ACLU

AMERICAN CIVIL LIBERTIES UNION of VERMONT

SURVEILLANCE ON THE NORTHERN BORDER

Executive Summary: Becoming A Surveillance Society

Vermont used to be a state where both the notion and the reality of privacy were true. Over the last 12 years, Vermonters' reality of privacy has eroded. We are being watched. Today, Vermonters can barely go anywhere without creating a trail of digital information that pinpoints a person's whereabouts at nearly any time, day after day.

One critical factor that sets Vermont apart is the international boundary it shares with Canada. The U.S. Border Patrol claims the authority to stop and search travelers without any reasonable suspicion of wrongdoing within 100 miles of an international border, making Vermont a perverse Ground Zero in the accelerating surveillance society.

The erosion of Vermonters' privacy is evident:

- **U.S. Border Patrol stops in Hartford, Vermont –** The U.S. Border Patrol now runs traffic stops along I-91 in Hartford, a location nearly 100 miles from the Canadian border. These stops are only a prelude to routinized highway surveillance. The Department of Homeland Security (DHS) has developed plans to erect permanent checkpoints along every major north-south Interstate highway in New England and New York.

- **Automated License Plate Readers (ALPRs) –** More than a decade after the 9-11 attacks, numerous federal grants to local police departments from DHS continue to pour into the state. ALPRs have been purchased by nearly three-dozen Vermont departments. The readers capture license plates from every passing car and check the plates against "hot lists." All Vermont data is retained for at least 18 months.

- **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 photo databases and video surveillance footage to determine a person's identity or track them through crowds.

- **Domestic Use of Drone Aircraft –** The rise of drones began in U.S. conflicts in Afghanistan and Iraq. Drones are automated or remotely controlled aircraft, which can carry surveillance equipment. As of 2011, Customs and Border Protection has eight drones in operation along the Mexican and Canadian borders.

- **Fusion Centers –** Originally created to combat terrorism, fusion centers are information-gathering hubs, receiving data from federal, state, and local governments and from private businesses, and analyzing and sharing information. Fusion centers either passively gather information or actively assist law enforcement in investigations.

The arrival of some of these surveillance tools is partly because of Vermont's position along an international border.

Vermonters have become caught in webs of surveillance with the capacity to track nearly everyone's movements. Tacit acknowledgement from state legislators, perfunctory approval by local select boards, or unquestioning acceptance by citizens has allowed numerous projects to get underway with little public discussion, political debate, or oversight.

Vermont, with little public discussion or acknowledgement, is moving towards a surveillance society. This report outlines the tools and practices that have enabled that to happen.

Consider A Typical Day

A woman drives from her home in St. Albans to her job in South Burlington, takes a walk to pick up lunch at noon, leaves for a doctor's appointment, makes a trip to the grocery store, and then drives to pick up the kids after school. All of these movements reveal information about her life: her employer, her physician, her eating habits, and where her children are educated.

The technologies discussed in this report not only capture and store information, but also reveal to law enforcement everything about her – from her name to where she gets her coffee in the morning – all without any special use of the technologies, without justifying to a court why the information is needed, and without the woman's knowledge that information about her life has been compiled and stored by the state, and shared with state and federal agencies through facilities like the Vermont Fusion Center.

More than 90 percent of Vermonters live within 100 miles of an international boundary.

On her drive to work she may have passed any of the Vermont State Police, Franklin County, St. Albans, Milton, Colchester, Winooski, South Burlington, or Burlington police cars now carrying an automated license plate reader (ALPR), all of which can record her location and store it in a database for at least the next 18 months.

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 warrant from a judge.

Perhaps a Border Patrol drone flies overhead, recording her drive, which it monitors because she, like more than 90 percent of Vermonters, lives within 100 miles of an international boundary. Or, if the Federal Aviation Administration (FAA) has approved more expansive domestic drone use, the state police or even local departments may have obtained drones through grants from the DHS and can follow her movements.

With data from the drone's high-resolution camera and facial recognition software, and access to the DMV database, **the state knows who she is, what cars she has registered with the state, what her driving record is, and potentially much more**, because the Vermont Fusion Center collects and aggregates data from many sources.

Improbable?

It is easy to think, tucked away in the Green Mountains, that comprehensive surveillance systems are not being used to monitor and intrude into the daily lives of Vermonters, but the technology systems in use and in the process of being implemented, have the potential of creating former national security advisor John Poindexter's "total surveillance society." What we do, where we go, and who we interact with reveals a lot about us. The more data that is collected and shared, **the closer we are to living in a world where surveillance is total and few things are private.**

How did this happen? That will be the question when we regret not having put laws and policies in place to regulate the use of these powerful tools.

Contents

American Civil Liberties Union of Vermont
137 Elm Street, Montpelier Vt. 05602
802-223-6304
www.acluvt.org
info@acluvt.org

Introduction

Late in 1999, the U.S. Border Patrol in Vermont arrested a Canadian woman and an Algerian man attempting to enter the country, both of whom were connected to a terrorism-related arrest in Brooklyn, New York.[1] In other words, **the pre-September 11th Border Patrol service did its job in preventing the entrance of individuals known to be connected to terrorists.** Two years later, however, public confidence in U.S. national security was shaken by the terrorist attacks of September 11th.

