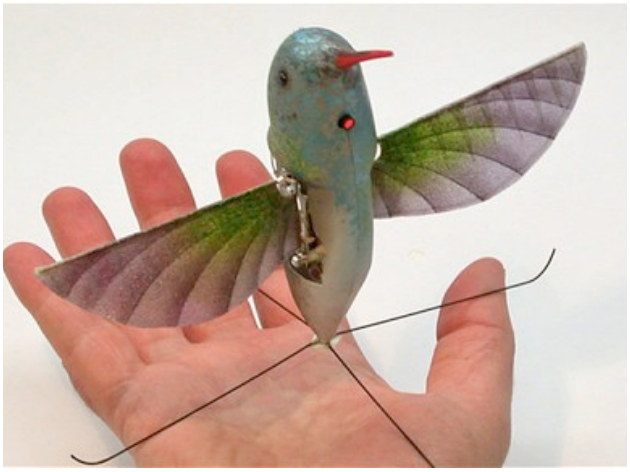
SURVEILLANCE IN THE FREE STATE:

Electronic Communications, Location Tracking, Automatic License Plate Readers, Drones and Facial Recognition



ACLU
AMERICAN CIVIL LIBERTIES UNION of MARYLAND

This report has been a project of the American Civil Liberties Union of Maryland. The report's primary author is ACLU of Maryland Public Policy Director Sara Love. ACLU of Maryland staff Toni Holness, Meredith Curtis and David Rocah all provided valuable feedback on the report.

A special thanks to Allen Gilbert, Executive Director of ACLU of Vermont, without whom there would be no report. The ACLU of Maryland also thanks Elonna Ekweani for her assistance with this report.

2/23/2014

EXECUTIVE SUMMARY: BECOMING A SURVEILLANCE SOCIETY

Maryland calls itself the Free State. But are we really? **We are being watched.** Today, Marylanders can barely go anywhere without creating a trail of digital information that pinpoints their whereabouts at nearly any time, day after day.

The erosion of Marylanders' privacy can be seen in the following specific instances. Each instance, alone, may not strike everyone as concerning. But understood together, the mass surveillance of Marylanders should strike everyone as alarming.

Electronic Communications Review: Outdated laws governing technology and privacy allow law enforcement to access your emails and Facebook messages and comments 6 months or older, stored cloud data, search queries, contacts and more.

Location Tracking Capabilities: Law enforcement can track you using data your cell phone generates with your cellular carrier. Where you go tells a tremendous amount about you: where you work, where you visit, where your doctor is, where (and whether) you pray.

Automated License Plate Readers (ALRPs): ALPRs photograph and read the license plates from every passing car and check the plates against "hot lists." Each license plate recorded is tagged with a date, time and location stamp, making an ever more detailed digital trail of where your car has gone. Almost all of the data is aggregated and retention time varies across the state.

Domestic Use of Drone Aircraft: Drones are automated or remotely controlled aircraft, which can carry surveillance equipment. Drones gained widespread military use in U.S. conflicts in Afghanistan and Iraq, but like other military surveillance technology, it is moving to domestic law enforcement use.

Facial Recognition Software: Using distinct parts of the human face, this technology allows for the creation of a "faceprint." This faceprint can be run against databases and video surveillance footage to determine a person's identity or track them through crowds.

CONSIDER A TYPICAL DAY

The technologies discussed in this report not only capture and store information, but also reveal to law enforcement a lot about us, all without any special use of the technologies, without justifying to a court why the information is needed, and without our knowledge that information about our lives has been compiled and stored by the state and shared with other agencies**.**

Consider this example: a woman leaves her home in Washington County, drives to her job in Annapolis, goes out for lunch where she does some personal emails, leaves for a doctor's appointment, makes a trip to the grocery store, and then drives back home. All of these things reveal information about her—her employer, her physician, her eating habits, her friends –and all can be tracked by law enforcement.

On her drive to work she may have passed any of the Maryland State Police, Washington County Sheriff, Hagerstown police, Frederick police, Montgomery County police, Takoma Park police, Prince George's County police, Anne Arundel County police or Annapolis police cars carrying an automatic license plate reader, or readers mounted in fixed locations, all of which record her location and store it in a database anywhere from 30 days to forever.

She carries a cell phone, which transmits data to her cell provider every few minutes, tracking where she is so she can make or receive calls. On request, records of that data are made available to police, whether or not police obtained a search warrant from a judge.

As she sends some personal emails over lunch, she notices she has some emails from friends that she got 7 months ago. She keeps meaning to respond, but hasn't done so yet. She posts some private photos on Facebook and stores some personal medical documents on cloud storage.

Law enforcement can get all of this data without a search warrant but simply a court order showing it was 'relevant' to an ongoing criminal investigation. – she doesn't even need to be the target of the investigation, perhaps she was at the same coffee shop and parks at the same garage as the person under investigation.

