with municipality through its council, board, commission, or officers, are bound to ascertain whether such bodies, officers, or agents have power to act and to take notice of limits of their authority. Baker v. City of Kalamazoo (1934) 256 N.W. 606, 269 **Mich.** 14. Municipal Corporations 🔑 230

The common council of a city has no power to prescribe new definitions for terms already having legal definitions. Allport v. Murphy (1908) 116 N.W. 1070, 153 **Mich.** 486. Municipal Corporations 🔑 60

Under Detroit City Charter 1904, § 241, requiring contracts involving an expenditure of more than $200 to be let only to the lowest responsible bidder, with adequate security, the city had no power to pass an **ordinance** limiting the hours of labor of employes of city contractors or subcontractors, the effect of which was to increase the bids for city contract work. Bird v. City of Detroit (1908) 116 N.W. 1065, 153 **Mich.** 525. Labor And Employment 🔑 2495(5)

Local Acts 1832, p. 40, § 3, which empowered the common council of the city of Detroit "to make all such by-laws and **ordinances** as may be deemed expedient for the purpose of preventing and suppressing houses of ill fame within the limits of the city" did not authorize the common council by **ordinance** and resolution to require the city marshal to demolish a house occupied as a house of ill fame and adjudged by such council to be a common nuisance. Welch v. Stowell (1846) 2 Doug. 332. Municipal Corporations 🔑 628

A home rule city, under the provisions of the Home Rule Act, (§ 117.1 et seq.) may adopt by reference the Building Code which has been adopted by another home rule city, if such code was promulgated by an organization organized and conducted for that purpose. Op.Atty.Gen.1955-56, No. 2061, p. 304.

A building code prepared through joint action with the City of Detroit may be adopted by one of the participating communities by reference. Op.Atty.Gen.1955-56, No. 2061, p. 304.

A home rule city, under the provisions of the Home Rule Act (§ 117.1 et seq.), could adopt by reference the Plumbing Code of another home rule city. Op.Atty.Gen.1955-56, No. 1963, p. 74.

Territory from two or more counties may not be incorporated into single city. Op.Atty.Gen.1945-46, No. O-3948, p. 466.

Charter commission is not a legislative body, in framing charter for new city to be formed from two old cities, commission could not select **ordinances** of one of the old cities and make them applicable throughout the territory of the new city. Op.Atty.Gen.1928-30, p. 552.

29. ---- Legislative powers of cities

Creation of program designed to facilitate rehabilitation of abandoned single-family dwellings in city was a proper exercise of city council's legislative powers. Moore v. City of Detroit (1985) 382 N.W.2d 482, 146 Mich.App. 448, vacated in part 384 N.W.2d 399, 424 **Mich**. 905, on remand 406 N.W.2d 488, 159 Mich.App. 199, appeal denied. Municipal Corporations 🔑 623(1)

Municipalities are not divested of all control even in areas where legislature has enacted laws, and portions of a field not covered by state law are open to local regulation. Miller v. Fabius Tp. Bd., St. Joseph County (1962) 114 N.W.2d 205, 366 **Mich**. 250. Municipal Corporations 🔑 592(1)

A municipality has power to enact **ordinances** dealing with offenses already prohibited by state statute. Delta County v. City of Gladstone (1943) 8 N.W.2d 908, 305 **Mich**. 50. Municipal Corporations 🔑 592(2)

Ordinance of city of Detroit, enacted pursuant to Home Rule Act (P.A.1909, No. 279), creating a pension fund system for civil employees, was within city's authority. Bowler v. Nagel (1924) 200 N.W. 258, 228 **Mich**. 434. Municipal Corporations 🔑 220(9)

The common council of the city of Detroit may choose its own method of collecting information to guide its legislative discretion, and may, if it chooses, conduct its investigation through a committee of outsiders or through the mayor, providing the investigation is made in its behalf in accordance with its directions, and subject to its control, and the results are reported to it for its action. Attorney General v. Murphy (1909) 122 N.W. 260, 157 **Mich.** 615. Municipal Corporations 🔑 60

The common council of a city is a distinctive and inseparable feature in municipal government under our existing institutions, and cannot be done away with; nor can it be stripped of its legislative powers. People ex rel. Attorney General v. Detroit Common Council (1874) 29 **Mich.** 108. Municipal Corporations 🔑 60

30. ---- Resolutions, powers of cities

Where substance of city action requires adoption of an **ordinance**, a resolution cannot operate as a de facto **ordinance**, and the attempt to legislate by resolution is simply a nullity. Rollingwood Homeowners Corp. v. City of Flint (1971) 191 N.W.2d 325, 386 **Mich.** 258. Municipal Corporations 🔑 85

Size and scope of matters involved are not proper yardsticks for determining whether city action requires adoption of an **ordinance** or whether action can be authorized by resolution of city commission; the difference lies in the nature of the act, not its impact. Rollingwood Homeowners Corp. v. City of Flint (1971) 191 N.W.2d 325, 386 **Mich.** 258. Municipal Corporations 🔑 85

An "**ordinance**" prescribes a permanent rule for conduct of government while a "resolution" is of a special or temporary character. Kalamazoo Municipal Utilities Ass'n v. City of Kalamazoo (1956) 76 N.W.2d 1, 345 **Mich.** 318. Municipal Corporations 🔑 85; Municipal Corporations 🔑 105

If no statute prescribes a method of action and no charter provision requires it, when action is merely declaratory of will of municipal corporation in a given matter, and it is in nature of a ministerial act, it is proper to act by resolution. Case v. City of Saginaw (1939) 288 N.W. 357, 291 **Mich.** 130. Municipal Corporations 🔑 85

Action by the city council of Detroit, amounting merely to a direction to the corporation counsel to institute suit to oust a street railway company from streets as to which its franchise had expired, is an exercise of administrative power, rather than of legislative power, no declaration by the council being necessary to terminate any rights, and so, under the city charter, need not be by "**ordinance**," a permanent continuing regulation, but is properly exercised by a "resolution," an act of a temporary character, not prescribing a permanent rule of government. City of Detroit v. Detroit United Ry. (1921) 184 N.W. 516, 215 **Mich.** 401. Municipal Corporations 🔑 85

It seems that action by a city council is not void merely because taken by motion, instead of by resolution, as provided by its charter. Bishop v. Lambert (1897) 72 N.W. 35, 114 **Mich.** 110. Municipal Corporations 🔑 85

A common council can act only by written resolution. Appeal of Powers (1874) 29 **Mich.** 504. Municipal Corporations 🔑 85

31. ---- Abolishment of offices, powers of cities

Actual words of abolition or their equivalent are not necessary for elimination or abolishing of public office created by city charter amendment when only proper reading of subsequent charter amendment as a whole shows purpose to eliminate or abolish such office. Millard v. Guy (1952) 55 N.W.2d 210, 334 **Mich**. 694. Municipal Corporations 🔑 126

City office is taken subject to contingency that it may be abolished lawfully. Sprister v. City of Sturgis (1928) 218 N.W. 96, 242 **Mich**. 68. Municipal Corporations 🔑 126

32. Taxation--In general

Local units of government may impose only those taxes expressly authorized by state statute. Market Place v. City of Ann Arbor (1984) 351 N.W.2d 607, 134 Mich.App. 567, appeal denied. Municipal Corporations 🔑 956(1)

Procedure whereby a hearing before the board of review on taxpayer's challenge to a real property tax assessment was conditioned upon a prior appearance before the board of assessors was established pursuant to a provision in city charter and, hence, was permissible when not unreasonably restrictive. Fink v. City of Detroit (1983) 333 N.W.2d 376, 124 Mich.App. 44. Municipal Corporations 🔑 974(3)

Ordinances of the City of Detroit providing, inter alia, that any person who had previously complained to the board of assessors with respect to a tax assessment "may appeal" to the common council sitting as a board of review were mandatory rather than voluntary in nature and, as such, required a hearing before the board of assessors a prerequisite to a hearing before the board of review. Fink v. City of Detroit (1983) 333 N.W.2d 376, 124 Mich.App. 44. Municipal Corporations 🔑 974(3)

An appeal before the board of assessors on taxpayer's challenge to a real property tax assessment was a mandatory step to an appeal to the common council sitting as a board of review. Fink v. City of Detroit (1983) 333 N.W.2d 376, 124 Mich.App. 44. Municipal Corporations 🔑 974(3)

A city has the power to create such appeal procedures as are not unreasonably burdensome to a taxpayer's right to appear before the common council sitting as a board of review. Fink v. City of Detroit (1983) 333 N.W.2d 376, 124 Mich.App. 44. Municipal Corporations 🔑 974(3)

A majority vote, under an unconstitutional law, for taxation, for a local purpose, will not render the taxation valid, as an enforcement thereof would deprive the minority of their property without due process of law. Anderson v. Hill (1884) 20 N.W. 549, 54 **Mich**. 477. Constitutional Law 🔑 4135

Taxation for a local purpose cannot be sustained if the law authorizing it be unconstitutional, even though the tax be voted by a majority; for, so far as the minority are concerned, its enforcement deprives them of their property without due process of law. Anderson v. Hill (1884) 20 N.W. 549, 54 **Mich.** 477. Constitutional Law 🔑 4059

A board of tax review is a local governing body empowered by statute to exercise governmental authority and a finding of the board of review is a "decision" within the meaning of § 15.262(d) of the Open Meetings Act (§ 15.261 et seq.); its determinations effectuate public policy, and therefore the meetings of boards of review are subject to the requirements of the Open Meetings Act. Op.Atty.Gen.1978, No. 5281, p. 377, 1978 WL 30698.

If a property owner whose tax assessment is under consideration by a board of review correctly asserts that the discussion of certain matters is exempt, the board may hold a closed session to discuss these matters by affirmative vote of two-thirds of the members. Op.Atty.Gen.1978, No. 5281, p. 377, 1978 WL 30698.

Tax date is home rule cities and villages, when not provided otherwise by city or village charter, is controlled by general tax law. Op.Atty.Gen.1941-42, No. 23194, p. 566.

33. ---- Subjects of taxation

Fact that municipality may derive profit from consumers in course of providing public service does not automatically make it an illegal tax. Alexander v. City of Detroit (1973) 205 N.W.2d 819, 45 Mich.App. 7, reversed on other grounds 219 N.W.2d 41, 392 **Mich.** 30. Municipal Corporations 🔑 956(1)

Provision of this section that subjects of taxation for municipal purposes should be same as for state, county and school purposes under general law applies only to ad valorem taxes on property, and is designed to provide unitary system of taxation and exemption from taxation of property throughout state by all taxing units of government. Dooley v. City of Detroit (1963) 121 N.W.2d 724, 370 **Mich.** 194. Municipal Corporations 🔑 959

Under its charter, the City of St. Clair Shores had ample authority to raise from its citizens by taxation all sums necessary to defray expenses of its municipal operations. Merrelli v. City of St. Clair Shores (1959) 96 N.W.2d 144, 355 **Mich.** 575. Municipal Corporations 🔑 958

Charter amendment of city of Pontiac providing that total amount of taxes assessed against property for all purposes should not exceed 1 1/2 per cent. of assessed valuation, except taxes for debt services, which should be separately assessed, did not impair obligation of city's prior contract with bondholders that all taxes levied for payment of principal and interest on refunding bonds should be levied as part of general city taxes, since bond holders still had same remedies to enforce city's obligation as they would have had before charter amendment. City of Pontiac v. Simonton (1935) 261 N.W. 103, 271 **Mich.** 647. Constitutional Law 🔑 2687; Constitutional Law 🔑 2704; Constitutional Law 🔑 2718

City **ordinance**, creating pension system for civil employees, was not violative of Const.1908, Art. 8, § 25 (see, now Const. Art. 7, §§ 25, 26) prohibiting taxes except for "public purpose." Bowler v. Nagel (1924) 200 N.W. 258, 228 **Mich.** 434. Taxation 🔑 2119

Grave doubt existed as to city's power to levy and collect an income tax, and, therefore, doubt would have to be resolved against the proposed tax. Op.Atty.Gen., 1951-52, No. 1409, p. 249.

