CONFRONTING AUTOMATED LAW ENFORCEMENT

Lisa Shay, Woodrow Hartzog, John Nelson, Dominic Larkin, and Gregory Conti

The time has come for a cohesive approach to automated law enforcement. The ubiquity of sensors, advances in computerized analysis and robotics, and widespread adoption of networked technologies have paved the way for the combination of sensor systems with law enforcement algorithms and punishment feedback loops. While in the past, law enforcement was manpower intensive and moderated by the discretion of the police officer on the beat, automated systems scale efficiently, allow meticulous enforcement of the law, provide rapid dispatch of punishment and offer financial incentives to law enforcement agencies, governments, and purveyors of these systems. Unfortunately, laws were not created with such broad attempts at enforcement in mind and the future portends significant harms to society where many types of violations, particularly minor infractions, can be enforced with unprecedented rigor.

This article provides a framework for analysis of automated law enforcement systems that includes a conceptualization of automated law enforcement as the process of automating some or all aspects of surveillance, analysis, and enforcement in an iterative feedback loop. We demonstrate how intended and unintended consequences can result from the automation of any stage in this process and provide a list of issues that must be considered in any automated law enforcement scheme. Those deploying automated law enforcement schemes should be extremely cautious to ensure that the necessary calculus has been performed and adequate safeguards have been incorporated to minimize the potential for public harm while preserving the benefits of automation.

Confronting Automated Law Enforcement

Lisa Shay,[1] *Woodrow Hartzog,*[2] *John Nelson,*[3] *Dominic Larkin,*[4] *and Gregory Conti*[5]

TABLE OF CONTENTS

[1] Assistant Professor in the Department of Electrical Engineering and Computer Science at the US Military Academy at West Point.

[2] Assistant Professor at the Cumberland School of Law at Samford University; Affiliate Scholar at the Center for Internet and Society at Stanford Law School.

[3] Assistant Professor in the Department English and Philosophy at the US Military Academy at West Point.

[4] Assistant Professor in the Department of Electrical Engineering and Computer Science at the US Military Academy at West Point.

[5] Associate Professor in the Department of Electrical Engineering and Computer Science at the US Military Academy at West Point.

INTRODUCTION: THE RISE OF AUTOMATION

We are rapidly approaching a time when automated law enforcement will no longer be an aberration, but rather a viable option for many law enforcement agencies. Consider the following hypothetical based on existing technology: Driving down a highway where the speed limit is 65mph, your vehicle's built-in GPS receiver detects that you are approaching a large city. Cross-referencing your location with a database of speed limits, the car determines that the speed limit reduces to 55mph in another mile. A pleasant computer-generated contralto emits from the speaker system, "Warning! Speed limit reducing to 55 mph."

However, there is excellent weather and visibility, and traffic is moving briskly. Unaware of new law enforcement policies in effect, you decide to maintain the prevailing traffic flow at 63 mph. As you cross into the 55mph zone, your vehicle's pleasant contralto announces, "Posted speed limit exceeded, authorities notified." Simultaneously, your vehicle's on-board communications system notifies a nationwide moving-violation tracking system indicating the date, time, location, vehicle registration, and recorded speed. The tracking system determines, based on location, the appropriate agency. The police agency's computer looks up the appropriate fine and emails a ticket to the person registered as the vehicle's owner as well as to the company insuring the vehicle. This is an example of "perfect surveillance and enforcement."[6] Alternatively, the vehicle could have been programmed to simply reduce speed to the posted speed limit, a sort of reverse cruise control. This would be an example of "perfect prevention" or "preemption."[7]

[6] Christina M. Mulligan, *Perfect Enforcement of the Law: When to Limit and When to Use Technology*, 14 RICH J.L. & TECH. 13 (2008); JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET—AND HOW TO STOP IT 101-126 (2008).

[7] Mulligan, *supra* note 6, at 8; ZITTRAIN, *SUPRA* NOTE 6, AT 108.