If the government were doing this surveillance by any other means, for example having a government agent follow you every time you walk out the door, we'd all viscerally understand the privacy invasion. The type of surveillance described in this report is the same thing. It is done by less obtrusive means, but no less invasive of our privacy. The mere fact of being constantly watched and tracked is chilling.

COMMUNICATIONS CONTENT PRIVACY

What Is Communications Content?

In essence, communications content relates to all those things we do online: emails, texts, twitter chats, Facebook messages and wall posts, photos posted on Flickr, Facebook or Instagram, YouTube videos, digital address books, dropbox accounts, comments in e-books, etc.

Ever since the National Security Agency (NSA) revelations began in June 2013, there have been serious questions about who has access to your electronic communications content. But it's not just the NSA that seeks access to our communications content: state and local law enforcement agencies seek access as well.

The federal Electronic Communications Privacy Act (ECPA) was enacted in 1986, and its Maryland counterpart was enacted in 1988. This was long before smart phones, cloud computing, Facebook, or the world wide web even were invented, much less widely used.

E-mail is a perfect example of the gap between ECPA and today's technology. In 1986, email was downloaded to a recipient's desktop computer (there were no laptops or smart mobile devices) when the recipient opened it. At that point, the email was deleted from the email provider's storage. If the email wasn't opened, it remained on the email provider's server. ECPA was written with this in mind: it requires a search warrant before the government can retrieve a message from an email provider's storage if the message is 180 days old or less and doesn't require a search warrant if the email is left on the server for more than 180 days. This is because in 1986, email left on the provider's server for more than 180 days was considered abandoned. Today, email is not downloaded onto our hardware, it is all stored on and accessed from remote servers belonging to the email provider. And many people have emails older than 180 days that they don't consider abandoned, and that they do consider private.

Today, under Maryland law, if law enforcement want to read your emails that are older than 6 months, or look at your contacts, or look at your drop box account, they simply need a court order saying the information is relevant to an ongoing criminal investigation.[1] This is a much lower standard than a search warrant, which requires probable cause to believe that the individual being investigated committed a crime, and that the information sought is evidence of that crime.

How Does Communication Content Access Affect Civil Liberties?

We increasingly lead our lives online. We write emails rather than letters; we keep contacts on our phones rather than in address books; we keep pictures in our drop box files rather than in a hardbound scrapbook. Our digital lives show everything about us.

If law enforcement wants access to that private information, they should have to get a search warrant – just as they would have to if they wanted to come into your house and look at your address book or your scrapbook.

We shouldn't have to choose between new technology and privacy. Our founders recognized the critical importance of privacy when they wrote the Fourth Amendment protection against

unlawful searches and seizures by the government. Our right of privacy for our "persons, houses, papers, and effects" remains as true today as it did over 200 years ago whether those "papers and effects" are stored in our desk drawers or in the cloud. The line should be clear: any communications content not intended to be viewable by the public, whether created offline or online, should be off limits for the government except in narrowly tailored investigations with appropriate judicial oversight.

Have Other States Regulated Access to Communications Content?

Yes. To date Texas and Maine have enacted laws regulating law enforcement's access to communications content.

LOCATION TRACKING

What Is Location Tracking?

Location tracking can refer to real-time surveillance where a person's location is determined by "triangulating" the cell phone towers with which that person's phone is interacting. Location tracking can also refer to reconstructing a person's past movements with "historical" cell tower triangulation data stored by cell phone companies. Service providers have different policies on how long they retain the data. But generally, cell records may be kept anywhere from four months to two years.[2]

In 2011, cell phone companies nationally responded to about 1.3 *million* requests from the FBI and state and local law enforcement for tracking data.[3] These requests often included multiple subscribers. And not all service providers were willing to disclose the number of requests they had received. This means that the actual number of data requests is likely much higher than 1.3 million annually.[4] The legality of accessing this data without warrants is being debated in courts across the country.

Is Location Tracking Used In Maryland?

Yes. Law enforcement tracks Marylanders—in real time and using historical data.[5] Legislators have tried to pass a law requiring Maryland's law enforcement to obtain a warrant prior to tracking someone using their cell phone but have been unsuccessful to date.

How Does Cell Phone Tracking Affect Civil Liberties?

Civil liberties are not violated when police have probable cause in an investigation and obtain a warrant before getting cell phone data from service providers. Judicial oversight guards against police invasion of someone's privacy rights.

However, civil liberties *are* violated when police gather, without a finding of probable cause by a judge, large amounts of data about individuals to create a comprehensive picture of a person's life and where he or she has been. As DC Circuit Judge Ginsburg wrote, one's location might reveal

> "whether he is a weekly church goer, a heavy drinker, a regular at the gym, an unfaithful husband, an outpatient receiving medical treatment, an associate of particular individuals or political groups – and not just one such fact about a person, but all such facts."[6]

Police and prosecutors claim the authority to track cell phone locations without court oversight by citing a 1979 U.S. Supreme Court decision, *Smith v. Maryland*, 422 U.S. 735 (1979). The so-called "third party doctrine" laid out by the court says information given by an individual to a "third party" to perform certain functions (such as to make a phone call) does not enjoy the usual privacy protections given personal property or information.