Home rule city of 50,000 or less may not levy a tax for a band over the charter tax limitation. Op.Atty.Gen.1945-46, No. O-3867, p. 444.

Home rule city under 150,000 population can levy not to exceed 2 mills above charter tax limitation for a garbage collection system. Op.Atty.Gen.1945-46, No. O-3867, p. 444.

34. ---- Limitations on taxing power

Home rule city, which by electoral vote had adopted an amendment increasing its charter tax limit from 15 mills for city purposes to 18 mills, could not insert in notice of sale of sewage bonds, a provision that bonds would be general obligations of city payable from ad valorem taxes within 18 mills charter tax limit but was required to insert provision that bonds were payable without limitation as to rate or amount, since provision of Municipal Finance Act (P.A.1943, No. 202, c. 7, § 1a, added by P.A.1945, No. 300) forbidding any limitation was required to be read into city's charter and controlled the 18 mill limitation. City of Hazel Park v. Municipal Finance Commission (1947) 27 N.W.2d 106, 317 **Mich.** 582. Municipal Corporations 🔑 79

Charter amendment of city of Pontiac providing that total amount of taxes assessed against property for all purposes should not exceed 1 1/2 per cent. of assessed valuation, except taxes for debt services, which should be separately assessed, placed city within constitutional 15-mill limitation in levying of taxes. City of Pontiac v. Simonton (1935) 261 N.W. 103, 271 **Mich.** 647. Municipal Corporations 🔑 957(3)

Power of taxation of city under Home Rule Act (P.A.1909, No. 279) was not subject to 15-mill constitutional tax limitation. Macomb County v. City of Mount Clemens (1935) 260 N.W. 885, 271 **Mich.** 334. Municipal Corporations 🔑 957(3)

City of Pontiac, operating under home rule charter and general tax limitation of 2 per cent. was authorized and required, under general statute, to exceed such limitation, where necessary for payment of city's bonded indebtedness and interest. Simonton v. City of Pontiac (1934) 255 N.W. 608, 268 **Mich.** 11. Municipal Corporations 🔑 957(3)

Provision limiting total amount of taxes assessed to 1 1/2 per cent. of assessed valuation did not change right of villages and fourth class cities to exercise power of local self-government and to fix tax limits for local purposes. School Dist. of City of Pontiac v. City of Pontiac (1933) 247 N.W. 474, 262 **Mich.** 338, rehearing denied 247 N.W. 787, 262 **Mich.** 338. Municipal Corporations 🔑 957(3)

Personal property acquired after April 1 cannot be added to Detroit assessment rolls. Detroit Trust Co. v. City of Detroit (1929) 227 N.W. 715, 248 **Mich**. 612. Municipal Corporations 🔑 966(1)

Provision of Const. Art. 7, §§ 6, 21, limiting total amount of general ad valorem taxes which may be levied by different units does not apply to home rule cities and would not apply to charter counties under proposed legislation prescribing tax limitations upon levy by county of ad valorem taxes. Op.Atty.Gen.1966, No. 4523.

35. ---- Levy and collection of taxes

Home rule cities have power to make all reasonable provisions for collection of ad valorem taxes. City of Detroit v. Walker (1994) 520 N.W.2d 135, 445 **Mich**. 682. Municipal Corporations 🔑 73

Where there was no showing that assessing officer of city added more than one per cent tax in excess of 20-mill limitation of city charter, or that formula used was discriminatory as to mining corporation, corporation was not entitled to enjoin collection of taxes. Sunday Lake Iron Co. v. City of Wakefield (1949) 35 N.W.2d 470, 323 **Mich**. 497. Municipal Corporations 🔑 979

Since state tax commission could not affect assessment and tax rolls as to city purposes after they had been delivered to collecting officer on or before July 1, and since there could not be one set of valuations for city purposes and another set of valuations for county purposes as determined in Board of State Commissioners, there was no deliberate and willful intent on part of assessing officer of city to disregard his duty in making assessments against mining corporation when he persisted in levying a ten mill rate in city despite correction made on roll by state tax commission, so as to entitle mining corporation to maintain a suit to enjoin collection of taxes. Sunday Lake Iron Co. v. City of Wakefield (1949) 35 N.W.2d 470, 323 **Mich**. 497. Municipal Corporations 🔑 979

The levying of municipal taxes is a matter of municipal prerogative to be exercised by proper municipal authorities and chancery court cannot substitute its judgment for that of municipal authorities or board of regents of state university as to whether taxes should be levied or contracts entered into for the furnishing of public facilities by city to university property. Lucking v. People (1948) 31 N.W.2d 707, 320 **Mich**. 495. Municipal Corporations 🔑 63.15(5)

Where provision of Detroit home-rule charter for a tax sale, other than a judicial sale, for city taxes was valid, and Detroit school taxes were levied and collected in the same manner as city taxes, the collection of school taxes by city of Detroit by means of a tax sale, other than a judicial sale, was proper. City of Detroit v. Collateral Liquidation (1940) 295 N.W. 218, 295 **Mich**. 440. Schools 🔑 106.34(1)

C.L.1929, § 2228 et seq. recognizing power of city to levy taxes contemplated power to make all reasonable provisions for collection thereof. City of Detroit v. Safety Inv. Corp. (1939) 285 N.W. 42, 288 **Mich**. 511. Municipal Corporations 🔑 978(1)

State could, by appropriate legislation, provide that sale for state and county taxes with purchase by and subsequent deed by state vests title in grantee free from contemporaneous taxes levied by city, if city upon notice by grantee of right to redeem does not redeem, but such legislation would have to be plainly expressed and could not be accomplished by construction or implication. Hoffman v. Otto (1936) 269 N.W. 225, 277 **Mich**. 437. Taxation 🔑 3068

Tax deed for state and county taxes did not vest title in grantee free from contemporaneous taxes levied by city, notwithstanding city upon notice by grantee of right to redeem did not redeem, since city was not required to redeem under notice given and so lost no rights in failing to do so. Hoffman v. Otto (1936) 269 N.W. 225, 277 **Mich**. 437. Taxation 🔑 3068

The legislature has power to correct any mere irregularity in the proceeding for the assessment and collection of taxes authorized by law, but, if the original tax was levied without any authority of law, such a curative act could not make it a legal demand. Hart v. Henderson (1868) 17 **Mich**. 218. Constitutional Law 🔑 4135

A city which levies and collects municipal taxes under its charter due on December 1, may not collect school taxes on the preceding July 1. Op.Atty.Gen.1981, No. 5859, p. 60, 1981 WL 153381.

Village tax anticipation notes are not legal tender for payment of taxes. Op.Atty.Gen.1930-32, p. 485.

A home rule city may not require city treasurer to accept tax anticipation bonds or notes in payment of special assessments in view of requirements for conformity to general law with respect to collection of taxes and requirements that **ordinances** be subject to the constitution and general laws, and general law provisions governing legal tender and disposition of funds collected. Op.Atty.Gen.1930-32, p. 481.

36. ---- Exemption from taxation

Michigan state apple commission is a state agency authorized to perform governmental functions only and personal property owned by it is exempt from general taxation by a home rule city. Op.Atty.Gen.1955-56, No. 2842, p. 737.

37. ---- Refunds of taxes, taxation

Charter provision that common council may direct refund of taxes illegally collected should be construed as requiring repayment by city. Blanchard v. City of Detroit (1931) 235 N.W. 230, 253 **Mich**. 491. Municipal Corporations 🔑 977

38. Police power--In general

Among the powers that may properly be exercised by a home rule city is the police power. Belle Isle Grill Corp. v. City of Detroit (2003) 666 N.W.2d 271, 256 Mich.App. 463. Municipal Corporations 🔑 65

Except where limited by constitution or statute, the police power of a home rule city is of the same general scope and nature as that of the state. Belle Isle Grill Corp. v. City of Detroit (2003) 666 N.W.2d 271, 256 Mich.App. 463. Municipal Corporations 🔑 589

Police power belongs to municipality only if specifically conferred on it by statute or by Constitution. Butcher v. City of Detroit (1984) 347 N.W.2d 702, 131 Mich.App. 698. Municipal Corporations 🔑 589

Ordinance prohibiting keeping more than three dogs on premises in areas zoned residential was constitutional exercise of city's police power. People v. Strobridge (1983) 339 N.W.2d 531, 127 Mich.App. 705. Zoning And Planning 🔑 1081

Municipal police power relates not merely to public health and public physical safety but also to public financial safety and laws may be passed within police power to protect public from financial loss. People v. Murphy (1961) 110 N.W.2d 805, 364 **Mich**. 363. Municipal Corporations 🔑 595

All property is held subject to right of government to regulate its use in exercise of police power, so that it shall not be injurious to rights of community, or so that it may promote its health, morals, safety and welfare. Patchak v. Lansing Tp. (1960) 105 N.W.2d 406, 361 **Mich**. 489. Zoning And Planning 🔑 1007

Ownership of property remains subject to reasonable exercise of police power. Lamb v. City of Monroe (1959) 99 N.W.2d 566, 358 **Mich**. 136. Municipal Corporations 🔑 600; Zoning And Planning 🔑 1007

A bottle club, designed to circumvent the liquor laws, in which soft drinks or mixes and food are sold as in the ordinary restaurant and which is run for the profit of an individual, is subject to the broad police power given to home rule cities. Mutchall v. City of Kalamazoo (1948) 35 N.W.2d 245, 323 **Mich**. 215. Food 🔑 1.6

Emergencies may require enactment of statutes or **ordinances** under police power which might be held improper in normal times. People v. Sell (1945) 17 N.W.2d 193, 310 **Mich**. 305. Municipal Corporations 🔑 589; States 🔑 21(2)

City **ordinances** designed to regulate municipal development, secure home life, preserve a favorable environment in which to rear children, protect morals and health, safeguard economic structure upon which public good depends, stabilize use and value of property, and to attract a desirable citizenship are within proper ambit of police power. Cady v. City of Detroit (1939) 286 N.W. 805, 289 **Mich**. 499, appeal dismissed 60 S.Ct. 470, 309 U.S. 620, 84 L.Ed. 984. Municipal Corporations 🔑 594(1); Municipal Corporations 🔑 597; Municipal Corporations 🔑 598; Zoning And Planning 🔑 1039