In response to the attacks, Congress passed the USA PATRIOT Act in 2001 and the Homeland Security Act in 2002. The Homeland Security Act combined 22 agencies into a new DHS.[2] **DHS's Customs and Border Protection (CBP) service now employs five times more agents on the northern border than it did in 2001, a total of 2,200,[3] or about 10 percent of all agents nationwide.**[4] In spite of this increase, DHS reported in 2010 that only 32 miles of the nearly 4,000-mile northern border had reached an "acceptable" level of security, and additional surveillance and agents should be expected.[5]

Vermont has no specific foreign or domestic terrorism threats, has had no terrorism-related convictions since Sept. 11, 2001, and has no urban areas that the federal government views as "high-threat, high density."[6] Nevertheless, since 9/11, **the state and its municipalities have received nearly $100 million in grants from DHS to deploy new surveillance technologies.** In addition to aiding in law enforcement, emergency response, and securing the Vermont-Canada border, such high-tech methods of surveillance have tremendous capacity to infringe on the civil liberties of Vermonters, particularly the right to privacy, which Vermonters value highly.

New technologies include automated license plate readers, facial recognition software, and drones. In addition, Vermont has established in Williston one of the more than 70 fusion centers nationwide. There, data about individual Vermonters is aggregated, stored, and shared. The source of the data ranges from local police departments to the Central Intelligence Agency.

The DHS has fundamentally changed Vermont's role as a border state and extended the scope of border security deep into the state. This report details how that has happened and the threats to individuals' privacy rights posed by the heightened surveillance that now envelops us.

We've created an online map (http://tinyurl.com/q8lwqcr) which identifies where the technologies and systems described in this report have been deployed around the state.

Technologies and Systems

Automated License Plate Readers

What Are ALPRs?

An Automated License Plate Reader (ALPR) is a device that uses digital cameras and optical character-recognition software[7] to read the numbers and letters on license plates. The device can be affixed to police cruisers or mounted on stationary objects such as overpasses or traffic lights. The camera is about 95-percent accurate in capturing a plate's numbers and letters. **An ALPR allows the police to read thousands of license plates per hour whether the vehicle is parked or moving, and to record the plates' GPS locations and the time each plate is read.**

The information is automatically entered into a database, allowing police to determine whether the vehicle has been reported lost or stolen, is being sought as part of an investigation, or may have been involved in a crime or other traffic violation.[8] **Many ALPR systems can connect to other government databases to access owner information.**[9] Vermont's systems currently are not able to do that; a call to the state Department of Motor Vehicles is still needed to identify the owner of the car.

A single ALPR costs around $20,000. States and municipalities typically receive grants from DHS to cover the purchase price.[10]

Are ALPRs Used In Vermont?

Yes. Early adopters included the Vermont State Police as well as police departments in St. Albans, Hartford, Newport, Rutland, and Shelburne.[11] After deploying the technology in St. Albans, police there increased suspended-license arrests 47 percent. As of 2010, **67 percent of all St. Albans patrol division arrests occurred because of an ALPR.**[12]

Currently, about 30 Vermont police agencies have ALPRs, with nearly 50 systems in use statewide. Data captured by the cameras around the state is transferred to a central database maintained by the state Department of Public Safety. The data was originally retained for four years,[13] but legislation passed in 2013 regulating ALPRs lowered the retention period to 18 months.

How Do ALPRs Affect Civil Liberties?

Proponents of ALPRs argue that the data collected is the same as what a police officer sitting and observing traffic could record. However, unlike a human police officer, **an ALPR "captures everything, forgets nothing** and never gets tired or distracted. It captures digital images that can be viewed at any time, from any place, as many times as desired, and can be modified and used well beyond the original intent of either the image collector or the subject."[14] (The ALPR systems Vermont police have been buying can capture 1,800 plates per hour, or 14,400 during an eight-hour shift.)

People's right to privacy is affected whenever government officers record movements of individuals who are not subjects of an investigation. Unlike an officer investigating a crime, these devices are used as a matter of technological routine. **There is no warrant requirement for their use and no judicial oversight.**[15] When the data collected from each reader is aggregated, the various GPS locations at which an ALPR read the license plate, as well as a date and time stamp, can reveal where a person has traveled.[16]