As technology has developed and data gathering and storage have become more sophisticated, the threat to privacy by the "third party doctrine" has become evident. No one purchases a cell phone expecting that it will be used as a personal tracking device enabling warrantless government surveillance of our every movement.

Not only is it unrealistic to ask Americans to choose between meaningful personal privacy and the modern necessities like a cell phone, but it is also largely impossible to think of doing anything in our daily lives without information being given to a third party. The result has been ongoing litigation between citizens wishing to protect their privacy and law enforcement wishing to tap the mountains of data third parties collect about each of us.

In 2012, the Unites States Supreme Court decided *U.S. v. Jones*, 132 S.Ct. 949 (2012). In that case the Court held that the government violated the Fourth Amendment when it used a GPS device to track a suspect's location for 28 days without a valid warrant. The majority ruling rests on relatively narrow grounds (the actual physical trespass of placing the GPS on the defendant's car), but a majority of the justices recognized that the long term monitoring of each and every single movement made by a person, no matter what technology is used, impinges on an individual's reasonable expectation of privacy. While the details of what this means are still being litigated, *Jones* is prompting serious discussions across the country as to the proper parameters of when law enforcement must get a search warrant for location tracking information.

Law Enforcement Should Get A Warrant – And Many Do

A number of enforcement agencies across the country, in states as diverse as California, Colorado, Hawaii, Kansas, Kentucky, Nevada, New Jersey, North Carolina, and Wisconsin, obtain probable cause search warrants in order to access cell phone location information. These law enforcement agencies are able to protect public safety and privacy by meeting the warrant and probable cause requirement, and so can Maryland.

AUTOMATED LICENSE PLATE READERS

What Are ALPRs?

Automated License Plate Readers (ALPRs) combine high-speed cameras that capture photographs of every passing license plate with software that analyzes those photographs to identify the plate number. The device can be affixed to police cruisers or mounted on stationary objects such as overpasses or traffic lights. License plate reader systems typically check each plate number against "hot lists" of plates that have been uploaded to the system and provide an instant alert to a law enforcement agent when a match or "hit" appears.[7]

A single ALPR can cost as low as $8,000.[8] States and municipalities typically receive grants from the Department of Homeland Security to cover the purchase price.[9]

Are ALPRs Being Used In Maryland?

Yes. Currently, about 68 Maryland police agencies have ALPRs, with nearly 411 systems in use statewide. Of those, 307 are mounted on police cars and 104 are fixed cameras.[10] These numbers have increased since 2012, when there were at least 371 ALPRs, with only 72 fixed cameras.[11]

Data captured by the cameras around the state is transferred to a central database maintained at the Maryland Fusion Center (known as the Maryland Coordination and Analysis Center, or MCAC). Approximately 80% of all Maryland agencies using ALPRs transfer their data to MCAC, which currently retains the data for one year.

According to statistics compiled by MCAC, from January - May, 2012, Maryland's license plate reader system had over 29 million reads (license plate scans). Only 0.2 percent of those license plates were associated with any crime, wrongdoing, minor registration problem, or even suspicion of a problem. Of those 0.2 percent, 97% were for a suspended or revoked registration or a violation of Maryland's Vehicle Emissions Inspection Program. **For every one million plate reads in Maryland, only 47 were potentially associated with more serious crimes**—a stolen vehicle or license plate, a wanted person, a violent gang or terrorist organization, a sex offender or Maryland's warrant flagging program.[12]

There is no problem with the use of license plate readers to identify individuals suspected of violating the law. But the above data provide a striking illustration of the wide dragnet that license plate readers often cast. Because they snap pictures of every passing vehicle, they generate millions of data points on the movements of individuals whom no one suspects of violating any law.

How Do ALPRs Affect Civil Liberties?

License plate readers would pose few civil liberties risks if they only checked plates against hot lists and these hot lists were implemented soundly. But these systems are configured to store the photograph, the license plate number and the date, time and location where all vehicles are

seen—not just the data of vehicles that generate hits. All of this information is being placed into databases and this data is then pooled into regional sharing systems or MCAC. As a result, enormous databases of motorists' location are being created.

More and more cameras, longer retention periods, and widespread sharing allow law enforcement agencies to assemble the individual puzzle pieces of where we have been over time. Databases of license plate reader information create opportunities for institutional abuse, such as using them to identify protest attendees merely because these individuals have exercised their First Amendment-protected right to free speech. And examples already exist: in Virginia the Virginia State Police recorded the license plates of vehicles attending President Obama's 2009 inauguration, as well as rallies for Obama and vice presidential candidate Sarah Palin.[13] If not properly secured, license plate reader databases open the door to abusive tracking, enabling anyone with access to pry into the lives of his boss, his ex-wife or his romantic, political or workplace rivals.