This scenario is not science fiction. Technologically, legal restrictions could be enforced through the use of sensors and computers in an iterative feedback loop.[8] Driving laws are not the only kind of law that could be automatically enforced. It is already possible to use GPS technology to enforce restraining orders.[9] A GPS-enabled bracelet or anklet could be fitted to an offender to track his or her location. If the offender enters a prohibited area, such as within 100 feet of a victim's home, the victim and police could be notified. If the victim were also carrying a GPS-enabled device (not necessarily a bracelet/anklet, it could just be a smart phone), the victim could be aware any time the offender came within any specified distance.

Social and political motivation is all that is needed to spur the actuality of many automated law enforcement systems capable of perfect surveillance and enforcement. However, no common legal or technical infrastructure has been widely adopted for the deployment and constraint of automated law enforcement schemes.[10] Given the inevitability of

[8] Many consumer grade automotive GPS devices display the posted speed limit for most major roads and highways. *See Frequently Asked Questions*, GARMIN.COM (Jan 8 2012), http://support.garmin.com/support/searchSupport/case.faces?caseId={c9512840-ea61-11de-5887-000000000000}. *OnStar For My Vehicle*, ONSTAR.COM, (Dec. 21, 2011). Many vehicles already have built-in GPS devices, such as those equipped with the OnStar system. Once offered only with GM vehicles, the OnStar system can now be installed in any vehicle with a rear-view mirror. Though not currently implemented, it would not be difficult to combine a database that maps the location determined by GPS with the posted speed limit to determine when infractions occur. The OnStar system includes a 2-way communications system that could not only relay customer distress calls to a central call processing center, but could relay data messages to a central traffic monitoring system. Another means of implementing this system is demonstrated by the "smart road" pilot project near Blacksburg, Virginia. The smart road will have a roadside communications system installed that would allow "data collection from sensors, and dynamic in-vehicle information systems." *Smart Road Facts,* VIRGINIA DEPARTMENT OF TRANSPORTATION (Jan. 10 2010), http://www.virginiadot.org/projects/constsal-smartrdfacts.asp.

[9] The Omnilink corporation offers this service for victims of domestic violence. *See Domestic Violence Offenders,* OMNILINK.COM, http://www.omnilink.com/Omnilink_Solutions/CriminalJustice/DomesticViolenceOffenders.html (accessed 26 March 2012).

[10] *See* Robin Miller, *Automated Traffic Enforcement Systems,* 26 A.L.R.6th 179 (2007); *cf* Press Release, TIA's First Smart Device Communications Specification Lays Foundation for Future Standards on M2M and the Internet of Things (Dec. 12, 2011), http://www.tiaonline.org/news_events/press_room/press_releases/2011/PR-1215_TIA_s_First_Smart_Device_Communications_Specificat.cfm .

technological progress, we must now confront automated law enforcement.

The capacity for automated law enforcement exists in many realms where sensors and computers observe and record an individual's activity, far beyond their driving behavior or a record of their location. The ubiquity of sensors,[11] advances in computerized analysis and robotics,[12] and widespread adoption of networked technologies have enabled the combination of sensor systems with law enforcement algorithms and punishment feedback loops.[13] While in the past, law enforcement was manpower intensive and moderated by an officer's discretion, automated systems scale efficiently, allow meticulous and tireless enforcement of many laws, promise rapid dispatch of punishment, and offer financial incentives to law enforcement agencies, governments, and purveyors of these systems.

In the past, laws were not created with an expectation of perfect enforcement. Yet the future portends significant harms to a society where many types of violations, particularly minor infractions, can be enforced with unprecedented range and rigor.[14] This article examines the potential scope of automated law enforcement in an attempt to theoretically refine the phenomenon as a concept capable of being carefully implemented and properly constrained. To that end, it provides a generalized framework for analysis of automated enforcement systems that includes a conceptualization of automated law enforcement as the process of

[11] *See, e.g.*, Gregory Conti, *Our Instrumented Lives: Sensors, Sensors, Everywhere*, Defcon 19, August 2011; Lisa Shay, Gregory Conti, Dominic Larkin, and John Nelson, *A Framework for Analysis of Quotidian Exposure in an Instrumented World,* submitted to the Privacy Enhancing Technologies Symposium, July 2012 (under review).