Municipal regulation which, reasonably applied, will promote community development, finds support in the police power. Cady v. City of Detroit (1939) 286 N.W. 805, 289 **Mich**. 499, appeal dismissed 60 S.Ct. 470, 309 U.S. 620, 84 L.Ed. 984. Municipal Corporations 🔑 594(1)

A municipality, under its general police power, has authority to adopt proper and reasonable **ordinances** having for their purposes the prevention of fires. Harrigan & Reid Co. v. Burton (1923) 195 N.W. 60, 224 **Mich**. 564. Municipal Corporations 🔑 603

While the legal incorporation and organization of a city for local governmental purposes necessarily invests it with primary police powers within the conceded sphere of such power fundamentally essential to the ends for which it was created, yet beyond the narrow limits of such necessary implication the police power must be expressly delegated by the Constitution or Legislature. Clements v. McCabe (1920) 177 N.W. 722, 210 **Mich**. 207. Municipal Corporations 🔑 590

Notwithstanding Const.1908, Art. 8 (see, now, Const. Art. 7), dealing with cities and villages, and giving general powers in § 21 (see, now, § 22) to regulate municipal concerns, or the so-called Home Rule Act (P.A.1909, No. 279), providing for protection of public health and property and for regulation of trade and occupations, the city of Detroit operating under a home rule charter was without authority under the guise of its police power to impose restrictions on otherwise unrestricted property by a general zoning system excluding trades and businesses from particular areas, and hence such attempted restrictions are invalid. Clements v. McCabe (1920) 177 N.W. 722, 210 **Mich**. 207. Zoning And Planning 🔑 1011

An **ordinance** making it an offense to indecently expose the person, without reference to the intent which accompanies the act, is a valid exercise of police power. City of Grand Rapids v. Bateman (1892) 53 N.W. 6, 93 **Mich**. 135. Municipal Corporations 🔑 598

Home rule city had authority under the police power to enact **ordinance** which required homeowners to connect to city water system, even though **ordinance** affected homeowner's valuable property right to groundwater. City of Gaylord v. Maple Manor Investments, LLC (2006) 2006 WL 2270494, Unreported. Water Law 🔑 2116

A city may adopt a housing-property maintenance code pursuant to its general police powers authorized by P.A.1909, No. 279, § 4j (§ 117.4j), despite the fact that P.A.1909, No. 279, § 3(k) [§ 117.3(k)] neither authorizes nor prohibits such adoption by reference. Op.Atty.Gen.1978, No. 5280, p. 393, 1978 WL 30704.

39. ---- Public peace, health and safety, generally, police power

City did not breach contract with tenant that leased concession stand on island by curtailing traffic to island as part of police plan to reduce traffic congestion and crime, as plan was an exercise of city's police power. Belle Isle Grill Corp. v. City of Detroit (2003) 666 N.W.2d 271, 256 Mich.App. 463. Municipal Corporations 🔑 722

City has right to make even innocent acts unlawful if these acts have a tendency to affect or endanger public in connection with health, safety, morals or general welfare. People v. Deutsch (1969) 172 N.W.2d 392, 19 Mich.App. 74. Municipal Corporations 🔑 595; Municipal Corporations 🔑 597; Municipal Corporations 🔑 598

There is a strong presumption in favor of the validity and constitutionality of local **ordinances** passed under statutory authorization to promote the health, morals, safety and welfare of the community. Johnson Const. Co. v. White Lake Tp. (1958) 88 N.W.2d 426, 351 **Mich**. 374. Municipal Corporations 🔑 122.1(2)

Where common council, in passing **ordinance**, declared **ordinance** to be necessary for preservation of public peace, health, and safety, although such declaration was not conclusive of power to enact, it was indicative of purpose of **ordinance**. People v. Pennock (1940) 293 N.W. 759, 294 **Mich**. 578. Municipal Corporations 🔑 595; Municipal Corporations 🔑 596; Municipal Corporations 🔑 597

City could lawfully offer reward for information leading to apprehension and conviction of violators of state law within city boundaries. Visch v. City of Grand Rapids (1932) 244 N.W. 488, 260 **Mich**. 318. Rewards 🔑 4

In matters of public health, of police, and such activities, municipalities act as agents of the state. Attorney General v. City of Detroit (1923) 196 N.W. 391, 225 **Mich**. 631. Municipal Corporations 🔑 590

While an individual has an inherent or natural right to engage in any lawful business on his own property, the nature of the business sought to be carried on may be such as to render it subject to regulatory control by the city in the interest of the public peace, health, morals, and general welfare, and such regulation may be exercised so long as it is reasonable, without discrimination, and fair to all alike. Melconian v. City of Grand Rapids (1922) 188 N.W. 521, 218 **Mich**. 397. Municipal Corporations 🔑 600

Enactment of nuisance abatement **ordinance**, allowing city commission to declare rental property to be public nuisance if it is used repeatedly for illegal drugs or prostitution and to padlock such property for one year, was valid exercise of city's police power in light of threat to public health, safety and welfare from illegal drug use and prostitution. Rental Property Owners Ass'n of Kent County v. City of Grand Rapids (1997) 566 N.W.2d 514, 455 **Mich**. 246. Nuisance 🔑 60

City of Lincoln Park could not refuse to furnish police and fire protection and other services to Liquor Control Commission warehouse in city in absence of city's payment of cost of such protection and services. Op.Atty.Gen.1957-58, No. 3242, p. 131.

In the city of Harper Woods, by charter and **ordinance**, the city manager, having the duty to see that the public peace and safety is maintained and to direct the chief of police in the manner and methods, has the implied power to employ a private investigator to investigate crime, without authority of the counsel subject to funds being available, and the mayor as conservator of the peace, has no such implied power. Op.Atty.Gen.1955-56, No. 2565, p. 283.

Ordinance of home rule city adopted under charter provision relating to public peace and health and to the safety of persons and property regulating steam boilers within city more stringently than state regulations is not in conflict with state law. Op.Atty.Gen.1945-46, No. O-2483, p. 12.

40. ---- Health measures, generally, police power

City refuse collection **ordinance**, under which waste from certain apartment buildings with more than four units was classed as "commercial" and subject to charges for refuse services provided free to others in a like class, contained a constitutionally improper classification denying equal protection under M.C.L.A. Const. Art. 1, § 1 and U.S.C.A. Const. Amend. 14, § 1. Alexander v. City of Detroit (1974) 219 N.W.2d 41, 392 **Mich.** 30. Constitutional Law 🔑 3533

Detroit water fluoridation **ordinance** is designed to protect or improve public health and is reasonable and lawful exercise of police power and does not conflict with charter requirements for furnishing pure and wholesome water. Rogowski v. City of Detroit (1965) 132 N.W.2d 16, 374 **Mich.** 408. Municipal Corporations 🔑 597; Water Law 🔑 1867; Water Law 🔑 2009

A city as a unit is responsible for the health of the entire city and each part thereof. Southfield Tp. v. Main (1959) 97 N.W.2d 821, 357 **Mich.** 59. Municipal Corporations 🔑 597

Grand Rapids **ordinance** providing for the regulation of restaurants in the interest of public health, insofar as it provides for revocation of licenses by city commission, is not objectionable as vesting commission with arbitrary power in light of provision prescribing a definite standard and procedure to be observed for protection of rights of a licensee. Prawdzik v. City of Grand Rapids (1946) 21 N.W.2d 168, 313 **Mich.** 376. Municipal Corporations 🔑 591

Under **ordinance** forbidding manufacture within city limits of mattresses from unsterilized secondhand material, evidence that defendant manufactured, but did not sell, mattress of secondhand material, and that defendant manufactured and sold within city mattress made from either shoddy or smak, justified conviction for violation of **ordinance** as to both mattresses. People v. Dushkin (1936) 268 N.W. 765, 276 **Mich.** 643. Municipal Corporations 🔑 640

It is legitimate exercise of municipal power to prevent spread of infectious diseases among workers in factory as well as the public at large. People v. Dushkin (1936) 268 N.W. 765, 276 **Mich.** 643. Municipal Corporations 🔑 597

Ordinance authorizing city commission to issue license for used automobile dealer business to "proper and suitable person" at "proper and suitable place" provided "proper sanitary facilities" were maintained could not be sustained as reasonable health measure where there was nothing about business which made it inherently dangerous to public health. People v. Sturgeon (1935) 262 N.W. 58, 272 **Mich.** 319. Municipal Corporations 🔑 597

A township, city, village or charter county when authorized by its charter may adopt air pollution control **ordinances**, provided that such **ordinances** are reasonably related to public health, safety and welfare and are no less stringent than corresponding requirements of federal and state air pollution control laws. Noncharter counties may not adopt air pollution control **ordinances.** Op.Atty.Gen.1998, No. 6992, 1998 WL 477690.

41. ---- Pollution, police power

Sole aim of city smoke abatement **ordinance** is the elimination of air pollution to protect the health and enhance the cleanliness of local community. Huron Portland Cement Co. v. City of Detroit, **Mich.**, U.S.Mich.1960, 80 S.Ct. 813, 362 U.S. 440, 4 L.Ed.2d 852. Environmental Law 🔑 245

Cities of Escanaba and Gladstone, home rule cities with power and duty to protect health and welfare of their people, could adopt **ordinances** to control air pollution to an extent which would constitute a "reasonable exercise of the local police power" to protect the health and safety of the inhabitants; such authority does not conflict with, and is not pre-empted by, the Air Pollution Act, § 336.11 et seq. Op.Atty.Gen.1970, No. 4696, p. 197.

Existing authority of local governmental units, such as home rule cities, villages, and townships, to adopt air pollution control **ordinances** is preserved by the Air Pollution Control Act, § 336.11 et seq., but scope of state law extends beyond all such local power and, to extent of the overreach, controls. Op.Atty.Gen.1970, No. 4696, p. 197.

42. ---- Smoke detectors, police power

A home rule city is authorized to require by **ordinance**, the installation of smoke detectors in structures built prior to the effective date of the state construction code (§ 125.1501 et seq.). Op.Atty.Gen.1978, No. 5264, p. 346, 1978 WL 30687.

Pursuant to the provisions of this section of the Home Rule Cities Act (§ 117.1 et seq.), a Home Rule City may adopt an **ordinance** requiring installation of smoke detectors in buildings within the city; the city may draft its own **ordinance** specifying the type or style of smoke detector required in each classification of buildings or adopt by reference the law, code or rules of a state agency or other organization which provides for smoke detection devices. Op.Atty.Gen.1978, No. 5264, p. 346, 1978 WL 30687.

Since pursuant to P.A.1917, No. 167, § 8 (§ 125.408), a Home Rule City may enact an **ordinance** exceeding the minimum fire prevention requirements as stated in P.A.1917, No. 167, § 82 (§ 125.482), an **ordinance** requiring smoke detection devices in buildings within the city is authorized. Op.Atty.Gen.1978, No. 5264, p. 346, 1978 WL 30687.