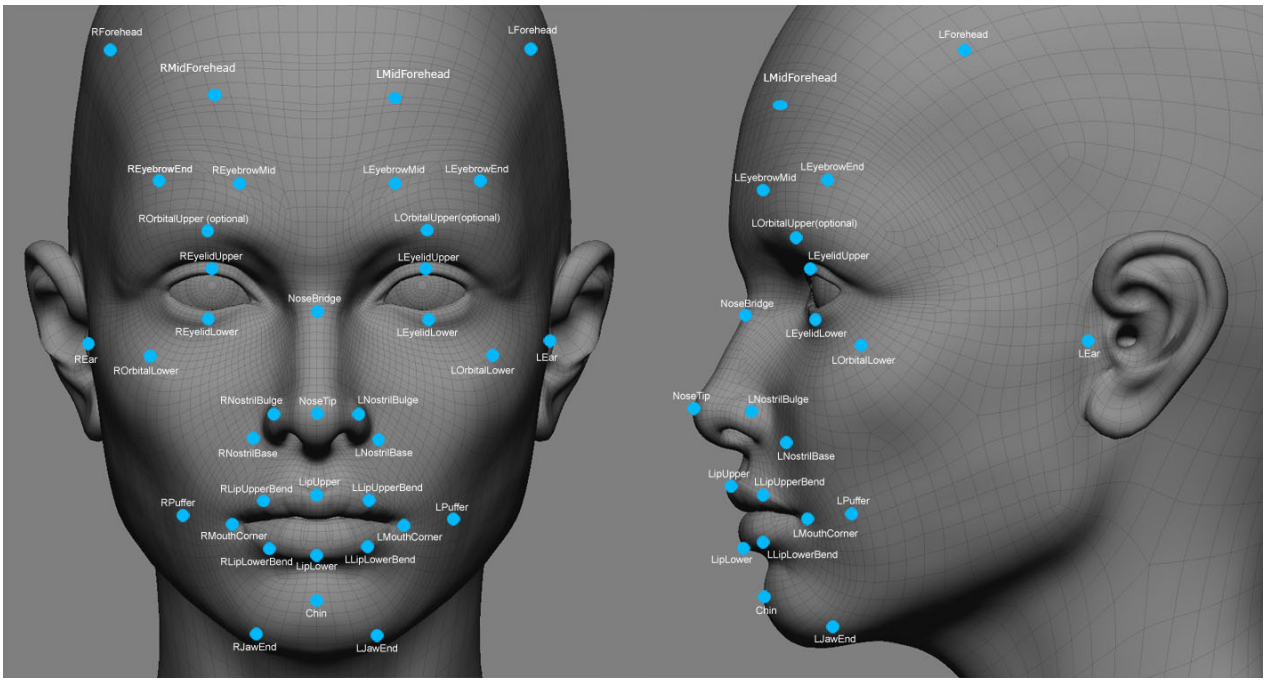
The ALPR systems Vermont police have been buying can capture 1,800 plates per hour.

In early 2012 the U.S. Supreme Court ruled that installing a GPS device on someone's vehicle to track their movements is a search for the purposes of the Fourth Amendment and cannot be conducted without a warrant.[17] However, the court reached its conclusion solely because placing a tracking device on someone's car without their permission is trespassing. The ruling is not a significant privacy protection because placing a tracking device on a car is already an outdated surveillance method. Machine vision systems like ALPRs require no physical intrusion upon a person's property, and hence do not entail the judicial oversight a GPS tracking device would require.

State and federal legislators have largely been left behind by the technology and have not developed laws regulating ALPR use. That changed in Vermont in 2013, when legislators agreed regulation was needed and passed S. 18 (Act 69). Access to what's called "historical" ALPR data is limited to four state police detectives.[18] The data is retained for 18 months on a statewide server; data can be held beyond that through a court-approved preservation order. (ALPR data in other states is retained between 0 days and indefinitely.)

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.[19] 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.[20]



Facial recognition software is part of many software applications we use everyday.

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.[21] 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.[22]

Facial recognition software is already in wide use by the federal government and private entities. The databases where facial recognition data is stored can be used to compare millions of faceprints per minute.[23] 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.[24]

Is Facial Recognition Software Used In Vermont?

Yes. In mid-2012, the DHS provided the Vermont Department of Motor Vehicles (DMV) with a grant to cover the $900,000 cost of using facial recognition software when issuing driver's license and personal ID cards.[25] Facial recognition software is already used for all U.S. passports and passport cards, so Vermonters who possess either identity document for international travel likely already have their photos, and their digital faceprint, in a federal database. Similiar information and images from Vermont driver's licenses will now be in a state database searchable by facial recognition software.

How Does Facial Recognition Software Affect Civil Liberties?

The DMV stressed, in 2012 when the system was bought, that it would use facial recognition software to prevent identity theft and to identify individuals who attempt to use more than one identity when obtaining a driver's license. **Department officials asserted that the DMV database would not be linked with other databases nor made available for use by law enforcement outside the scope of the DMV.**[27] In June 2013, however, DMV officials said the earlier statement had not been accurate and that **the system was in fact being utilized to help police departments in investigations**.[26]

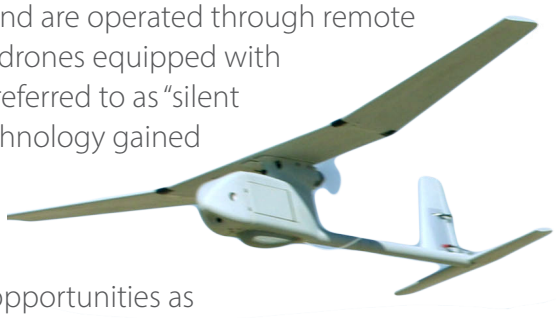
This transformation -- mistaken or not -- is an example of the "repurposing" of identifiers and databases. Created for one purpose, information systems often end up being used for another. Social Security numbers, for instance, were initially prohibited as a form of individual identifier, but they have become a common form of identification.[28]

The collection of information about a person who is not suspected of committing any crime, and the capacity of police to aggregate this information and develop an electronic profile of a person, raise serious privacy concerns. **Through the use of tools such as ALPRs and facial recognition software, the government is conducting a constant investigation, without any reasonable suspicion of wrongdoing. Everyone is, by default, a suspect.**

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."[29] Drone technology gained popular attention for military use overseas, but manufacturers see domestic market opportunities as well.



Drones, manufacturers say, can provide valuable information to first responders and law enforcement. Drones can be used to identify radioactivity in the event of a dirty bomb, to track a gun disposed of by a fleeing criminal, to find the source of wildfires, and to locate missing persons.[30]

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.[31] 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.[32] 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.[33] It can operate day or night.

A U.S. soldier launches a Raven B drone by hand.