[12] *See, e.g.*, Lora G. Weiss, *Autonomous Robots In the Fog of War*, IEEE SPECTRUM, 30-34,56-57 (August 2011).

[13] *See, e.g.*, Richard Retting, Susan Ferguson, & A. Shalom Hakkert, *Effects of Red Light Cameras on Violations and Crashes: A Review of the International Literature*, 4 TRAFFIC INJURY PREVENTION 17; Declan McCullagh, *Homeland Security moves forward with 'pre-crime' detection*, CNET.COM (Oct. 7, 2011), http://news.cnet.com/8301-31921_3-20117058-281/homeland-security-moves-forward-with-pre-crime-detection/ (describing the US Department of Homeland Security's Future Attribute Screening Technology (FAST) initiative.).

[14] *See, e.g.*, Amar Toor, *Cordon multi-target photo-radar system leaves no car untagged*, ENGADGET (Oct. 31, 2011); Mark Gillispie, *High-tech carts will tell on Cleveland residents who don't recycle... and they face $100 fine*, CELEVELAND.COM, (Aug. 20, 2010), http://blog.cleveland.com/metro/2010/08/city_of_cleveland_to_use_high-.html.

automating some or all aspects of surveillance, analysis, and enforcement in an iterative feedback loop.

This article explores the consequences of automating any stage in the law enforcement process and provides a list of issues critical to any automated enforcement scheme. Our goal is not to answer the many questions that arise with automated law enforcement, but rather provide an analytic framework to analyze those questions. The focus of most currently automated law enforcement schemes, as well as the focus of this paper, is largely on minor infractions. However, the potential scope of such systems threatens to be much larger.

The approach to the implementation of these automated law enforcement schemes has thus far been incomplete.[15] Technological failures, administrative burdens,[16] inadvertent lawmaking when designing software,[17] loss of discretion, threats to an individual's legal rights, and the social cost of perfect enforcement are all potential consequences of automation that should, but are often not, be considered when employing these systems. This paper will rely on empirical and theoretical research to outline the necessary calculus that should be performed in order to deploy an automated law enforcement scheme. This framework will help ensure adequate safeguards to minimize public harm while preserving the benefits of automation.[18]

[15] *See, e.g.,* Jeffery A. Parness, *Beyond Red Light Enforcement Against the Guilty But Innocent: Local Regulations of Secondary Culprits,* 47 WILLAMETTE L. REV. 259 (2011); Robin Miller, *Automated Traffic Enforcement Systems,* 26 A.L.R.6th 179 (2007); Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age,* 88 TEX. L. REV. 669 (2010); Joel O. Christensen, Note, *Wrong on Red: The Constitutional Case Against Red Light Cameras,* 32 WASH. U. J.L. & POL'Y 443 (2010).

[16] Our definition of "administrative burdens" includes the burden placed on citizens when correcting errors. Bureaucratic processes have been criticized as inefficient in such cases, perhaps best exemplified by the convoluted and time consuming processes for correcting credit report errors and combating identity theft. *See, e.g., How To Dispute Credit Errors,* FEDERAL TRADE COMMISSION (Oct. 2011), http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre21.shtm.

[17]*See* Danielle Keats Citron, *Technological Due Process,* 85 WASH. U. L. REV. 1249 (2008); James Grimmelmann, Note, *Regulation by Software,* 114 YALE L. J. 1719 (2005); LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999).

[18] *See* Elizabeth Joh, *Discretionless Policing: Technology and the Fourth Amendment,* 95 CAL. L. REV. 199, 203-04 (2007).

I. CONCEPTUALIZING AUTOMATED LAW ENFORCEMENT

The first challenge in confronting automated law enforcement is determining what the concept actually entails. There is no set conceptualization for what constitutes an automated law enforcement system. This is perhaps an obvious problem—that which remains undefined is incapable of being properly restrained and controlled. Thus, this article attempts to encapsulate the concept by giving it as pliable and technology-neutral definition as possible.