Have Other States Regulated ALPR Use?

Five states to date regulate ALPR use: Arkansas, New Hampshire, Maine, Utah and Vermont.

DRONES

What Are Drones?

"Drones," "unmanned aerial vehicles," "unmanned systems," and "robotic aircraft" all describe a class of aircraft that range in size and capability and are operated through remote piloting. In war zones, drones equipped with weapons systems are referred to as "silent predators."[14]

On June 19, 2013, Federal Bureau of Investigation Director Robert Mueller testified before Congress and admitted that the FBI uses drones for surveillance on U.S. soil. He added that this was in a "very, very minimal way and very seldom," but the fact remains that it has been and is being done. According to the FAA, as of 2012 there were around 300 active operating licenses, and that 700-750 had been issued between 2006-2012.

Several law enforcement agencies have acquired drones, including Houston, Texas; Miami-Dade County Police Department, Florida; Mesa County Sheriff's Office, Colorado; Arlington, Texas; North Little Rock, Arkansas; Herrington, Kansas; Gadsden, Alabama; Polk County, Florida. In March 2013, the City of Seattle, Washington cancelled the use of two federally funded drones after residents raised concerns over privacy rights.

In addition to large airplane-like drones, manufacturers have developed model-plane-sized drones and even smaller devices with high-quality sensors and tremendous surveillance capacity.[15] The Raven B, for example, manufactured by AeroVironment, weighs only 4.2 pounds. The Raven has a line-of-sight range up to six miles.[16] It is equipped with software that automatically detects moving objects, captures that movement through electro-optical and infrared motion video, and stamps the images with geo-location data. The Raven is battery-powered and can stay airborne for up to 90 minutes at speeds up to 50 mph.[17] It can operate day or night.

Another AeroVironment product, the Wasp, weighs less than one pound. The Wasp travels about 40 mph and operates at altitudes between 50 and 1,000 feet. Like the Raven, it is equipped with a high-resolution camera that allows surveillance day or night.[18]

How Do Drones Affect Civil Liberties?

Increased surveillance. The high cost of aircraft has always imposed a limit on the government's aerial surveillance capacity. The low cost and flexibility of drones erode that limit.

Drone use is largely covert. It is hard for people to find out who may be operating drones in their area, let alone why they have been deployed. And, unlike a search of your home, which requires a warrant (and notice to you of the search), drones have the capacity to fly at altitudes

where they cannot be seen or heard. The surveillance occurs without a warrant, and information unrelated to any specific investigation may be collected.

More invasive technology. Increasing technology—such as high-powered night vision cameras, see-through imaging, the ability to identify if an individual has a gun or to track their cell phone – exacerbate privacy issues. In conjunction with other new technologies, including facial recognition software, drones give law enforcement the capacity to monitor lawful activities, identify specific individuals, crosscheck with other databases, and store collected information for undetermined lengths of time.[19]

Free speech. Surveillance curtails individual liberty and freedom by placing Americans under constant scrutiny. Innocent people may fear punishment if they exercise their First Amendment rights on issues where they do not agree with the government.

Are Drones Used In Maryland?

Most likely, yes. The Electronic Frontier Foundation received documents showing that several entities, including the Queen Anne's County Sheriff's Office, received Certificates of Authority from the FAA to operate drones.[20]

In addition, news reports revealed that in October of 2014, the Pentagon plans to deploy two large blimp-like aircraft over Aberdeen Proving Ground in Harford County. From 10,000 feet in the air, these blimps will be able to scan from Raleigh, N.C., to Boston, M.A., to Lake Erie.[21] While the stated intent behind these blimps is to scan for missiles, these blimps can be fitted with surveillance systems powerful enough to track people and vehicles from miles away.[22] The Army did not rule out the possibility of mounting surveillance cameras, or of sharing the information with federal, state and local law enforcement.[23]

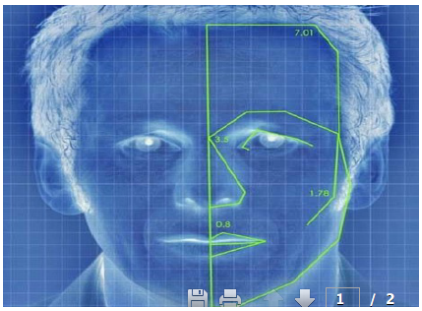
Have Other States Regulated Drone Use?

To date several states place responsible limits on the use of domestic drones: Florida, Idaho, Illinois, Montana, Oregon, Tennessee and Texas. North Carolina and Virginia have put moratoriums on the use of drones while they study them and determine the right policies.

FACIAL RECOGNITION SOFTWARE

What Is Facial Recognition Software?