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.[34]

Small surveillance drones range in price from $30 to $40,000.[35]

Congress has authorized the FAA to establish new rules for the use of public airspace.[36] However, **no federal agency has been assigned responsibility to watch over the privacy implications of drone usage.**[37] In the interim, the FAA has issued hundreds of testing permits.[38] According to some estimates, 30,000 domestic drones could be deployed in the next decade.[39]

How Do Drones Affect Civil Liberties?

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.

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.[40]

Drone technology runs a high risk of invading individuals' privacy rights, yet **there are few guidelines to regulate their use or to regulate the use and retention of the data they collect.**[41] Some municipalities and states have adopted drone regulations, but Vermont and the federal government have not. (A drone regulation bill was proposed in the Vermont legislature in 2013, but it was not acted upon. U.S. Rep. Peter Welch has introduced a drone regulation bill in Congress.)

The AeroVironment Wasp

Are Drones Used In Vermont By Police?

We do not know. As of September 2013 there had been no confirmed reports of law enforcement-operated drones over Vermont. The state's public safety commissioner, Keith Flynn, has said the state has "no immediate plans" to acquire drones. He promised a robust public review process before any were obtained.[42] No law or regulation is in place requiring such a review, however.

CBP flies the drones for state and local law enforcement.

Unarmed drones were approved for use along both the Mexican and Canadian borders in 2005.[43] By 2011, the CBP service was operating eight Predator drones on the northern and southwestern borders.[44] **There have been confirmed reports of drone use along the northern border in the 950 miles between Minnesota and Washington as well as the 200-mile border between New York and Ontario.**[45]

CBP uses the drones to search for smugglers and undocumented entrants. But it also flies the drones for state and local law enforcement. In 2011, for example, CBP drones were used to locate an individual suspected of cattle rustling in North Dakota.[46]

Drones can also be purchased and used by private individuals and companies (and such drone use has been confirmed in Vermont). Regulation of the use of private drones requires that the right balance be struck between safety and privacy concerns on the one hand, and the right of individuals to own and operate the devices for legitimate purposes on the other hand.

Cell Phone Tracking

What Is Cell Phone Tracking?

Cell phone tracking can refer to real-time surveillance where a person's location is determined by "triangulating" the cell phone towers that the person's phone is interacting with. Cell phone 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 are kept anywhere from four months to two years.[47]

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.**[48] 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.[49] The legality of this practice is being debated in courts across the country, with courts reaching different conclusions.

Is Cell Phone Tracking Used In Vermont?

Yes. In 2010, the **Vermont Attorney General's Office acknowledged that it had obtained cell phone tracking data and had done so without getting a warrant from a court.**[50] It is unclear whether the attorney general followed any standards in justifying collection of the information. It is also unclear how widespread law enforcement's use of cell phone tracking is.[51] What oversight we know about has been through secret proceedings called "inquests."

Case: 2009-215462 Back | Print
Target: [redacted]

GPS ID	Request Date (CST)	Location Date (CST)	Status	Points	Accuracy	Bill
7715912	10/9/2009 9:42:31 AM	10/9/2009 9:45:30 AM	Success	40.00178 - 82.96392	4999.00*	D
7715434	10/9/2009 9:27:27 AM	10/9/2009 9:30:24 AM	Success	40.00069 - 82.97771	80.00	D
7715419	10/9/2009 9:26:50 AM	10/9/2009 9:28:47 AM	Success	40.00178 - 82.96392	4999.00*	D
7715077	10/9/2009 9:17:25 AM	10/9/2009 9:20:28 AM	Failure		0.00	N
7714609	10/9/2009 9:02:16 AM	10/9/2009 9:03:36 AM	Success	40.0004 - 82.97674	25.00	D
7714142	10/9/2009 8:47:09 AM	10/9/2009 8:34:45 AM**	Success	40.00178 - 82.96392	4999.00*	N

Cell phone tracking data.

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, store that information, and use it in conjunction with other intelligence to create a comprehensive picture of a person's life and where he or she has been.**

Government does not have the right to build profiles of citizens, absent a showing of wrongdoing.

Police and prosecutors claim the authority to track cell phone locations without court oversight by citing a 1979 U. S. Supreme Court decision, United States v. Miller, 425 h.s. 436 (1976). 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 or transfer money) 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 opens a bank account or purchases a cell phone expecting that all of his or her resulting data will be shared with the government in the absence of a search warrant.**

Not only is it not realistic to ask Americans to choose between meaningful personal privacy and the modern necessities of a bank account or 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.

Vermont 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.[52] **Between 2001 and 2007, individual states received around $380 million in federal funding to establish these centers.**[53] **There are more than 70 centers around the country, with at least one in each state.**[54]

Despite the country's myriad fusion centers, the Government Accountability Office has found that information-sharing between Border Patrol and local law enforcement is inconsistent.[55] A report by the U.S. Senate Homeland Security Subcommittee in late 2012 termed the centers a waste of money that often step on citizens' rights.[56]

A report by the U.S. Senate Homeland Security Subcommittee deemed fusion centers a waste of money that often step on citizens' rights.

Does Vermont Have A Fusion Center?