We define automated law enforcement as any computer-based system that uses input from unattended sensors to algorithmically determine that a crime has been or is about to be committed and then takes some responsive action, such as to warn the subject or inform the appropriate law enforcement agency. Additionally, these systems will be capable of automatically imposing some form of punishment. Our proposed conceptualization of automated law enforcement is based on a model that is subject to automation at various points, shown in Figure 1.

That model consists of a subject, the person monitored who may or may not commit a crime; law enforcement agencies who conduct surveillance, analysis, and enforcement; and a judicial system that determines guilt and imposes punishment in certain cases. There are also feedback mechanisms that relay warnings and/or notices of crimes back to the subject and to the designated agency. Automation anywhere in these three areas can trigger the considerations listed later in this article.

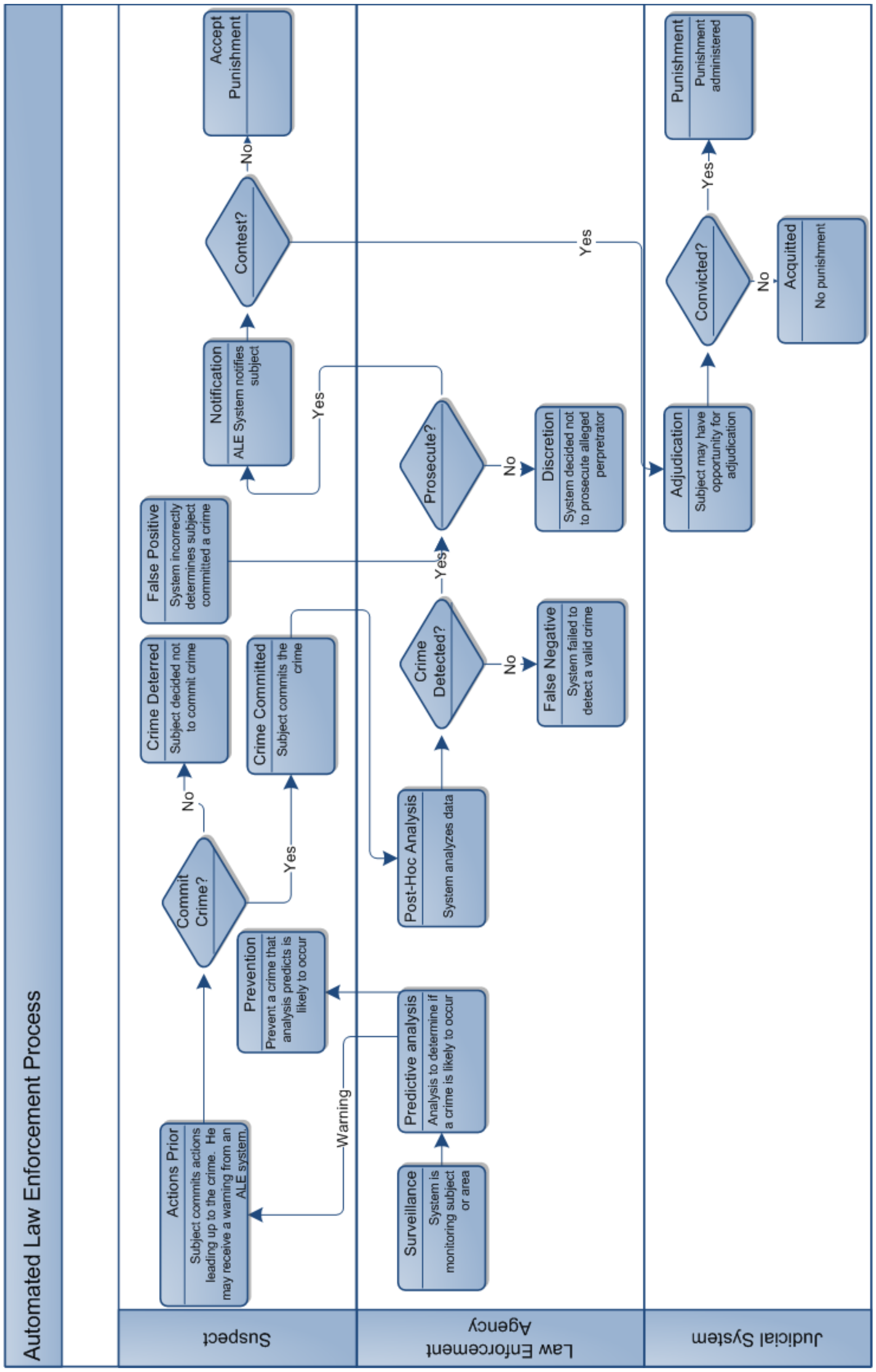
Our model draws on the symbols used in computer flowcharts. Rectangles indicate processes or actions that the subject, law enforcement agency (or computerized system), or the judicial system takes. Diamond shapes indicate decision points, which always have two possible outcomes: yes/no or true/false. Two arrows lead outward from the diamond, corresponding to each possible outcome.