43. ---- Sunday laws, police power

Generally, governing body of a municipality clothed with power to enact and enforce **ordinances** for observance of Sunday is vested with discretion in determining kinds of pursuits, occupations, or businesses to be included or excluded, and its determination will not be interfered with by courts provided classification and discrimination made are founded upon reasonable distinctions and have some reasonable relation to public peace, welfare and safety. People's Appliance & Furniture, Inc. v. City of Flint (1959) 99 N.W.2d 522, 358 **Mich.** 34. Municipal Corporations 🔑 63.20; Sunday 🔑 2

Under Home Rule Act (§ 117.1 et seq.), cities are authorized to require business places to be closed on Sunday, such requirement being a sanitary measure not in conflict with general law of the State. Petition of Berman (1956) 75 N.W.2d 8, 344 **Mich**. 598. Municipal Corporations 🔑 592(1)

Enactment of **ordinance** requiring closing of furniture and appliance stores on Sunday except for persons who observe seventh day of week as Sabbath was valid exercise of police power. Petition of Berman (1956) 75 N.W.2d 8, 344 **Mich**. 598. Sunday 🔑 2

Under municipal **ordinance** providing for closing of furniture and appliance stores on Sunday but exempting persons who conscientiously believe that seventh day of week should be observed as the Sabbath and actually refrain from such secular business and labor on that day, one who kept one store closed on Saturday but opened on Sunday and kept two other stores open on Saturday was guilty of violation. Petition of Berman (1956) 75 N.W.2d 8, 344 **Mich**. 598. Sunday 🔑 5

A city **ordinance** prohibiting the sale and distribution of groceries and meats on Sunday was not invalid as class legislation, notwithstanding that it did not apply to all commodities. People v. Krotkiewicz (1938) 282 N.W. 852, 286 **Mich**. 644. Sunday 🔑 2

Municipal **ordinance**, declaring it unlawful "to sell or offer for sale any groceries or meats or to keep any grocery store, meat market or other place in which groceries or meats are sold or kept for sale, on the first day of the week, commonly called Sunday," was not void for uncertainty. People v. Derose (1925) 203 N.W. 95, 230 **Mich**. 180. Sunday 🔑 2

Lansing City Charter, c. 4, § 59, subd. 38, authorizing council to make regulations necessary for safety and good government of city and general welfare of its inhabitants, authorized council's adoption of **ordinance** prohibiting selling of groceries and meats on Sunday or keeping open of place therefor. People v. Derose (1925) 203 N.W. 95, 230 **Mich**. 180. Sunday 🔑 2

Municipal **ordinance** prohibiting sale of groceries or meats on Sunday or keeping open of place therefor, exempting drug stores, tobacco shops, and other places, was not invalid as class legislation. People v. Derose (1925) 203 N.W. 95, 230 **Mich**. 180. Sunday 🔑 2

To "keep open," in the sense of the Sunday **ordinance** "relative to quiet and good order," implies a readiness to carry on the usual business in the "store, shop, saloon," etc., and, if this business is not within the exceptions of the **ordinance**, the offence is committed. Miles v. Goffinet (1868) 16 **Mich**. 472.

44. Officers and employees--In general

There was evidence to support finding of jury that intent of city, which hired plaintiffs for jobs in connection with city-established special program for testing, counseling and selection of youths for occupational training by means of letter which failed to set forth specified period of time but gave salary at an annual rate, was that the contracts of employment would be for a one-year period. Hall v. City of Detroit (1970) 177 N.W.2d 161, 383 **Mich**. 571. Municipal Corporations 🔑 217.6

Those dealing with public officials must take notice of their powers. Kaplan v. City of Huntington Woods (1959) 99 N.W.2d 514, 357 **Mich**. 612. Municipal Corporations 🔑 230

Persons dealing with a municipal corporation through its officers must at their peril take notice of the authority of particular officer to bind corporation, and if officer's act is beyond limits of his authority, municipality is not bound. Sittler v. Board of Control of **Michigan** College of Min. & Technology (1952) 53 N.W.2d 681, 333 **Mich**. 681. Municipal Corporations 🔑 230

A representative is one chosen by a principal to exercise for him a power, or perform for him a trust, and implies as much a particular purpose as a particular person; and a person authorized by a city to represent it for one purpose cannot be clothed by the state with authority in purely local matters to represent the city for another and different purpose for which it had no power to appoint him originally. People ex rel. Board of Detroit Park Com'rs v. Detroit Common Council (1873) 28 **Mich**. 228, 15 Am.Rep. 202. Municipal Corporations 🔑 67(1)

45. ---- Appointment, officers and employees

Act No. 419, Local Acts of 1893, supplemental to charter of the city of Detroit providing that the city counselor shall be appointed by the mayor, for the term of three years, repealed the provision of the charter that the city counselor shall be appointed by the common council on the nomination of the mayor, and vested the exclusive power of appointment in the mayor. Ellis v. Corliss (1894) 57 N.W. 410, 98 **Mich**. 372; Speed v. Common Council of City of Detroit (1893) 56 N.W. 570, 97 **Mich**. 198.

City charter provision that vacancy in office of commissioner shall be filled by appointment by a majority of remaining members must be read in connection with provision relating to number of commissioners necessary to constitute a quorum and providing that a less number than a quorum may adjourn from day to day and compel the attendance of absent members, and two members constituting less than a quorum had no power to fill a vacancy in commission. Burns v. Stenholm (1945) 17 N.W.2d 781, 310 **Mich**. 639. Municipal Corporations 🔑 90

Where notice of special meeting of city commissioners stated that it was for purpose of submitting proposed **ordinance** to electors, but contained no provisions relative to the appointment to fill vacancies in commission, and only three of the five members were present one of whom objected to consideration of appointment, resolutions concerning appointments to fill vacancies were void. Burns v. Stenholm (1945) 17 N.W.2d 781, 310 **Mich**. 639. Municipal Corporations 🔑 89; Municipal Corporations 🔑 90

Under charter of Battle Creek, approved in 1913, the city attorney in office at the time of the approval continues, and one appointed by the newly elected mayor was not even a de facto officer. North v. City of Battle Creek (1915) 152 N.W. 194, 185 **Mich**. 592. Municipal Corporations 🔑 149(4)

Grand Rapids city charter provides that appointed officers shall hold their offices for a period of one year from the time of their appointment unless sooner removed; that, whenever a vacancy occurs in any office, the council may fill it, but, if elective, it shall continue only until the first Monday of the next May and a new election shall be held at the annual election, and by another section an officer "elected" shall hold over after his term until his successor is elected or appointed and qualified; the council was not precluded from filling an office held by appointment of the council where no one was holding it for a regular term. Saunders v. City of Grand Rapids (1881) 9 N.W. 495, 46 **Mich**. 467. Municipal Corporations 🔑 149(1)

46. ---- Dual office-holding, officers and employees

It was within authority of the Home-Rule Act (§ 117.1 et seq.) to impose as a qualification for office of councilman that person holding such office not be employed by any other unit of government which raises its operating budget in whole or in part by public taxation. Doyle v. City of Dearborn (1963) 121 N.W.2d 473, 370 **Mich**. 236 . Municipal Corporations 🔑 142

A member of the state Legislature at the time of his election to council of a home-rule city making it unlawful for any elective officials to hold any position on another public payroll had an option either to resign from the Legislature and qualify as councilman or to refuse the oath as councilman and stay in the Legislature, but he could not validly hold both offices. Doyle v. City of Dearborn (1963) 121 N.W.2d 473, 370 **Mich**. 236. Municipal Corporations 🔑 142

47. ---- Eligibility requirements, officers and employees

De jure status of councilmen, who had been duly elected to office and who had not been challenged as to their right to perform functions thereof, could not be collaterally attacked by persons challenging action of council in overriding mayor's veto of certain provisions of city budget adopted by council. Detroit Police Officers Ass'n v. City of Detroit (1969) 170 N.W.2d 260, 17 Mich.App. 700. Officers And Public Employees 🔑 80

Where one is in public office exercising authority thereof under color of law, except in a direct proceeding to test his right to office, court cannot pass on right to hold office, and there is no difference between acts of de facto and de jure officers insofar as public interests are concerned. Detroit Police Officers Ass'n v. City of Detroit (1969) 170 N.W.2d 260, 17 Mich.App. 700. Officers And Public Employees 🔑 80

Party does not have a right to directly attack official act of legislative body of municipality through collateral attack on credentials of its membership. Detroit Police Officers Ass'n v. City of Detroit (1969) 170 N.W.2d 260, 17 Mich.App. 700. Officers And Public Employees 🔑 80

City council, which under charter provision was the judge of the eligibility and qualification of its own members but which had refused to judge the eligibility of an allegedly ineligible member, was empowered to take formal action on its own motion to judge eligibility of member. Crossman v. Hanson (1966) 143 N.W.2d 783, 4 Mich.App. 98. Municipal Corporations 🔑 84

A local city or village charter may contain a provision barring a person convicted of a felony from eligibility to seek an office within a local governmental unit, and such a charter provision would not violate the equal protection provisions of M.C.L.A.Const. Art. 1, § 2 or U.S.C.A.Const. Amend. 14. Op.Atty.Gen.1980, No. 5647, p. 594, 1980 WL 114015.

A city charter provision making eligibility to file as a candidate for or hold an elective or appointive city office dependent upon two years' residency in the city violates equal protection of the law under Const. Art 1, § 2. Op.Atty.Gen.1979, No. 5552, p. 364, 1979 WL 36882.

Under city charter provision that vacancy would be deemed to exist in administrative office if officer moved from city, office of city assessor became vacant when officer moved from city to township and officer was then ineligible to hold office and to represent city on county board of supervisors. Op.Atty.Gen.1957-58, No. 3277, p. 213.

City charter may contain provision excluding from office one who is in default to the city, but the term, "default" contemplates a willful omission to account or pay over funds belonging to the city with a corrupt intention and does not bar one who is merely delinquent in payment of taxes. Op.Atty.Gen.1935-36, No. 120, p. 316.