The Vermont Fusion Center (it is now known formally as the "Vermont Information and Analysis Center") is run by the Vermont State Police and has been located in Williston since its establishment in 2005, along with the DHS's Immigration and Customs Enforcement Law Enforcement Support Center. In addition to information provided by state police, county sheriffs, and municipal police departments, the Vermont Fusion Center receives counter-terrorism and intelligence information from federal agencies such as the Bureau of Alcohol, Tobacco, Firearms and Explosives, and the Drug Enforcement Administration, as well as the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, and Quebec Provincial Police.[57]

How Do Fusion Centers Affect Civil Liberties?

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.[58]

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.**[59]

Second, even if not actively engaged in investigations, **a fusion center is, by its nature, dangerously close to invading the privacy of everyday citizens.**[60] The centers collect so much information about people from various sources that a picture of an individual's daily activities can readily be developed. Vermonters 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 a "total surveillance society."

How Does The NSA Fit With Fusion Centers?

The National Security Agency (NSA) is an ultra-secret federal agency largely shielded from public view and oversight. Certain members of Congress receive confidential briefings on its activities, but the scope and breadth of its operations are largely unknown.

Due to the high level of secrecy surrounding the NSA, we do not know what interaction the NSA has with fusion centers. However, we do understand the basic function of the NSA is to aggregate huge amounts of data – both foreign and domestic. We also know that fusion centers are storing data from state police, county sheriffs, and municipal police departments *as well as* federal agencies. **It seems likely that there is data sharing between the NSA and fusion centers**.

In May 2013, an NSA contracted employee, Edward Snowden, leaked details of a massive NSA program that was collecting not only basic phone call routing ("meta data") information (number called, time of call, length of call, etc.) but possibly also entire phone conversations, as well as other electronic communications such as e-mails. The bright light shone by Snowden led to calls for greater scrutiny of NSA programs, and more information about the confidential court orders issued by the secret Foreign Intelligence Surveillance court, which has some limited oversight of NSA activities.

The NSA has told Congress that it needs to collect all this information just in case it is needed later to solve terrorist crimes. It claims, broadly, that it is not snooping into innocent Americans' lives. Specific data is accessed only when the NSA shows to the FISA court its legitimate, lawful need for the data, officials say.

With no public oversight of this process, though, it is impossible to know if information detailing the private lives of Americans – and likely others around the world – is secure. The American rule of law is that government does not collect information about people unless they are suspected of committing a crime and police can convince a court that a warrant to violate what would otherwise be private information is justified.

That principle is now being turned on its head by the ease with which information about us and our activities is collected, stored, and retrieved. Information is now largely reduced to a universal digital form, stored in massive central databases. The information can easily be searched by sophisticated software programs and used to compile highly detailed profiles of an individual. **The privacy of obscurity once offered by paper records in manila folders tucked in file cabinets in offices scattered around towns, states, and the country is largely gone.** Access now is often no more than a few keystrokes away, from anywhere in the world. The legal system has not kept up with this fundamental shift. We are left living in a society where information becomes power -- a power not yet checked by the normal rules of law.

How Has All This Happened?

A decade into the 21st century, Vermont in many ways remains behind the times, technologically speaking. Cell phone coverage remains limited in significant areas of the state. The slow expansion of high-speed broadband Internet continues to lag behind build-out in other states and countries. So why, when personal use of technology has not reached its potential, have state and local governments in Vermont been able to adopt a range of high-tech surveillance tools to monitor people and their movements?

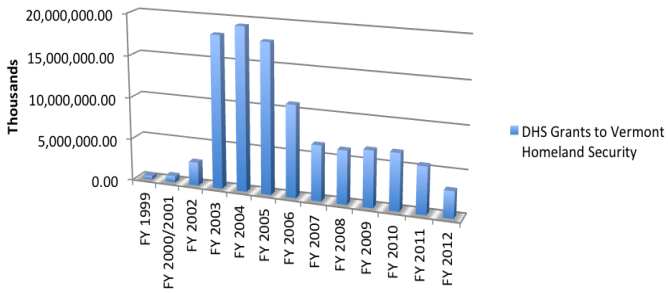
Federal Dependence on Local Law Enforcement

Since September 11, 2001, the federal government has recognized that it needs the assistance of local law enforcement to succeed in counter-terrorism efforts, particularly to expand information-sharing among federal, state, local, and tribal law enforcement.[61] After all, while the FBI has approximately 13,000 special agents, **state and local law enforcement agencies nationwide comprise a force of around 765,000 full-time officers,** most of whom are generally more familiar with local communities than FBI agents.[62]

Local law enforcement is now expected to respond to terrorism-related emergencies, and their public protection role includes a prioritized awareness of guarding against terrorist threats.[63] However, a focus on intelligence-gathering poses substantial threats to civil liberties – threats that may often not be recognized in the surveillance tools and systems utilized by individual agencies.[64] The aggregation of these tools, however, creates a society unlike any that Vermonters have ever known.

Money and Manpower

When police engage in activities beyond their traditional scope, the traditional checks on police power also become strained. **Historically, police have been held accountable to their communities through control over the police budget** by elected officials and citizens' electoral control either directly over police leadership (such as an elected county sheriff) or, one step removed, over the elected officials who oversee police departments.



Source:* Vermont Homeland Security, Department of Public Safety, Homeland Security Grants: *http://hsu.vermont.gov/grants

For many years, the U.S. Department of Justice has supported local law enforcement with federal grants for community-oriented policing. These grants have not tended to refocus the mission or operation of state, municipal, or tribal police.[65] However, the new homeland security role expected of local police has changed things. Not only is their expanded role supported in large measure by federal grants rather than local tax dollars, but more importantly, the expansion is a departure from the traditional role of a local police department. Federal homeland security grants are not made to improve local, on-the-street policing. Instead, they support surveillance tools and technologies that are part of a larger national security program.