Facial recognition software is technology that uses mathematics to measure facial features that aren't easily manipulated even by cosmetic surgery.[24] Facial recognition software is one of a number of technologies used to collect what is known as "biometric" information; other biometrics include fingerprints and iris scans.[25]



The measurements taken by facial recognition software generally include the distance between the eyes, the width of the subject's nose, and the depth of his or her eye sockets.[26] The photos and measurements are stored in a database and can be compared to other photos to verify a person's identity. This digital representation is known as a "faceprint" and is believed to be as unique in confirming identity as a fingerprint.[27] The databases where facial recognition data is stored can be used to compare millions of faceprints per minute.[28]

Facial recognition software is already in wide use by the government and private entities. Thirty seven states use facial-recognition technology with their driver's license registries.[29] The majority of those states allow federal, state and local law enforcement agencies to search or request searches of these databases to learn identities of people who the agencies consider "relevant" to investigations.[30]

In addition, facial recognition can be—and has been—used for general surveillance. For example, facial recognition was used at the 2001 Super Bowl in Tampa, Florida. Pictures were taken of every attendee as they entered the stadium and compared against a database of an undisclosed kind. The software flagged 19 individuals, though the police admitted that some of those were false alarms, and no one was anything more than a petty criminal such as a ticket scalper.[31]

Private companies use the software, too. When a website such as Facebook or Google Plus suggests that you tag a picture with the name of a friend or family member, it uses facial recognition software to compare other already-tagged faces with your newly added photos.[32]

Is Facial Recognition Software Being Used In Maryland?

Yes. In March 2011, Maryland initiated a system with more than 2.1 million photos of known offenders.[33] In December of that same year, Maryland executed a memorandum of understanding with the FBI to launch a Facial Recognition Pilot Program and gain access to the national repository of mug shots.[34] Maryland further expanded its use of facial recognition

software in the Spring of 2013 when the Department of Public Safety and Correctional Services (DPSCS) added more than 5.8 million Motor Vehicle Administration (MVA) photos to its database, thus, allowing facial recognition software to search driver's license photos and other state-issued photo identifications.[35]

Presently, the Governor's Office of Crime Control and Prevention works with DPSCS to enable law enforcement to utilize facial recognition software through a program called Dashboard. According to DPSCS, Dashboard enables law enforcement to compare information from numerous state and criminal justice databases in a matter of seconds.[36]

How Does Facial Recognition Software Affect Civil Liberties?

Facial recognition software technology is not inherently invasive of civil liberties. But combined with surveillance technologies—particularly drones—to facilitate remote and covert identification it causes significant privacy concerns. One concern is the threat of increased use and increased surveillance. We have already seen facial recognition grow from matching mug shots to using drivers' license databases to scanning crowds. The ready availability of data and the prospect of adding ever more data is seductive and further threatens our privacy.

Another concern is the threat of abuse. The use of facial recognition depends on widespread video monitoring, an intrusive form of surveillance that can record in graphic detail personal and private behavior. But video monitoring systems are operated by humans, who bring their existing prejudices and biases. In Great Britain, for example, which has used closed circuit cameras in public places, camera operators have been found to focus disproportionately on people of color, and the mostly male operators frequently focus voyeuristically on women.[37]

Then there is the secrecy within which most of these systems operate. Most people do not know the systems that the government has and uses for surveillance. Thus the surveillance is conducted without proper public discussion and, through it, proper oversight.[38]

The prospect of a drone flying overhead, scanning everyone in the crowd and using facial recognition to find people is no longer the subject of sci-fi movies, but a reality. With such technology the government has the capability of tracking and identifying individuals wherever they are, without judicial oversight or suspicion that these people have done anything wrong. Through the use of these tools, the government is conducting a constant investigation, without any reasonable suspicion of wrongdoing. Everyone is, by default, a suspect.

MARYLAND FUSION CENTER

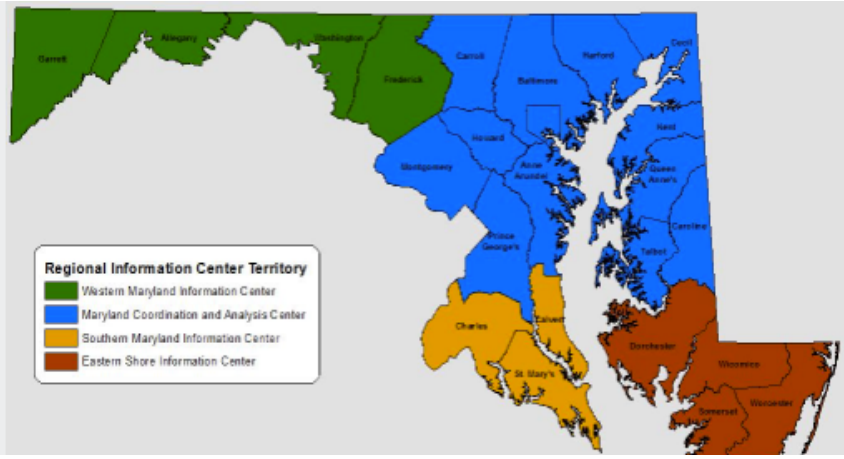
What Is A Fusion Center?