Ideally, a subject who does not commit a crime is not accused of committing one. However, due to sensor malfunction or system error, a "false positive" could occur. This could be due to an identification error, in which the suspect is confused with an innocent person, or it could be a sensor error where the person is correctly identified, but the criminal activity (or location, time, velocity, or other attribute) is in error. Errors can also result from software design that fails to effectuate the law it seeks to enforce. The possibility of design errors is addressed in Part III.

In our framework, both subject and activity errors are indicated by the "False Positive" rectangle with an arrow leading down to the "prosecute" decision diamond. In our model, if the falsely accused subject is prosecuted, he has the opportunity to contest the action. His case would be referred to the judicial system which would give him the opportunity to correct the error.

Conversely, it is possible that due to sensor malfunction or system error, a crime remains undetected. This is indicated by the "False Negative" rectangle.

Figure 1: Automated law enforcement model with interactions among the subject, the law enforcement agency, and the judicial system.


Automated Law Enforcement Process
Suspect
Law Enforcement Agency
Judicial System
Actions Prior
Subject commits actions leading up to the crime. He may receive a warning from an ALE system
Warning
Surveillance
System is monitoring subject or area
Predictive analysis
Analysis to determine if a crime is likely to occur
Prevention
Prevent a crime that analysis predicts is likely to occur
Commit Crime?
No
Yes
Crime Deterred
Subject decided not to commit crime
Crime Committed
Subject commits the crime
Post-Hoc Analysis
System analyzes data
Crime Detected?
No
False Negative
System failed to detect a valid crime
Yes
False Positive
System incorrectly determines subject committed a crime
Prosecute?
No
Discretion
System decided not to prosecute alleged perpetrator
Yes
Notification
ALE System notifies subject
Contest?
No
Accept Punishment
Yes
Adjudication
Subject may have opportunity for adjudication
Convicted?
No
Acquitted
No punishment
Yes
Punishment
Punishment administered

II. A TAXONOMY OF AUTOMATION CAPABILITIES

The use of automation is growing increasingly prevalent in our daily lives and unattended sensors are becoming ubiquitous. In the realm of law enforcement, we consider four capabilities that automation provides that make the law enforcement systems more efficient, but also can seriously degrade individual rights, such as privacy and due process. Automated law enforcement systems are capable of surveillance, analysis, aggregation, and punishment.