The additional homeland security money can be substantial. In Vermont, the Department of Public Safety saw

almost a threefold increase in federal funding in the first fiscal year after September 11th.[66] Within three years, Vermont received $39 million in DHS grants, whereas in the three fiscal years immediately preceding September 11th, the state received only around $1.15 million in similar federal funds. (Annual grant funds are now around $3 million.)[67]

Public Disclosure

In addition to diminishing local control, the homeland security role adopted by local police generally demands secrecy, so that the public is only partially aware, or completely unaware, of the tactics and activities utilized in this new area of police services.

After the Watergate scandals of the early 1970s, Congress placed a series of checks on secret surveillance activities. These checks were largely rolled back by the USA PATRIOT Act of 2001, however.

Further secrecy results from the confusion of who has the responsibility for running and overseeing surveillance activities. **Sufficient checks are unlikely to be in place, particularly because inter-branch or outside monitoring may not be as extensive, or as formal, as on the federal level.**[68] The development, scope, and implementation of the statewide Automated License Plate Reader (ALPR) system in Vermont, for example, only became public knowledge through a public records request submitted by the ACLU of Vermont.[69]

All of this is further aggravated by the lack of judicial oversight. When police monitor public areas, the general legal rule is that no warrant is required because the activities are in public view.[70] This doctrine has been extended to high-tech tools such as ALPRs and drones – despite the fact that these sophisticated devices have much deeper capabilities for gathering information.

The Northern Border

The DHS operates a multi-layered border surveillance system. The first two layers include line watch and roving patrol.[71] In addition, **DHS claims authority (citing a 1970s court case) up to 100 miles, as the crow flies, from a border (including coast lines)** and operates traffic checkpoints within this buffer zone. Because Vermont is only 157 miles long from north to south, and the eastern part of the state is within 100 miles of the Atlantic coast, **approximately 94 percent of Vermonters live within 100 miles of either the Vermont-Canada border or the eastern seacoast.**[72]

The DHS unit responsible for border security is the U.S. Border Patrol, whose primary mission is to "prevent terrorists and terrorist weapons, including weapons of mass destruction, from entering the United States."[73] The Border Patrol also retains its historic mission to prevent smugglers, drugs, contraband, and undocumented foreign nationals from entering the country. **In 2010 DHS spent nearly $3 billion protecting the northern border, made 6,000 arrests and interdicted 40,000 pounds of illegal drugs.**[74]

Generally, when police officers or other law enforcement officials want to stop your vehicle, they are required to have at least reasonable suspicion that the driver has committed a crime, or that there is evidence of a crime in

the vehicle. However, the U.S. Supreme Court has ruled that individuals have fewer protections against stops and searches conducted by the Border Patrol. The Border Patrol takes that authority one step further by asserting that its agents can establish fixed checkpoints within the 100-mile border zone and question occupants even without reasonable suspicion that they are illegal aliens.[75] Checkpoint agents also claim wide discretion to subject vehicles to secondary inspection and additional questioning.[76] Because DHS says it can operate in nearly all of Vermont, this allows DHS, though not state or local police, to establish checkpoints and make stops without any suspicion that drivers or passengers have done anything wrong.

At the Border

The DHS maintains ports of entry in Vermont in Beecher Falls, Derby Line, Highgate Springs, Norton, and Richford.[77] The Burlington International Airport also operates as a port of entry, and St. Albans is home to a service port.[78]

Securing the area between ports of entry, however, is an ongoing project for CBP. In 2011, DHS abandoned a program that involved affixing sensors, radar, and cameras to towers between ports of entry to transmit information to command centers. The program failed cost-effectiveness and viability standards.[79] In its place, DHS plans to invest in remote video and mobile surveillance as well as hand-held equipment.[80]

Internal Checkpoints

The Border Patrol operates interior checkpoints generally between 25 and 100 miles from the U.S. border. The goal of the checkpoints is to arrest foreign nationals attempting to enter the United States without documentation, as well as to interdict contraband.[81] **As of 2009, interior checkpoints accounted for about one-third of Border Patrol drug seizures.**[82] Some internal checkpoints are temporary, while others involve permanent structures. Permanent checkpoints also generally include off-highway areas where agents conduct vehicle inspections, as well as physical space for detention of suspects. They are also networked for access to national law enforcement databases. Most checkpoints operate on the southwestern border with Mexico.

In December 2003 CBP established a traffic checkpoint on I-91 in Hartford, as a temporary checkpoint operating on weekends, and then expanded it to a full-time operation.[83] **Within a year, after taking over 600 people into custody at the location, DHS sought to make the checkpoint permanent.**[84] However, the checkpoint was criticized for alleged racial profiling practices. Area schools began instructing their international students to carry documentation of their legal status.[85] In 2005, U.S. Sen. Patrick Leahy questioned then-CBP Commissioner Robert Bonner at a congressional hearing on the checkpoint, suggesting that it resulted in unnecessary stops of area residents, not increased border security.[86]

Even so, CPB continued to operate the checkpoint sporadically, and has the capacity to add additional checkpoints at its discretion. In fact, CPB has developed plans to erect permanent interior checkpoints along all major interstate highways in New England and New York leading south from Canada. Through a public records request, the ACLU-VT obtained documents showing site plans and analysis of various specific locations. The plans appear on hold at the moment.