48. ---- Salaries, officers and employees

Charter retirement pensions, insurance premium payments and the furnishing of uniforms were "compensation" within city of Flint charter provision that like classifications of work are to receive like compensation, notwithstanding that city could legally discontinue these benefits. Kane v. City of Flint (1955) 69 N.W.2d 156, 342 **Mich**. 74. Municipal Corporations 🔑 220(2)

Provision in city of Flint charter that like classifications of work are to receive like compensation does not deprive city commission of its power to fix compensation of all officers and employees of city. Kane v. City of Flint (1955) 69 N.W.2d 156, 342 **Mich**. 74. Municipal Corporations 🔑 162; Municipal Corporations 🔑 220(1)

Personnel regulation providing that so far as is practicable, grants of leave shall be made prior to beginning of period of absence and no payment for absence shall be made unless leave is properly approved, but that if employee is unable, by reason of illness or incapacity, to file application for leave in time for payment for absence on payroll for period of which absence occurred, such payment may be secured on subsequent payroll after leave has been granted, is applicable to a grant of sick leave. Sovia v. City of Saginaw (1952) 51 N.W.2d 910, 332 **Mich**. 373. Municipal Corporations 🔑 220(5)

If interpretation had been placed on language of resolution setting forth salary plan for civil service employees, at variance with its clearly expressed intent, such interpretation would be disregarded by the court. Dearborn Fire Fighters Ass'n v. City of Dearborn (1949) 35 N.W.2d 366, 323 **Mich**. 414. Municipal Corporations 🔑 220(2)

Under resolution of city council setting forth salary plan for civil service employees, employees were entitled to have their compensation determined on basis fixed in the resolution regardless of any failure on part of civil service board and common council to agree as to the salaries to be paid for any fiscal year. Dearborn Fire Fighters Ass'n v. City of Dearborn (1949) 35 N.W.2d 366, 323 **Mich**. 414. Municipal Corporations 🔑 220(2)

Where charter required civil service board to prepare salary plan for civil service employees and common council adopted a proposed plan which provided for cost of living adjustments determined from reports published by the United States Department of Labor, civil service employees were entitled to cost of living adjustment in salaries as provided in plan without the necessity of action by the civil service board, approved by the council. Dearborn Fire Fighters Ass'n v. City of Dearborn (1949) 35 N.W.2d 366, 323 **Mich**. 414. Municipal Corporations 🔑 220(2)

Claims for interest and amounts withheld from salaries of employees of the city of Detroit during the depression were not required to be presented to the common council for audit as required by the city charter provision in order to maintain an action thereon, where city had previously paid part of the claims and offered to pay the balance on execution of a release which the employees refused to sign. Thal v. City of Detroit (1947) 25 N.W.2d 598, 316 **Mich**. 497. Municipal Corporations 🔑 220(8)

Where city charter provided that remuneration of city employees should be set by the director of each respective department, and that the city civil service board's salary plan when adopted should constitute the official salary plan for the city positions, city council, without consent of board, could not order city comptroller to pay city employees additional compensation to cover increased cost of living. Local 321, State, County and Mun. Workers of America, C.I.O. v. City of Dearborn (1945) 19 N.W.2d 140, 311 **Mich**. 674. Municipal Corporations 🔑 220(3)

City's tax budget for fiscal year, even if it included an estimated amount to meet pay of the city employees, did not irrevocably devote tax collections thereunder to continuance of any particular pay to employees. Detroit Mun. Employees Ass'n v. City of Detroit (1944) 17 N.W.2d 858, 310 **Mich**. 480. Municipal Corporations 🔑 220(2)

Where part of city employees' salaries was deducted under invalid **ordinance**, and thereafter city council passed resolution authorizing city controller and treasurer to honor payrolls for one-half of total sum of each employee's pay, payment under such resolution of one-half of claims of employees waived need of subsequent presentation for other half of same claims in common council for audit, so that delay in bringing action to recover money deducted did not constitute laches. Detroit Mun. Employees Ass'n v. City of Detroit (1944) 17 N.W.2d 858, 310 **Mich**. 480. Municipal Corporations 🔑 220(8)

City charter which provided that failure to present claims or demands to council for audit or allowance would bar action barred action by employee for compensation while wrongfully laid off, notwithstanding claim was liquidated. Burkheiser v. City of Detroit (1935) 259 N.W. 125, 270 **Mich**. 381. Municipal Corporations 🔑 220(8)

Board of estimates of city of Saginaw was empowered to reduce several items of estimate of council relating to payment of salaries of officers and employees employed by council or of employees hired by several commissioners in their respective departments. Council of City of Saginaw v. Board of Estimates of City of Saginaw (1932) 239 N.W. 872, 256 **Mich**. 624. Municipal Corporations 🔑 220(3)

City charter fixing salaries of commissioners or councilmen and mayor has force of law. Council of City of Saginaw v. Board of Estimates of City of Saginaw (1932) 239 N.W. 872, 256 **Mich**. 624. Municipal Corporations 🔑 58

Under the charter of the city of Detroit, where the board of estimates has stricken an item for the salary of a certain clerk from the estimate for the expenses of a department, the controller cannot be compelled by the council to draw a warrant for the salary of such clerk, though provided to be paid from a fund derived otherwise than from taxation. City of Detroit v. Blades (1903) 94 N.W. 1134, 133 **Mich**. 249. Municipal Corporations 🔑 220(7)

The legislature has the power to fix the salaries of public officers, and to change them at any time even during terms of office, and it may delegate such power to municipal councils. City of Wyandotte v. Drennan (1881) 9 N.W. 500, 46 **Mich**. 478. Municipal Corporations 🔑 67(5)

Even though salaries of election officials of a home rule city are determined by the Local Officers Compensation Commission, the members of the city council may establish and pay fringe benefits to the city officials, including members of the council. Op.Atty.Gen.1978, No. 5255, p. 327, 1978 WL 30678.

49. ---- Overtime compensation, officers and employees

Overtime service of employees of city of Highland Park was rendered in an "emergency" so as to entitle employees to overtime compensation under city charter, where serious loss, damage, or impairment of city services would have resulted if city employees had not worked overtime. Olson v. City of Highland Park (1946) 21 N.W.2d 286, 312 **Mich**. 688. Municipal Corporations 🔑 220(2)

The acceptance and endorsement of semimonthly pay checks for regular salary did not constitute either a waiver or estoppel precluding city employees from claiming overtime compensation pursuant to city charter amendment. Olson v. City of Highland Park (1945) 20 N.W.2d 773, 312 **Mich**. 688, rehearing denied 21 N.W.2d 286, 312 **Mich**. 688. Municipal Corporations 🔑 220(2)

50. ---- Gratuities and annuities, officers and employees

A city lacks power to pay gratuities, and, if retirement pension plan were deemed payment of gratuity, it would be ultra vires. Kane v. City of Flint (1955) 69 N.W.2d 156, 342 **Mich**. 74. Municipal Corporations 🔑 220(9); Municipal Corporations 🔑 871

The Dearborn city **ordinance**, requiring members of city employees retirement system to contribute 5 per cent of their compensation to annuity reserve fund and requiring city council to appropriate and city to pay into annuity reserve fund annually amount of city's contribution thereto, as determined by actuary under mortality and other tables adopted by board of trustees of system, created no contract finding city to contribute amount so determined. Thiesen v. Parker (1948) 31 N.W.2d 806, 320 **Mich.** 446. Municipal Corporations 🔑 220(9)

51. ---- Mayor, officers and employees

Complaint which sought to compel mayor and city police commissioner to change methods with respect to police recruitment and discipline in certain specified areas with respect to civil rights failed to state a cause of action under Civil Rights Act (42 U.S.C.A. § 1981 et seq.) since alleged derelictions were mere conclusions unsupported by any allegation of fact. Peek v. Mitchell, C.A.6 (**Mich.**)1970, 419 F.2d 575. Mandamus 🔑 99

Ordinance providing that no amusement park license shall be issued unless place for which it is to be issued complies with all laws and **ordinances**, and with all rules and regulations of building department, police department, and board of health, and in opinion of mayor is a safe and proper place to be used as an amusement park, does not constitute delegation of arbitrary power, but rather confers upon mayor a proper discretion and contemplated action, not upon whim or caprice, but upon disinterested and impartial exercise of judgment in reasonable manner in interest of public. Tower Realty v. City of East Detroit, C.A.6 (**Mich.**)1952, 196 F.2d 710. Municipal Corporations 🔑 591

A city charter providing for the election by the council of one of their number as mayor does not conflict with the Home Rule Act (P.A.1909, No. 279). Kopczynski v. Schriber (1917) 161 N.W. 238, 194 **Mich.** 553. Municipal Corporations 🔑 124(2)

52. ---- Treasurer, officers and employees

Fact that city treasurers had determined investment policy for surplus funds for many years without objection from city council did not establish the treasurer's right to do so where city charter and state statute (§ 129.91) were to the contrary. City of Warren v. Dannis (1984) 357 N.W.2d 731, 136 Mich.App. 651, appeal denied. Municipal Corporations 🔑 884

City treasurer did not have the right to refuse to sign checks to pay debts when the disbursements had been duly authorized by the city council, since no section of the city charter granted treasurer the power to refuse to disburse funds as authorized by the council, and since, in issuing checks per council orders, the treasurer would be acting in a ministerial capacity. City of Warren v. Dannis (1984) 357 N.W.2d 731, 136 Mich.App. 651, appeal denied. Municipal Corporations 🔑 883

A deputy city treasurer may attend meetings of the police and fire pension board in place of the city treasurer and may act in his stead; however, the duties and responsibilities of the city treasurer may not be supplanted or substituted by those of his deputy; rather, ultimate responsibility remains with the city treasurer and his deputy acts as his agent in his absence. Op.Atty.Gen.1976, No. 4913, p. 244.

53. ---- Police officers, officers and employees

Ordinance requiring that city police officers be residents of city was unreasonable and invalid when applied to officers, who, prior to enactment of **ordinance,** had established homes outside of city in reliance on police commissioner's express written waiver of residency rule then in effect. Detroit Police Lieutenants and Sergeants Ass'n v. City of Detroit (1974) 224 N.W.2d 728, 56 Mich.App. 617. Municipal Corporations 🔑 184(2)

Detroit common council had power to pass **ordinance** which unqualifiedly required its police officers to reside in city. Detroit Police Officers Ass'n v. City of Detroit (1971) 190 N.W.2d 97, 385 **Mich.** 519, appeal dismissed 92 S.Ct. 1173, 405 U.S. 950, 31 L.Ed.2d 227. Municipal Corporations 🔑 184(2)

Section 24 of the charter of the city of Traverse City, incorporated under P.A.1909, No. 279, which provided that no person should be eligible as a candidate for any elective office in the city unless 25 years of age, a citizen of the United States, and should have resided in the city and been a taxpayer for five years, etc., did not require that an appointive officer, such as police marshal, be a citizen of the United States. Coxe v. Carson (1916) 160 N.W. 534, 194 **Mich.** 304.

Emergency reserve police officers meeting the training requirements of the Law Enforcement Officers Training Council Act of 1965, § 28.601 et seq. and whose duties potentially include patrolling city streets and parks in marked police vehicles, issuing citations and making arrests, may be employed by a home rule city. Op.Atty.Gen.1984, No. 6235, p. 335, 1984 WL 192577.

54. Contracts

Persons contracting with municipality through its council, board, commission, or officers, are bound to ascertain whether such bodies, officers, or agents have power to act and to take notice of limits of their authority. Utica State Sav. Bank v. Village of Oak Park (1937) 273 N.W. 271, 279 **Mich.** 568; Baker v. City of Kalamazoo (1934) 256 N.W. 606, 269 **Mich.** 14.