1. Surveillance

The first capability that automation brings is the ability to continuously surveil large areas at little cost. Automated Law Enforcement systems can take advantage of complex, networked sensor systems that may be emplaced by the law enforcement agency or by others.[19] The following are some surveillance capabilities that an automated sensor system provides law enforcement agencies. There are as many different measurements as there are types of sensors, so this section examines capabilities that have clear law-enforcement applications. As technology advances and as system developers work to expand automated law enforcement systems, this list will expand.

a. Location

Location is an important aspect for the rule of law as laws may vary widely given the myriad, and sometimes overlapping, jurisdictions of law making and enforcing entities. Automated law enforcement systems are no exception. Technology provides such systems automated and highly accurate mechanisms for determining location. Consider GPS. Providing location information is one of five capabilities provided by GPS receivers.[20] While law enforcement agencies could emplace a GPS receiver on personal property, that may not be necessary. Many people willingly

[19] *See, e.g.,* Lisa Shay, Gregory Conti, Dominic Larkin, and John Nelson, *A Framework for Analysis of Quotidian Exposure in an Instrumented World,* submitted to the Privacy Enhancing Technologies Symposium, July 2012 (under review).

[20] GPS Sensors can be used for location, navigation, tracking mapping, and timing. *See GPS Tutorial.* TRIMBLE.COM, http://www.trimble.com/gps/index.shtml (accessed 13 March 2012).

carry GPS-enabled devices with them, such as a smart phone.[21] Others have GPS-enabled devices built into their vehicles. A person carrying a GPS-enabled device or traveling in a GPS-equipped vehicle could have his or her location identified to within a few meters.[22]

Other types of sensors at a known location can also determine the location of the subject under observation. Touch sensors such as pressure plates or buttons indicate that the subject is in contact with the sensor. Smart card readers used for building, elevator, or computer access indicate the presence of the smart card and, presumably, the smart card's owner. Both buttons and smart cards require the subject's active, though perhaps unknowing (if the pressure sensor is hidden), participation in the observation.

In contrast, RFID tags can be read from a distance of a few feet to a few dozen feet and merely require the presence of a tag, not any particular action by the user.[23] An RFID sensor is an non-invasive, passive way of determining that a particularly-coded RFID tag is in the vicinity.[24] This is

[21] Mobile devices have already been shown to collect massive amounts of GPS location data without users' knowledge. *See* Brian Chen, *Apple Promises Fix for Location Gathering 'Bug' on iPhone*, WIRED GADGET LAB BLOG, (Apr. 27, 2011), http://www.wired.com/gadgetlab/2011/04/iphone-location-bug/. Governments have shown significant interest in real time tracking of its citizenry. *See* Atideb Sarkar, *Soon, the government will keep track of where every mobile user is*, INDIAN EXPRESS (Feb. 16, 2002), http://www.indianexpress.com/news/soon-govt-will-keep-track-of-where-every-mobile-user-is/912681/.

[22] The accuracy of a location reported by a GPS device (the "fix") depends on a number of factors, including the number of GPS satellites in view and the locations of those satellites relative to the GPS receiver. The accuracy of a GPS fix is quantified by a measure called "dilution of precision." For a discussion of this concept, see Richard B. Langley, *Dilution of Precision*, GPS WORLD, (May 1999), http://gauss.gge.unb.ca/papers.pdf/gpsworld.may99.pdf.

[23] *See, e.g., RFID System Components and Costs*, RFID JOURNAL http://www.rfidjournal.com/article/view/1336 Also, Texis Instruments RFID system specifications can be found at http://www.ti.com/rfid/docs/manuals/brochures/rfid_prodspec.pdf (accessed 15 March 2012).

[24] New applications for RFID tags are continually under development. For example, 20,000 students in the Brazilian City of Vitoria da Conquista's public schools were given t-shirts with embedded chips to monitor students' presence in the classroom. *See* Stan Lehman, Brazilian city uses computer chips embedded in school uniforms to keep track of students, ABC NEWS (Mar. 22, 2012),

the basis of the E-Z Pass automated toll collection system. A surveillance camera pointed in a known direction that observes a subject of interest identifies that the subject is somewhere within the field of view of the camera. Triangulation among multiple cameras can more precisely locate the subject. Alternatively, an infrared (IR) or ultrasonic sensor can determine the range to a subject.[25] If the location and direction of the IR or ultrasonic sensor are known, an algorithm can determine the subject's location.

b. Time

A commercial-grade GPS receiver unit reports the time of day accurate to one second, which is more than accurate for many law enforcement applications, such as enforcing lower speed limits in school zones during school hours. The GPS-enabled car could determine that the driver was approaching a school zone during the school day, which might trigger a more insistent warning than in a non-school area.