Fusion centers are information-gathering hubs, receiving data from federal, state, and local governments and from private businesses, and analyzing and sharing information. Their original mission was to fight terrorism, but that mission has crept into other areas—from emergency response to public health issues to general law enforcement.[39] **Between 2001 and 2007, individual states received around $380 million in federal funding to establish these centers.**[40] There are more than 70 centers around the country, with at least one in each state.[41]

The Maryland Fusion Center—the "Maryland Coordination and Analysis Center" (MCAC)—is a "joint federal, state, and local initiative" with 30 partners, including the Annapolis Police Department, the Baltimore Fire Department, the University of Maryland, the Bureau of Alcohol, Tobacco, Firearms and Explosives, and Immigration and Customs Enforcement.[42] According to the MCAC website, "fusion centers add significant value to their customers by providing a state and local context to help enhance the national threat picture. Fusion centers provide the federal government with critical state and local information and subject matter expertise that it did not receive in the past – enabling the effective communication of locally generated threat-related information to the federal government. Integrating and connecting these state and local resources creates a national capacity to gather, process, analyze, and share information in support of efforts to protect the country."[43]

Regional Information Centers

In addition to the statewide fusion center, Maryland has four regional information centers (RICs). The mission of the RICs is to "collect, evaluate, collate, analyze, and disseminate information on individuals and groups suspected of being involved in gang and other illegal activity identified as a priority to the RICs (Advisory Board). The RICs will strive to be the repository for the collection and dissemination of information between local, state and federal law enforcement agencies in an effort to be proactive in initiating criminal investigations."[44]



How Do Fusion Centers Affect Civil Liberties?

A two-year bipartisan investigation by the U.S. Senate Homeland Security Subcommittee found that DHS's "efforts to engage state and local intelligence 'fusion centers' has not yielded significant useful information to support federal counterterrorism intelligence efforts." Further, the report found that "[i]nstead of strengthening our counterterrorism efforts, [state fusion centers] have too often wasted money and stepped on Americans' civil liberties."[45]

The scope of work and the limits to the uses and storage of data collected at fusion centers are not entirely clear. Some fusion centers are engaged primarily in information sharing, while others actively conduct investigations.[46] The risks to civil liberties are twofold. First, for centers that engage in investigations, monitoring could easily stray into surveillance of individuals engaged in lawful activities.[47]

Second, even if not actively engaged in investigations, a fusion center is, by its nature, dangerously close to invading the privacy of everyday citizens.[48] The centers collect so much information about people from various sources that a picture of an individual's daily activities can readily be developed, regardless of whether they are suspected of any crime. Marylanders do not expect to submit to constant warrantless surveillance just by walking out their front door – or by using digital tools such as cell phones and the Web to go about their business. Fusion centers have the potential to become the nerve center of the "total surveillance society."

CONCLUSION

I haven't done anything wrong, so why should I care?

Each type of surveillance—electronic communications review, location tracking, drones, ALPR—may not seem like an invasion of privacy of and in itself. But combined, the public begins to understand the massive amount of data the government is obtaining about us every day.

Many people think that because they haven't done anything wrong, this data gathering about our private lives is not a problem. But it is a problem. At its core, this massive governmental data gathering violates a basic tenet of our society: that the government doesn't gather data on us just in case we do something wrong. This principle is as old and as fundamental to our society as the Fourth Amendment.

More personally, there are the examples of wrongful identity. Many people have been put on a watch list and targeted when, in fact, they haven't done anything wrong.[49]

Perhaps even scarier, the troves of data can imply connections where there are none. Brandon Mayfield , a former U.S. Army platoon leader and attorney specializing in child custody, divorce and immigration law, is a prime example. Al-Qaeda-inspired terrorists coordinated a bombing in Madrid in 2004. When fingerprints recovered during the investigation were shared with the FBI, it came up with 20 possible matches, including Mayfield's (whose prints were in the system due to his military service). Despite finding that the prints were not an identical match, and despite repeated warnings by the Spanish police that the prints didn't match, the FBI conducted massive surveillance of Mayfield and his family and concocted a theory of his guilt based upon details of his life that fit their theory. A report by the Office of the Inspector General found that the FBI's requests for material witness and criminal search warrants "contained several inaccuracies that reflected a regrettable lack of attention to detail."[50] The FBI so believed it had the right man that it aggregated coincidences to make a case, refused to see contrary evidence, and even provided misleading sworn statements to a judge.[51]

Finally, once people know they are under constant surveillance, they begin to change their behavior – even if they weren't doing anything wrong. The possibility of curtailing people's exercise of their fundamental freedoms becomes more than a possibility. As one example, a report on the New York Police Department's covert surveillance of the Muslim community documents that the surveillance had an impact on: free speech, anything from people's engagement in public protests to their coffeehouse banter; on students choices of classes; and on the free exercise of religion, as "congregants became suspicious of one another, imams hesitated when advising their congregants, and individuals refrain[ed] from appearing overtly 'Muslim' to avoid triggering surveillance."[52]

What can we do about this?