Quitclaim deed by city of Detroit to county of Wayne of portion of city park for erection of children's welfare shelter for nondelinquent children was not invalid merely because action of Detroit common council authorizing deed was by resolution rather than by **ordinance**. Brozowski v. City of Detroit (1957) 87 N.W.2d 114, 351 **Mich.** 10. Municipal Corporations 🔑 85

To extent that terms and conditions of public employment are governed by statute or charter, they are not subject to modification by contract, and concerted labor activity instigated for purpose of affecting terms and conditions is not sanctioned by law. City of Detroit v. Division 26 of Amalgamated Ass'n of Street, Elec. Ry. & Motor Coach Employees of America (1952) 51 N.W.2d 228, 332 **Mich.** 237, appeal dismissed 73 S.Ct. 37, 344 U.S. 805, 97 L.Ed. 627, rehearing denied 73 S.Ct. 164, 344 U.S. 882, 97 L.Ed. 683. Labor And Employment 🔑 1423; Municipal Corporations 🔑 244(1)

Contract of home rule city for construction of sewer was not ultra vires although a budget containing no item for sewer construction was adopted prior to date of execution of contract, and city was precluded from issuing additional bonds. DiPonio v. Garden City (1948) 30 N.W.2d 849, 320 **Mich**. 230. Municipal Corporations 🔑 868(1)

Evidence sustained $7,000 judgment for plaintiff against city for services rendered as an appraiser of property to be condemned at $50 a day for the appraisal and $25 a day for a reappraisal to bring the appraisal up to date. Ely v. City of Detroit (1943) 10 N.W.2d 892, 306 **Mich**. 300. Municipal Corporations 🔑 220(8)

Where city's common council had authorized corporation counsel to institute condemnation proceedings, corporation counsel, as a necessary incident to preparation of the case and without further approval of common council, was authorized to employ plaintiff to appraise property to be condemned and to reappraise the property to bring his original appraisals up to date notwithstanding charter provision requiring city's contracts to be approved by the common council. Ely v. City of Detroit (1943) 10 N.W.2d 892, 306 **Mich**. 300. Municipal Corporations 🔑 214(1)

Where draftsman claimed contract with municipality for year's employment at fixed salary, it was required to be shown that terms of contract, at least in broad outline, were before the city officials, stating names of parties and other important terms, before approval of such contract by municipality could be found. Brubaker v. City of Detroit (1937) 276 N.W. 460, 282 **Mich**. 309. Municipal Corporations 🔑 220(8)

Where plaintiff, who was employed by municipality as junior civil draftsman for Rapid Transit Commission, was interviewed by chief engineer of the commission to determine what compensation was acceptable to plaintiff, and budget, approved by city officials, purpose of which was only to estimate expenditures, contained item "Junior Civil Draftsmen (3) $7200," and detailed minutes of the commission made no reference to contract with plaintiff for year's employment at $2,400, no such contract existed between municipality and plaintiff so as to entitle plaintiff to such salary. Brubaker v. City of Detroit (1937) 276 N.W. 460, 282 **Mich**. 309. Municipal Corporations 🔑 220(2)

Under charter authorizing municipality to acquire property by purchase or in other ways therein provided, municipality was entitled to enter into contract to purchase property. City of Pontiac v. Ducharme (1936) 270 N.W. 754, 278 **Mich**. 474. Municipal Corporations 🔑 224

Contract to purchase land for sewage disposal site acquired by municipality through a realty agent who took property in his own name and then assigned to municipality, when transaction was then ratified, was valid, as against contention transaction was invalid because there was not a strict compliance with charter provisions regarding proceeding by **ordinance** or resolution and forbidding liabilities to be incurred by any officer of city. City of Pontiac v. Ducharme (1936) 270 N.W. 754, 278 **Mich**. 474. Municipal Corporations 🔑 224

55. Meetings

Where a special meeting of city commissioners is called for purpose of electing or removing officers, the facts should be stated in the notice of the meeting and the necessity of such notice can only be waived by consent of all members, and a unanimity of consent to transact any business, ordinary or extraordinary, should plainly appear from the recorded declaration, acts or conduct. Burns v. Stenholm (1945) 17 N.W.2d 781, 310 **Mich.** 639. Municipal Corporations 🔑 89; Municipal Corporations 🔑 100

Where notice of special meeting of city commissioners stated that it was for purpose of submitting proposed **ordinance** to electors, but contained no provisions relative to the appointment to fill vacancies in commission, and only three of the five members were present one of whom objected to consideration of appointment, resolutions concerning appointments to fill vacancies were void. Burns v. Stenholm (1945) 17 N.W.2d 781, 310 **Mich.** 639. Municipal Corporations 🔑 89; Municipal Corporations 🔑 90

Action taken at a special meeting of a city council is not invalid for want of proof of due notice of the meeting, where it appears from the record of the vote taken that all of the members were present. Turner v. Hutchinson (1897) 71 N.W. 514, 113 **Mich.** 245. Municipal Corporations 🔑 89

56. Appropriations

Where budget prepared in November, 1952, and appropriation **ordinance** passed in January, 1953, were based on equalized valuation for city of certain amount, and in May, 1953, Board of Supervisors of county increased valuation for city, city commission could amend appropriation order and appropriate additional available revenue not provided for in original budget or original appropriation **ordinance** for acquisition and development of public parking lots. Stolorow v. City of Pontiac (1954) 63 N.W.2d 611, 339 **Mich.** 199. Municipal Corporations 🔑 889.1

The Dearborn city **ordinance**, empowering board of trustees of city employees retirement system to determine amount of city's contribution to annuity reserve fund, without fixing any standards to guide board, except by provisions that it shall adopt mortality and other tables deemed necessary and compute such amount on basis of actuarial valuation of system's assets and liabilities under such tables, is invalid as delegating power to make appropriations and, indirectly, power to impose taxes partly to administrative board, contrary to home rule act (P.A.1909, No.279). Thiesen v. Parker (1948) 31 N.W.2d 806, 320 **Mich.** 446. Municipal Corporations 🔑 220(9); Municipal Corporations 🔑 858; Municipal Corporations 🔑 956(1)

Under home rule provisions of Constitution and City Home Rule Act (P.A.1909, No. 279), city of Kalamazoo had right to join the **Michigan** Municipal League, avail itself of such league's services, and expend money from public funds in payment therefor; such expenditures being for city "public purpose". Hays v. City of Kalamazoo (1947) 25 N.W.2d 787, 316 **Mich.** 443. Municipal Corporations 🔑 861

A city's contribution of public funds in payment of annual dues to **Michigan** Municipal League for services thereof in presenting to members and committees of legislature statistics, information and arguments respecting merits of legislation affecting municipal problems, such as operation of public utilities, is not against public policy, though league officers and agents may take position at variance with that of city in particular instance. Hays v. City of Kalamazoo (1947) 25 N.W.2d 787, 316 **Mich.** 443. Municipal Corporations 🔑 861

A charter provision that no resolution appropriating money shall be adopted by the council except by a specified vote cannot be evaded by embracing such action in the form of a motion. Bishop v. Lambert (1897) 72 N.W. 35, 114 **Mich.** 110. Municipal Corporations 🔑 85

Judicial proceedings are not by the provision of the Constitution made a necessary prerequisite to the appropriation of property by the government under the power of taxation. Weimer v. Bunbury (1874) 30 **Mich.** 201. Constitutional Law 🔑 4135

57. Wards

Home Rule Law (P.A.1909, No. 279), allowing cities to reduce the number of wards to one when adopting a new charter, presumably contemplated that the number of members of the board of education might change accordingly. MacQueen v. City Commission of City of Port Huron (1916) 160 N.W. 627, 194 **Mich.** 328. Municipal Corporations 🔑 211

58. Powers and duties of courts--In general

Courts may consider and pass upon reasonableness of municipal **ordinances** based upon general home **rule** powers and not specifically authorized by charter or statute. State, County and Municipal Emp. Local 339, AFL-CIO v. City of Highland Park (1961) 108 N.W.2d 898, 363 **Mich.** 79. Municipal Corporations 🔑 63.20

Wisdom or desirability of action by law-making body of city was not before Supreme Court. Gray v. Grand Trunk Western R. Co. (1958) 91 N.W.2d 828, 354 **Mich.** 1. Municipal Corporations 🔑 63.10

While it is within the province of the courts to pass upon the validity of statutes and **ordinances**, courts may not legislate or undertake to compel legislative bodies to do so one way or another. Randall v. Township Bd. of Meridian Tp., Ingham County (1955) 70 N.W.2d 728, 342 **Mich.** 605. Constitutional Law 🔑 2473; Municipal Corporations 🔑 63.1

While it is within province of courts to pass upon validity of statutes and **ordinances**, courts may not legislate or undertake to compel legislative bodies to do so one way or another. Tel-Craft Civic Ass'n v. City of Detroit (1953) 60 N.W.2d 294, 337 **Mich.** 326. Constitutional Law 🔑 2473; Municipal Corporations 🔑 63.1

Judgment of municipal officers in execution of powers conferred upon them by law or charter is not subject to control and correction by courts in absence of fraud or clear abuse of discretion. Moran v. Leadbetter (1952) 54 N.W.2d 310, 334 **Mich.** 234. Municipal Corporations 🔑 63.5

To warrant interposition of court of equity in municipal affairs, there must be a malicious intent, capricious action, or corrupt conduct, something which shows action of body whose acts are complained of did not arise from exercise of judgment and discretion vested by law in them. Moran v. Leadbetter (1952) 54 N.W.2d 310, 334 **Mich.** 234. Municipal Corporations 🔑 63.5

While it is within province of courts to pass upon validity of statutes and **ordinances**, courts may not legislate nor undertake to compel legislative bodies to do so one way or another. Northwood Properties Co. v. Perkins (1949) 39 N.W.2d 25, 325 **Mich.** 419. Constitutional Law 🔑 2473; Municipal Corporations 🔑 63.1

Municipal **ordinances** although ostensibly enacted as public regulations which are so framed as to control or regulate a common and useful private business or occupation are subject to review and investigation in courts to determine validity by test of whether under guise of police regulation there is arbitrary, unreasonable or unwarranted interference with constitutional rights of private citizens to pursue lawful business or calling and to make contracts with others in relation thereto. S.S. Kresge Co. v. Couzens (1939) 287 N.W. 427, 290 **Mich.** 185. Municipal Corporations 🔑 63.15(3); Municipal Corporations 🔑 63.20

The local governmental policy of municipality, the power to govern which is vested by the people in local municipal officers in pursuance of law, cannot be dictated by the courts. Nelson v. Wayne County (1939) 286 N.W. 617, 289 **Mich.** 284. Municipal Corporations 🔑 63.1

Acts of legally authorized city commissioners are not subject to judicial control. Veldman v. City of Grand Rapids (1936) 265 N.W. 790, 275 **Mich.** 100. Municipal Corporations 🔑 63.1

Discretion vested in city officials is not subject to review by courts. White v. City of Grand Rapids (1932) 244 N.W. 469, 260 **Mich.** 267. Municipal Corporations 🔑 63.5

Whether an **ordinance** is reasonable, and within the range of the discretionary power of the municipal authorities, is a judicial question. People v. Gibbs (1915) 152 N.W. 1053, 186 **Mich.** 127, Am.Ann.Cas. 1917B,830. Municipal Corporations 🔑 63(2)

59. ---- Interference by courts, generally, powers and duties of courts

Judiciary will not interfere in discretionary acts of municipal governments, absent fraud or a clear abuse of discretion. Brent v. City of Detroit (1970) 183 N.W.2d 908, 27 Mich.App. 628. Municipal Corporations 🔑 63.5