In June 2013 Sen. Leahy added a provision to the Senate's immigration bill that would prohibit internal checkpoints such as the one that CPB has operated at White River Junction.

The ACLU-VT is grateful to Rachel Seelig, Esq., for researching and drafting this report.

The ACLU-VT has endeavored to ensure that the information in this report is as complete and accurate as possible. Surveillance techniques and applications change rapidly – as does the information made available about them due to the secrecy that sometimes surrounds these matters. Please write us at info@acluvt.org if you believe there are errors or omissions in this report. We are committed to fair, accurate, and comprehensive reporting on this issue, and we will update our online edition of the report if inaccuracies are found.

End Notes

1 John Kifner & William Rashbaum, Brooklyn Man is Charged With Aiding in Bomb Plot, N.Y. Times, Dec. 31, 1999.

2 Creation of the Department of Homeland Security, http://www.dhs.gov/creation-department-homeland-security (last visited Aug. 1, 2012).

3 Border Security Results, http://www.dhs.gov/border-security-results (last visited Aug. 2, 2012).

4 Government Accountability Office, Border Patrol: Checkpoints Contribute to Border Patrol's Mission, but More Consistent Data Collection and Performance Measurement Could Improve Effectiveness 5 (2009), available at http://www.gao.gov/assets/300/294548.pdf [hereinafter GAO Checkpoints Report].

5 See Government Accountability Office, Border Security: Enhance DHS Oversight and Assessment of Interagency Coordination is Needed for the Northern Border (2010).

6 Top Secret America: A Washington Post Investigation, Wash. Post, available at http://projects.washingtonpost.com/top-secret-america/states/vermont/.

7 Ken Picard, Digital Apprehensions, Seven Days Dec. 8, 2010.

8 Id.

9 American Civil Liberties Union of Vermont, ALPR Could Be Tracking Where You Drive, Oct. 22, 2010, available at http://www.acluvt.org/blog/2010/10/22/alpr-could-be-tracking-where-you-drive/; Ken Picard, Digital Apprehensions, Seven Days Dec. 8, 2010.

10 Picard, Digital Apprehensions, supra note 28.

11 Id.

12 Id.

13 Community Decision: Norwich Rejects Plate Reader, Valley News, May 20, 2012; Driving? An LPR is Watching You, ACLU-VT Aug. 9, 2012, available at http://www.acluvt.org/blog/2012/08/09/driving-an-lpr-is-watching-you/.

14 Carla Scherr, Note, You Better Watch Out, You Better Not Frown, New Video Surveillance Techniques are Already in Town (and Other Public Spaces), 3 I/S J.L. & Pol'y For Info. Soc'y 499, 505 (2007–08)

15 See Picard, Digital Apprehensions, supra note 28.

16 Id. (describing a criminal case in which data from ALPRs mounted on cars that responded to a number of robberies were aggregated and identified a vehicle that appeared on multiple occasions).

17 United States v. Jones, --- U.S. ---, 132 S. Ct. 945 (2012).

18 Id.

19 Ken Picard, Vermont DMV to Use Facial Recognition Software On All New Driver's License Photos and IDs, Seven Days, July 16, 2012 [hereinafter Vermont DMV to Use Facial Recognition].

20 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).

21 Id.

22 James Temple, Facial Recognition Software's Privacy Concerns, SFGate, June 19, 2012.

23 Bennett, supra note 46 at 155.

24 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_.