Bi-partisan legislators in both the Maryland Senate and House are working to pass sensible legislation that balances enabling law enforcement to use technology to solve crimes and Marylanders' privacy.

Support:
Electronic Communications Privacy – SB 924/HB 912
Ensuring law enforcement obtains a search warrant prior to reading our emails.

Location Tracking – SB 698/HB 1161
Ensuring law enforcement obtains a search warrant prior to tracking people via their cell phones.

Automatic License Plate Readers – SB 699/HB 289
Codifying parameters around how long information from ALPRs is kept and who can access that information.

Drones – SB 926/HB 847
Ensuring law enforcement obtains a search warrant prior to using a drone for surveillance.

END NOTES

[1] Maryland Courts and Judicial Proceedings, §§10-4A-04 *et seq*.
[2] ACLU, *Cell Phone Location Tracking Request Response – Cell Phone Company Data Retention Chart*, *available at* http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.
[3] Megha Rajagopalan, *How Many Millions of Cellphones Are Police Watching?*, PROPUBLICA (July 11, 2012, 3:05pm), http://www.propublica.org/article/how-many-millions-of-cellphone-are-police-watching.
[4] *Id.*
[5] http://www.fredericknewspost.com/news/crime_and_justice/courts/cellphone-records-at-issue-in-murder-trial/article_61bffe31-550f-5a2a-973c-6991b70c77b9.html; http://www.wusa9.com/news/article/285293/158/Cellphone-data-spying-Its-not-just-the-NSA; http://silverspring.wusa9.com/m/node/442311.
[6] *U.S. v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).
[7] ACLU, *You Are Being Tracked: How License plate Readers Are Being Used To Record Americans' Movements*, https://www.aclu.org/alpr
[8] http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/. A simple Google search turned up readers for as little as $289.
[9] http://www.baltimoresun.com/news/maryland/carroll/westminster/ph-ce-license-plate-readers-1006-20131001,0,3944085.story; *see, e.g.*, Responses to ACLU of Maryland MPIA requests on ALPRs, housed at the ACLU of Maryland; Ken Picard, *Maryland DMV to Use Facial Recognition Software On All New Driver's License Photos and IDs*, SEVEN DAYS (July 16, 2012).
[10] Farrell, *Maryland license plate recognition networks prompt state, federal privacy concerns*, GAZETTE.NET, http://www.gazette.net/article/20140214/NEWS/140219560/-1/maryland-license-plate-recognition-networks-prompt-state-federal&template=gazette (2/14/2104).
[11] *ACLU says license plate readers violate drivers' privacy* (July 17, 2013), http://www.baltimoresun.com/news/maryland/crime/blog/bs-md-license-plate-readers-20130717,0,4598979.story.
[12] *You Are Being Tracked, supra* note 7.
[13] *Virginia State Police Used License Plate Readers At Political Rallies, Built Huge Database* (October 8, 2013), https://www.aclu.org/blog/technology-and-liberty-national-security/virginia-state-police-used-license-plate-readers.
[14] *Drones: Who is Watching You?*, ABC NEWS, FEB. 15, 2012, *available at* http://abcnews.go.com/Nightline/video/drones-watching-15661073.
[15] *Fact and Fiction: Plenty to Worry About Drones*, VALLEY NEWS, June 24, 2012.
[16] UAS: RAVEN, AEROVIRONMENT, http://www.avinc.com/uas/small_uas/raven/ .
[17] RAVEN, AEROVIRONMENT, http://www.avinc.com/downloads/Raven_Gimbal.pdf .
[18] WASP, AEROVIRONMENT, http://www.avinc.com/downloads/USAirForceFactSheet.pdf .
[19] Larry Abramson, *Drones: From War Weapon to Homemade Toy*, VPR NEWS (Aug. 2, 2012), http://www.vpr.net/npr/157441681/.
[20] EFF Map of Domestic Drone Flights, https://www.google.com/fusiontables/embedviz?viz=MAP&q=select+col2+from+1WuTyH62PmUF97oxo6IreT1BL_aw9HJN5pocwmwg&h=false&lat=44.08758502824518&lng=-85.5615234375&z=4&t=1&l=col2&y=1&tmplt=2.
[21] *Blimplike surveillance craft set to deploy over Maryland heighten privacy concerns* (Jan. 22, 2014), http://www.washingtonpost.com/business/technology/blimplike-surveillance-crafts-set-to-deploy-over-maryland-heighten-privacy-concerns/2014/01/22/71a48796-7ca1-11e3-95c6-0a7aa80874bc_story.html
[22] *Is a blimp watching you? New surveillance craft raises privacy questions*, http://www.foxnews.com/us/2014/01/24/blimplike-surveillance-craft-set-to-fly-over-maryland-raises-privacy-questions/.
[23] *Id*.
[24] Picard, *supra* note. 9.
[25] Kanya A. Bennett, Comment, *Can Facial Recognition Technology Be Used to Fight the New War Against Terrorism?: Examining the Constitutionality of Facial Recognition Surveillance Systems*, 3 N.C. J.L. & TECH. 151, 155 (2001–02).
[26] *Id.*
[27] James Temple, *Facial Recognition Software's Privacy Concerns*, SFGATE, June 19, 2012.