In order to warrant interposition of court of equity in municipal affairs, there must be a malicious intent, capricious action, or corrupt conduct. Detroit Fire Fighters Ass'n Local No. 344, I.A.F.F. v. Board of Fire Com'rs of City of Detroit (1962) 114 N.W.2d 195, 366 **Mich.** 45. Municipal Corporations 🔑 63.1

To warrant the interposition of a court of equity in municipal affairs, there must be a malicious intent, capricious action, or corrupt conduct, something which shows the action of the body whose acts are complained of did not arise from an exercise of judgment and discretion vested by law in them. City of North Muskegon v. Bolema Const. Co. (1953) 56 N.W.2d 371, 335 **Mich.** 520. Municipal Corporations 🔑 63.5

Where a municipality has power to engage in an activity for a public purpose, the courts will not interfere with the discretionary acts of its municipal officials. City of North Muskegon v. Bolema Const. Co. (1953) 56

N.W.2d 371, 335 **Mich**. 520. Municipal Corporations 🔑 63.15(1)

Where municipality has power to engage in activity for public purpose, courts will not interfere with discretionary acts of municipal officials. Moran v. Leadbetter (1952) 54 N.W.2d 310, 334 **Mich**. 234. Municipal Corporations 🔑 63.15(1)

Where a municipality has power to engage in an activity for a public purpose, the courts will not interfere with discretionary acts of its municipal officials. Wolgamood v. Village of Constantine (1942) 4 N.W.2d 697, 302 **Mich**. 384. Municipal Corporations 🔑 63.5

Courts are not disposed to interfere with the management of an authorized business, conducted by the municipal authorities presumably in the interest of and for the benefit of the city and its inhabitants unless dishonesty or fraud is manifest, or the vested power with its implied discretion has been clearly exceeded or grossly abused. Nelson v. Wayne County (1939) 286 N.W. 617, 289 **Mich**. 284. Municipal Corporations 🔑 63.15(1)

Court cannot interfere with discretion of city commission so long as commission's action is not contrary to law or opposed to sound public policy. Veldman v. City of Grand Rapids (1936) 265 N.W. 790, 275 **Mich**. 100. Municipal Corporations 🔑 63.5

Courts cannot dictate local governmental policy of municipality, the government and control of which has been vested by people in local municipal officers in pursuance of law. Veldman v. City of Grand Rapids (1936) 265 N.W. 790, 275 **Mich**. 100. Municipal Corporations 🔑 63.1

Court of equity will not interfere in municipal affairs unless body whose acts are complained of acted with malicious intent, capricious action, or corrupt conduct showing body did not exercise judgment and discretion vested in it by law. Veldman v. City of Grand Rapids (1936) 265 N.W. 790, 275 **Mich**. 100. Municipal Corporations 🔑 63.5

60. ---- Mandamus as remedy, powers and duties of courts

Mandamus proceedings to compel the restoration of an alderman to a seat from which he has been wrongfully removed by the council do not concern the legality of his title. Doran v. De Long (1882) 12 N.W. 848, 48 **Mich**. 552. Mandamus 🔑 77(4)

Where the charter of a city makes the common council the final judges of the election of aldermen, mandamus will not lie to compel them to reinstate one whom they had excluded without a proper hearing on the merits. People ex rel. Cooley v. Fitzgerald (1879) 2 N.W. 179, 41 **Mich**. 2. Mandamus 🔑 77(4)

61. ---- Injunction as remedy, powers and duties of courts

Generally, a court of equity has no power to restrain violation of a criminal statute or **ordinance**, but where facts form a basis for equitable relief, jurisdiction of court will not be destroyed by fact that a criminal act will be restrained. Garfield Tp. v. Young (1954) 66 N.W.2d 85, 340 **Mich**. 616. Injunction 🔑 102

Where facts form basis for equitable relief, jurisdiction of court of equity is not destroyed by the fact that a criminal act will be restrained. Township of Warren v. Raymond (1939) 289 N.W. 201, 291 **Mich**. 426. Injunction 🔑 102

A court of equity had jurisdiction to enjoin breach of a municipal **ordinance** forbidding the removal of garbage. Board of Health of City of Grand Rapids v. Vink (1915) 151 N.W. 672, 184 **Mich**. 688. Injunction 🔑 85(1); Injunction 🔑 102

A building **ordinance** authorizing the department of buildings to stop the construction or removal of any building constructed in violation of the **ordinance**, and, if the order be not obeyed, to apply to any court, empowers the department of buildings to sue in equity to enjoin a threatened violation of the **ordinance**. Building Commission of City of Detroit v. Kunin (1914) 148 N.W. 207, 181 **Mich**. 604, Am.Ann.Cas. 1916C,959. Injunction 🔑 102

62. Claims against cities

Presentment of claim pursuant to requirement of city charter is not required if it would be a useless gesture. Fulco, Inc. v. Martin Tropf & Sons, Inc. (1971) 193 N.W.2d 194, 36 Mich.App. 39. Municipal Corporations 🔑 1001

Where third-party defendant city by resolution declared contractor engaged to construct hangars at municipal airport to be in default and terminated its right to proceed, so that contractor's presentment of claim under contract to common council of City as required by city charter would have been a useless gesture, contractor was excused from complying with presentment of claims provision. Fulco, Inc. v. Martin Tropf & Sons, Inc. (1971) 193 N.W.2d 194, 36 Mich.App. 39. Municipal Corporations 🔑 1001

Operation of airport by City of Detroit was a governmental and municipal function, and, therefore, presentment of claims provision of city charter was applicable to contract claim filed against city in connection with construction of hangars at airport. Fulco, Inc. v. Martin Tropf & Sons, Inc. (1971) 193 N.W.2d 194, 36 Mich.App. 39. Municipal Corporations 🔑 1001

63. Elections

Subdivision (c) of this section may be construed to permit advisory elections as means of carrying out some of powers given to city council by city charter, but did not authorize city council to spend public funds in straw vote in area entirely outside powers of city council. Southeastern **Michigan** Fair Budget Coalition v. Killeen (1986) 395 N.W.2d 325, 153 Mich.App. 370. Municipal Corporations 🔑 65

Case involving validity of petition for special election to amend city charter involved public question, and no costs would be awarded. Grosse Pointe Farms Fire Fighters Ass'n v. Caputo (1968) 157 N.W.2d 695, 11 Mich.App. 112. Costs 🔑 221

Proposed purchase and use of voting machines by City of Detroit was not violative of statute or charter. Moran v. Leadbetter (1952) 54 N.W.2d 310, 334 **Mich.** 234. Elections 🔑 222; Municipal Corporations 🔑 221

A city charter providing for the election by the council of one of their number as mayor does not conflict with, requiring each city charter to provide for the election of a mayor, since "election" is not limited in its meaning to the process of choosing a person for a public office by vote of the qualified electors (citing Words and Phrases, First and Second Series, Election). Kopczynski v. Schriber (1917) 161 N.W. 238, 194 **Mich.** 553.

A provision in the charter of a home rule city which prohibits the election or appointment to any office, within 3 years after a petition for his recall and removal, a person who has been removed from any office by recall or who has resigned from such office after a petition for his recall and removal has been filed, is valid. Op.Atty.Gen.1976, No. 4956, p. 364.

City of Detroit having adopted home rule charter may change time of holding elections by means of charter amendment without the necessity of obtaining an enabling act. Op.Atty.Gen.1945-46, No. O-3040, p. 182.

64. Records

In view of Detroit City Charter, c. 1, § 17, the mere filing of the "Building Code" of the city, a book of 504 sections, in 156 pages, with the city clerk, did not give it the character of a public record, enabling the common council by means of an **ordinance** to adopt and approve of it by reference simply to its several articles. L.A. Thompson Scenic Ry. Co. v. McCabe (1920) 178 N.W. 662, 211 **Mich.** 133. Municipal Corporations 🔑 114

Where for convenience examiners temporarily removed records, and papers from office of city treasurer and thereafter turned them over to prosecutor for use as evidence against such city treasurer, the prosecutor, in holding them, was in no better position than had he secured them by unlawful search and seizure. Barnard v. Dunham (1916) 158 N.W. 202, 191 **Mich.** 567. Records 🔑 13

Where the city prosecutor, without legal authority, holds public records of the city treasurer's office for evidence in a prosecution of such officer for embezzlement, the court in which the prosecution is pending has discretion to order such records deposited with the clerk of court for free access to defendant. Barnard v. Dunham (1916) 158 N.W. 202, 191 **Mich.** 567. Records 🔑 13

65. Rates

Under provision of § 141.121 that rates for services furnished by public improvements shall be fixed and revised from time to time by the governing body of the borrower and provision of § 141.103 defining "governing body" to mean, in case of a city, the body having legislative powers, city council of home rule city had final authority for fixing water and sewer rates despite charter provision stating that a charter-created department of water supply should periodically establish such rates. Op.Atty.Gen.1975, No. 4886, p. 129.

66. Governmental immunity

Where officers who had called for backup assistance at time of street fight were acting during course of their employment and within scope of their authority, and decision to request and await backup assistance was impliedly authorized by Constitution (Const.Art. 7, § 22), statute (§ 117.3) and city charter, city was entitled to governmental immunity from tort liability for injuries which arose during street fight. Ross v. Consumers Power Co. (1984) 363 N.W.2d 641, 420 **Mich**. 567. Municipal Corporations 🔑 747(3)

Emergency assistance system and police dispatch system, including internal procedures for determining seriousness of calls in dispatching vehicles, are impliedly authorized by Constitution (Const. Art. 7, § 22), statute (§ 117.3) and city charter; thus, where injury arose while city's employees were engaged in exercise or discharge of governmental function in prioritizing calls which came over emergency system, city was entitled to governmental immunity from tort liability in action in which it was alleged that plaintiff's parents sustained fatal injuries as result of delayed response to emergency call. Ross v. Consumers Power Co. (1984) 363 N.W.2d 641, 420 **Mich**. 567. Municipal Corporations 🔑 747(3)

Police officers were entitled to governmental immunity from damages for death of occupant of automobile involved in high-speed chase where police officers were engaged in governmental function in attempting to apprehend vehicle. Custard v. McCue (1983) 335 N.W.2d 104, 124 Mich.App. 612. Automobiles 🔑 187(1)

Complaint alleging that operators and dispatcher failed to correctly interpret emergency calls and failed to dispatch police vehicles quickly did not make out a claim for intentional tort; operators and dispatcher were engaged in activity that was in exercise or discharge of governmental function, and, thus, city was immune from liability. Trezzi v. City of Detroit (1982) 328 N.W.2d 70, 120 Mich.App. 506, affirmed 363 N.W.2d 641, 420 **Mich**. 567. Municipal Corporations 🔑 742(4); Municipal Corporations 🔑 747(3)

City's operation of emergency dispatch system was essentially a unique activity associated with operation of police department, and, thus, it was a governmental function entitled to immunity from tort liability. Trezzi v. City of Detroit (1982) 328 N.W.2d 70, 120 Mich.App. 506, affirmed 363 N.W.2d 641, 420 **Mich**. 567. Municipal Corporations 🔑 747(3)

M. C. L. A. 117.3, MI ST 117.3

The statutes are current through P.A.2012, No. 200, 202-224 of the 2012 Regular Session, 96th Legislature.