25 Picard, Vermont DMV to Use Facial Recognition, supra note 45.

26 Id.

27 Id.

28 Jay Stanley & Barry Steinhardt, Bigger Monster, Weaker Chains: The Growth of An American Surveillance Society 13 (2002).
29 Drones: Who is Watching You?, ABC News, Feb. 15, 2012, available at http://abcnews.go.com/Nightline/video/drones-watching-15661073.
30 Brian Bennett, Drones Tested as Tools for Police and Firefighters, L.A. Times, Aug. 5, 2012 [hereinafter Drones Tested for Police].
31 Fact and Fiction: Plenty to Worry About Drones, Valley News, June 24, 2012.
32 UAS: Raven, AeroVironment, http://www.avinc.com/uas/small_uas/raven/ (last visited Aug. 8, 2013).
33 Raven, AeroVironment, http://www.avinc.com/downloads/Raven_Gimbal.pdf (last visited Aug. 8, 2013).
34 Wasp, AeroVironment, http://www.avinc.com/downloads/USAirForceFactSheet.pdf (last visited Aug. 8, 2013).
35 W.J. Hennigan, Idea of Civilians Using Drone Aircraft May Soon Fly with FAA, L.A. Times, Nov. 27, 2011; Peter Finn, Privacy Issues Hover Over Police Drone Use, Wash. Post Jan. 23, 2011 at A-01.
36 Id.; Hennigan, supra note 14; Fact and Fiction: Plenty to Worry About Drones, supra note 9.
37 Allison Grande, New Drone Bill Highlights Growing Privacy Concerns, Law360, July 25, 2012.
38 Leslie Harris, Opinion, UAVs: Will Our Civil Liberties Be Droned Out? ABC News, June 7, 2012, available at http://abcnews.go.com/Technology/unmanned-aerial-vehicles-civil-liberties-droned/story?id=16511914#.UBpsxDFWofj; Hennigan, supra note 14.
39 Kevin McCaney, Bill Would Require Warrants for Domestic Drone surveillance, Government Computer News, June 14, 2012.
40 Larry Abramson, Drones: From War Weapon to Homemade Toy, VPR News (Aug. 2, 2012), http://www.vpr.net/npr/157441681/ (last visited Sept. 1, 2012).
41 Harris, supra note 18; Bennett, Drones Tested for Police, supra note 8.
42 Bob Kinzel, Domestic Drones on Law Enforcement's Radar, VPR News (Aug. 21, 2012), http://www.vpr.net/news_detail/95605/domestic-drones-on-law-enforcements-radar/.
43 American Civil Liberties Union of Vermont, Drones Over Vermont?, June 15, 2010, available at http://www.acluvt.org/blog/2010/06/15/drones-over-vermont/.
44 Brian Bennett, Police Employ Predator Drone Spy Planes on Home Front, L.A. Times, Dec. 10, 2011, available at http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211 [hereinafter Police Employ Predator Drone].
45 Border Security Results, supra note 3.
46 Bennett, Police Employ Predator Drone, supra note 21.
47 Cell Phone Location Tracking Request Response – Cell Phone Company Data Retention Chart, ACLU, available at http://www.aclu.org/cell-phone-location-tracking-request-response-cell-phone-company-data-retention-chart.
48 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.
49 Id.
50 AG Gathering Cell Phone Tracking Data, ACLU-VT http://www.acluvt.org/blog/2010/11/12/ag-gathering-cell-phone-tracking-data-info-obtained-without-warrant/ (last visited Sept. 1, 2012).
51 What Goes On At An Inquest?, ACLU-VT, Mar. 23, 2011; http://www.acluvt.org/blog/2011/03/23/what-goes-on-at-an-inquest/#more-734.
52 Department of Homeland Security, State and Major Urban Area Fusion Centers, available at http://www.dhs.gov/state-and-major-urban-area-fusion-centers (last visited Aug. 20, 2012).
53 Mary Beth Sheridan, States Setting Up Own Antiterror Centers, Boston Globe, Jan. 1, 2007, available at http://www.boston.com/news/nation/washington/articles/2007/01/01/states_setting_up_own_antiterror_centers/?page=1.
54 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).

55 Government Accountability Office, Border Security: DHS Progress and Challenges in Securing the U.S. Southwest and Northern Borders 16 (2011), available at http://www.gao.gov/new.items/d11508t.pdf [hereinafter GAO Border Security Progress Report).

56 Permanent Subcommittee on Investigations, Investigative Report Criticizes Counterterrorism Reporting, Waste At State & Local Intelligence Fusion Centers, available at http://www.hsgac.senate.gov/subcommittees/investigations/media/investigative-report-criticizes-counterterrorism-reporting-waste-at-state-and-local-intelligence-fusion-centers

57 Top Secret America: A Washington Post Investigation, supra note 6.

58 Sheridan, supra note 67.

59 Id.

60 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).

61 Waxman, supra note 68 at 377 (2009).

62 See Brian A. Reaves, Bureau of Justice Statistics, Census of State and Local Law Enforcement Agencies, 2008 1 (2011), http://bjs.ojp.usdoj.gov/content/pub/pdf/csllea08.pdf.

63 Waxman, supra note 68 at 383–84.

64 Id. at 385.

65 Id. at 392.

66 Vermont Homeland Security, Department of Public Safety, Homeland Security Grants, http://hsu.vermont.gov/grants (last visited Oct. 1, 2012).

67 Id.

68 Id. at 398.

69 See Driving? An LPR is Watching You, supra note 34.

70 See, e.g. Coolidge v. New Hampshire, 403 U.S. 443 (1971); Arizona v. Hicks, 480 U.S. 321 (1987).

71 GAO Checkpoint Report, supra note 4.

72 Vermont in the United States, http://academics.smcvt.edu/vtgeographic/textbook/vtinUS/vermont_in_the_united_states_and.htm (last visited Aug. 20, 2012); ACLU Constitution Free Zone – Map, ACLU, http://www.aclu.org/constitution-free-zone-map#NM (last visited Aug. 20, 2012).

73 GAO Checkpoint Report, supra note 4, at 7.

74 Dan Freedman, GAO Report Criticizes U.S. Effort on Northern Border, Albany Times-Union, Feb. 1, 2011.

75 U.S. v. Martinez-Fuerte, 428 U.S. 543, 545 (1976).

76 Id. at 563–64.

77 Vermont, http://cbp.gov/xp/cgov/toolbox/contacts/ports/vt/ (last visited Aug. 7, 2012).

78 Id.

79 GAO Border Security Progress Report, supra note 70, at 18.

80 Id.

81 GAO Checkpoint Report, supra note 4 at 5.

82 Id.

83 Border Patrol Stops, ACLU-VT http://www.acluvt.org/issues/border_patrol_stops.php (last visited July 30, 2012).

84 Steve Zind, Border Patrol Wants I-91 Checkpoint to Be Permanent, VPR (Dec. 30, 2004), available at http://www.vpr.net/news_detail/72431/border-patrol-wants-1-91-checkpoint-to-be-permanen/.

85 Hannah Kuhar, Border Patrol Creates Checkpoints, The Dartmouth (Dec. 16, 2009).

86 See Residents, Senators Raise Questions About I-91 Checkpoint, VPR News (March 7, 2005), available at http://www.vpr.net/news_detail/72801/residents-senators-raise-questions-about-i-91-chec/.