[28] Kanya A. Bennett, Comment, *Can Facial Recognition Technology Be Used to Fight the New War Against Terrorism?: Examining the Constitutionality of Facial Recognition Surveillance Systems*, 3 N.C. J.L. & TECH. 151, 155 (2001–02).
[29] *State photo-ID databases become troves for police* THE WASHINGTON POST, June 16, 2013, http://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_print.html.
[30] *Id.*
[31] ACLU, *Q&A on Facial Recognition*, (Sept. 2, 2003), https://www.aclu.org/technology-and-liberty/qa-face-recognition.
[32] *Daily Report: Germans Reopen Facebook Privacy Inquiry*, NYTIMES.COM BITS BLOG (Aug. 15 2012, 8:46 a.m.), http://bits.blogs.nytimes.com/2012/08/15/daily-report-germans-reopen-facebook-privacy-inquiry/; Sharon Guadin, *Google unveils 'Find My Face' tool for Google+, Social Network Gets Facial Recognition Tool to Help Users Tag Their Photos*, COMPUTERWORLD.COM (Dec. 9, 2011 12:54 p.m.), http://www.computerworld.com/s/article/9222550/Google_unveils_Find_My_Face_tool_for_Google_.
[33] *Facial Recognition Fact Sheet*, GOVERNOR'S OFFICE OF CRIME CONTROL AND PREVENTION, https://www.goccp.maryland.gov/msac/documents/FactSheets/facial-recognition.pdf (last visited 2/12/2014).
[34] *Id.; What Facial Recognition Technology Means for Privacy and Civil Liberties*: Before Subcomm. on Privacy, Technology, and the Law, 112th Cong. 2 (2000) (Statement of Jerome M. Pender, Deputy Assistant Director of Criminal Justice Information Services, Federal Bureau of Investigation) available at http://www.fbi.gov/news/testimony/what-facial-recognition-technology-means-for-privacy-and-civil-liberties.
[35] GOCCP Fact Sheet, *supra* note 33.
[36] *Catching a Bad Guy with Facial Recognition Technology*, DEPARTMENT OF PUBLIC SAFETY AND CORRECTIONAL SERVICES, http://www.dpscs.maryland.gov/publicinfo/features/face_recognition.shtml (last visited 2/12/2014).
[37] ACLU, *supra* note 31.
[38] ACLU, *Ready, Fire, Aim: Ohio officials implement statewide face recognition program without a whiff of public debate* (Sept. 3, 2013), https://www.aclu.org/blog/technology-and-liberty-national-security/ready-fire-aim-ohio-officials-implement-statewide-face.
[39] Department of Homeland Security, *State and Major Urban Area Fusion Centers*, available at http://www.dhs.gov/state-and-major-urban-area-fusion-centers.
[40] Mary Beth Sheridan, *States Setting Up Own Anti-terror Centers*, BOSTON GLOBE (Jan. 1, 2007), http://www.boston.com/news/nation/washington/articles/2007/01/01/states_setting_up_own_antiterror_centers/?page=1.
[41] Matthew Waxman, *Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11*, 3J. NAT'L SEC. L. & POL'Y 377, 390 (2009).
[42] http://www.mcac.maryland.gov/about_mcac/partners/.
[43] http://www.mcac.maryland.gov/about_mcac/Fusion%20Centers/.
[44] http://www.mcac.maryland.gov/about_mcac/RICs/index.html.
[45] Permanent Subcommittee on Investigations, *Investigative Report Criticizes Counterterrorism Reporting, Waste At State & Local Intelligence Fusion Centers,* http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers
[46] Sheridan, *supra* note 40.
[47] *Id.*
[48] Cynthia Laberge, *To What Extent Should National Security Interests Override Privacy in a Post 9/11 World?*, 3 VICTORIA U. WELLINGTON WORKING PAPER SER. 1, 6–7 (2010) (Explaining that information privacy refers to collecting, and controlling personal information about oneself).
[49] *See, e.g.* https://www.aclu.org/blog/national-security/no-fly-list-where-fbi-goes-fishing-informants
[50] *The terrifying surveillance case of Brandon Mayfield* (February 14, 2014), http://america.aljazeera.com/opinions/2014/2/the-terrifying-surveillancecaseofbrandonmayfield.html.
[51] *Id.*
[52] *CLEAR Project Issues Report on Impact of NYPD Surveillance on American Muslims*, http://www1.cuny.edu/mu/law/2013/03/11/clear-project-issues-report-on-impact-of-nypd-surveillance-on-american-muslims/