END OF DOCUMENT

January 31, 2012

Federal Trade Commission
600 Pennsylvania Avenue N.W.
Room H-113 (Annex P)
Washington, DC 20580

On behalf of the Security Industry Association (SIA), I would like to thank you for the opportunity to comment on the FTC's workshop, "Face Facts," A Forum on Facial Recognition, Project No. P115406 held on December 8, 2011. SIA represents more than 400 manufacturers, integrators, dealers, and specifiers of electronic physical security solutions. Facial recognition technology can be used within security systems and therefore SIA members have a direct interest in this proceeding.

The benefits of using facial recognition in a commercial setting are many. For example, facial recognition technology can be an effective tool in promoting public safety. Facial recognition can screen for known threats and automatically alert facility staff or public safety officers. The technology could also provide after-incident forensic analysis that would assist law enforcement, and biometric identification can be used to raise the level of security in applications like access control. It could also allow small businesses to track coarse retail demographics such as gender and age without recognizing particular individuals. And facial recognition technologies are used every day in consumer applications such as digital photography and video to improve image quality.

The FTC workshop addressed a number of important topics that will impact the use of this technology within security systems and other applications. For instance, the workshop addressed the issue of whether facial recognition technology always enables personal identification. In our view - whether the technology collects personal information or not - appropriate notification as to <u>what is being collected</u> is currently considered "best practice" in the industry and that practice should continue.

SIA urges the Commission to recognize a distinction between facial detection and facial recognition or identification. As you know, facial detection describes technologies that can detect the presence of a human face (such as its applications to allow you to take better pictures) or identify certain demographic characteristics of a face. This abstract information is stored in aggregate and without retaining the captured images or identifying the individuals. This is in contrast to facial recognition applications that "match a face with a name." Second, SIA believes that consumers should have appropriate notice and the ability to "opt-in" to the use of facial recognition that is linked to personal identification. This opt-in could facilitate rapid service processes which require personal identification (such as airline check-in) and its use in high security access control application where access is tied to an enrolled biometric identifier. Particularly in public applications, consumers should always have notice and the option to opt-out by using alternative methods of identification.

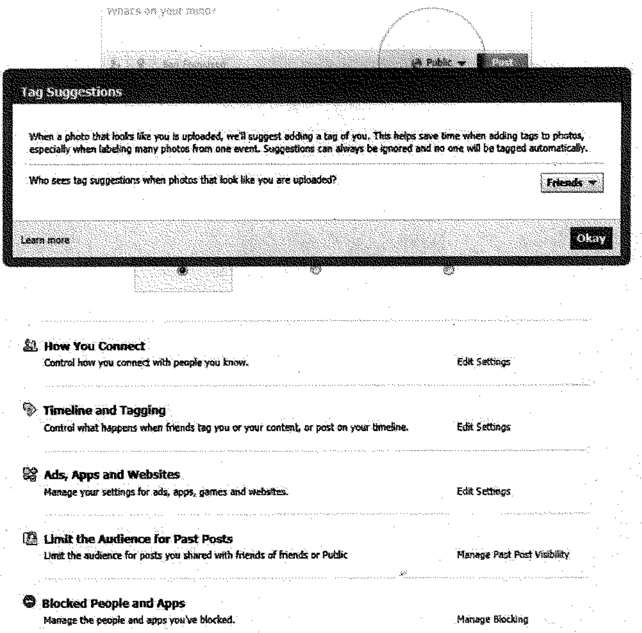
Further, privacy controls should be adjusted for the duration of any image retention by an application. For example, an application that catalogs the image of every person who enters a given store and retains that information indefinitely creates a requirement for explicit disclosure. On the other hand, an application that does not store images and only extract demographic data, which is then kept in aggregate, may require fewer privacy controls.

SIA is proud of its members' leadership in the area of enabling privacy-protecting enhancements within security systems. In 2011, SIA members adopted a "Privacy Framework" that describes certain principles and serves as a guide for the government and industry in striking the right balance between privacy and security. The document is scheduled for review but the current SIA Privacy Framework can be found on the SIA website (http://goo.gl/TK3kB).

Thank you for the opportunity to provide comments on this important proceeding. SIA is prepared to work with you as you continue your examination of facial recognition technology. Many SIA members participate in the use and development of software, hardware and other applications relevant to facial recognition and would appreciate being involved with any policy or regulation development.

Sincerely,

Don Erickson
Chief Executive Officer
Security Industry Association



Tag Suggestions

When a photo that looks like you is uploaded, we'll suggest adding a tag of you. This helps save time when adding tags to photos, especially when labeling many photos from one event. Suggestions can always be ignored and no one will be tagged automatically.

Who sees tag suggestions when photos that look like you are uploaded? Friends ▾

Learn more

Okay

How You Connect
Control how you connect with people you know. Edit Settings

Timeline and Tagging
Control what happens when friends tag you or your content, or post on your timeline. Edit Settings

Ads, Apps and Websites
Manage your settings for ads, apps, games and websites. Edit Settings

Limit the Audience for Past Posts
Limit the audience for posts you shared with friends of friends or Public Manage Past Post Visibility

Blocked People and Apps
Manage the people and apps you've blocked. Manage Blocking

C

Effective: September 1, 2009

Vernon's Texas Statutes and Codes Annotated Currentness
Business and Commerce Code (Refs & Annos)
Title 11. Personal Identity Information
Subtitle A. Identifying Information
Chapter 503. Biometric Identifiers
→→ **§ 503.001. Capture or Use of Biometric Identifier**

(a) In this section, "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.

(b) A person may not capture a biometric identifier of an individual for a commercial purpose unless the person:

(1) informs the individual before capturing the biometric identifier; and

(2) receives the individual's consent to capture the biometric identifier.

(c) A person who possesses a biometric identifier of an individual that is captured for a commercial purpose:

(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

(A) the individual consents to the disclosure for identification purposes in the event of the individual's disappearance or death;

(B) the disclosure completes a financial transaction that the individual requested or authorized;

(C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or

(D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose in response to a warrant;

(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a

manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses; and

(3) shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the purpose for collecting the identifier expires, except as provided by Subsection (c-1).

(c-1) If a biometric identifier of an individual captured for a commercial purpose is used in connection with an instrument or document that is required by another law to be maintained for a period longer than the period prescribed by Subsection (c)(3), the person who possesses the biometric identifier shall destroy the biometric identifier within a reasonable time, but not later than the first anniversary of the date the instrument or document is no longer required to be maintained by law.

(c-2) If a biometric identifier captured for a commercial purpose has been collected for security purposes by an employer, the purpose for collecting the identifier under Subsection (c)(3) is presumed to expire on termination of the employment relationship.

(d) A person who violates this section is subject to a civil penalty of not more than $25,000 for each violation. The attorney general may bring an action to recover the civil penalty.

CREDIT(S)

Added by Acts 2007, 80th Leg., ch. 885, § 2.01, eff. April 1, 2009. Amended by Acts 2009, 81st Leg., ch. 1163, § 1, eff. Sept. 1, 2009.

HISTORICAL AND STATUTORY NOTES

2009 Legislation

Acts 2009, 81st Leg., ch. 1163 rewrote subsec. (c); and added subsecs. (c-1) and c-2). Prior to amendment, subsec. (c) read:

"(c) A person who possesses a biometric identifier of an individual:

"(1) may not sell, lease, or otherwise disclose the biometric identifier to another person unless:

"(A) the individual consents to the disclosure;

"(B) the disclosure completes a financial transaction that the individual requested or authorized;

"(C) the disclosure is required or permitted by a federal statute or by a state statute other than Chapter 552, Government Code; or

"(D) the disclosure is made by or to a law enforcement agency for a law enforcement purpose; and

"(2) shall store, transmit, and protect from disclosure the biometric identifier using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits, and protects any other confidential information the person possesses."

Section 2 of Acts 2009, 81st Leg., ch. 1163 provides:

"(a) The changes in law made by this Act apply to a biometric identifier possessed by a person:

"(1) on or after the effective date of this Act; or

"(2) before the effective date of this Act, subject to Subsection (b) of this section.

"(b) A person who before the effective date of this Act possesses a biometric identifier that is required to be destroyed because of the changes in law made by this Act shall destroy the biometric identifier on or before October 1, 2009."

2009 Main Volume

Prior Laws:

Acts 2001, 77th Leg., ch. 634, § 1.

V.T.C.A., Bus. & C. Code § 35.50.

RESEARCH REFERENCES

Encyclopedias

TX Jur. 3d Consumer & Borrower Protection Laws § 203, Miscellaneous Regulatory Provisions.

V. T. C. A., Bus. & C. § 503.001, TX BUS & COM § 503.001

Current through the end of the 2011 Regular Session and First Called Session of the 82nd Legislature

END OF DOCUMENT

SUBMISSIONS FOR THE RECORD NOT PRINTED DUE TO VOLUMINOUS NATURE, PREVIOUSLY PRINTED BY AN AGENCY OF THE FEDERAL GOVERNMENT, OR OTHER CRITERIA DETERMINED BY THE COMMITTEE, LIST OF MATERIAL AND LINKS CAN BE FOUND BELOW:

EPIC Comments—January 31, 2012.:

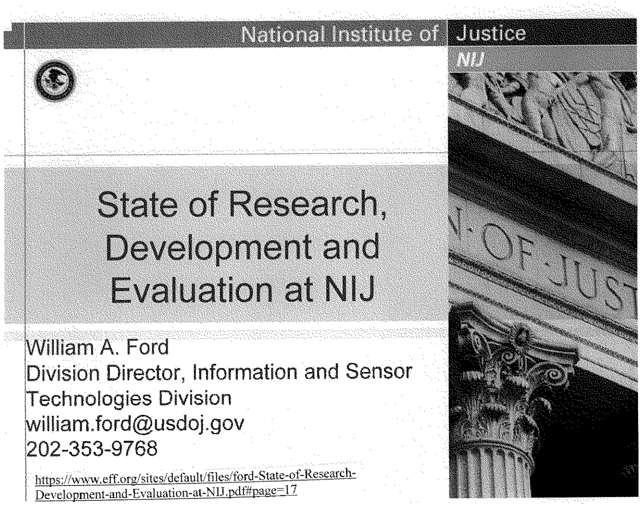
http://www.ftc.gov/os/comments/facialrecognitiontechnology/00083-0982624.pdf

National Institute of Justice (NIJ), William A. Ford, Director, State of Research, Development and Evaluation.:

https://www.eff.org/sites/default/files/ford-State-of-Research-Development-and-Evaluation-at-NIJ.pdf#page=17

Farahany, Nita A., Testimony Attachment—Pennsylvania Law Review:

http://www.pennumbra.com/issues/pdfs/160-5/Farahany.pdf



National Institute of Justice

NIJ

State of Research, Development and Evaluation at NIJ

William A. Ford
Division Director, Information and Sensor Technologies Division
william.ford@usdoj.gov
202-353-9768

https://www.eff.org/sites/default/files/ford-State-of-Research-Development-and-Evaluation-at-NIJ.pdf#page=17