Some parks have curfews that are enforced at a specific time. This regulation was highlighted in the fall of 2011 during the various "Occupy" movements. In Albany, NY, protesters entered Lafayette Park after the 11PM curfew with the intent of getting arrested and generating publicity for their movement.[26] Rather than sending police to the scene, an automated law enforcement system could have erected barriers to entry at the curfew time (pre-emptive law enforcement) or photographed and ticketed the offenders after curfew (post-hoc enforcement). A police dispatch could have been saved for more serious infractions, such as protesters causing damage.

However, the GPS system is capable of producing a time signal that is much more accurate than a standard clock. For example, the Trimble

http://abcnews.go.com/International/wireStory/computer-chips-track-students-brazil-15979607#.T3YP2WEgfA0.

[25] An ultrasonic sensor available from a popular robotics equipment vendor, Parallax, has a range of 3m and sells for $30. For $11 the same company sells an infrared range finder that measures distances from 10 to 80cm. *See* PARALLAX.COM (accessed 14 March 2012).

[26] Dayelin Roman & Jennifer Gish, *24 Arrested at Occupy Albany: Demonstrators Taken Away After Curfew by State Troopers at Occupy Albany Site*, ALBANY TIMES-UNION (Nov. 13, 2011), http://www.timesunion.com/local/article/24-arrested-at-Occupy-Albany-2265945.php.

"Mini-T GPS Disciplined Clock Board" is a 1" x 5" electronic circuit board that produces a clock signal accurate to 15 nanoseconds.[27] (A nanosecond is one-billionth of a second.) While the law enforcement community has yet to exploit this feature, since traditional laws were written before these highly-precise time standards were commonly available, algorithmic law enforcement systems could exploit this technology. However, not all automated systems can guarantee such a high degree of accuracy and clock synchronization remains a challenging problem.[28] A lack of synchronization could cause False Positive or False Negative errors discussed in the previous section.

c. Tracking

Recording a series of locations at intervals in time produces a track or path the object traversed. Law enforcement can apply tracking to suspected criminals or their vehicles to determine locations of drug transfer points, warehouses used to store drugs or other contraband, border crossing sites used for human or object trafficking, or a myriad other applications. GPS receivers are designed to produce this data, but a track can also be inferred by combining time-stamped data from multiple sensors. For instance, the "E-Z Pass" automatic toll collection system automatically records the time and date participating vehicles enter and leave highways or cross bridges.[29] If a suspect's vehicle has an E-Z Pass transponder, the E-Z Pass database could be queried to determine every toll road and bridge the suspect traveled on in any given time period. Even vehicles without E-Z Pass have the potential to be tracked. Traffic cameras routinely monitor highways in and around major cities.[30]

Although the current resolution of most general-purpose traffic cameras is insufficient to read license plates, the color and type of vehicle

[27] *See* Mini-T GPS Disciplined Clock Board Data Sheet, TRIMBLE.COM (accessed 12 March 2012).

[28] *See* Julien Ridoux & Darryl Veitch. *Principles of Robust Timing Over the Internet*, 53 COMMUNICATIONS OF THE ACM 54-61.

[29] Features of the E-Z Pass system are explained at https://www.e-zpassny.com (accessed 14 March 2012).

[30] Atlanta makes traffic cameras publicly available on the world-wide web: http://www.511ga.org/traffic/cam.php (accessed 14 March 2012). The "TrafficLand" service allows web access to 10,000 cameras in over 200 cities in the U.S., plus cities in Australia, Canada, Denmark, New Zealand and the UK.

(sedan, pickup truck, van, etc) are identifiable. Computer algorithms could be used to scan thousands of photos of likely intersections or roads looking for "a red pickup truck."

The recent Supreme Court decision *United States v. Jones* determined that the installation of a GPS device on a suspect's vehicle was a "search" for Fourth Amendment purposes.[31] However, the case leaves open how to treat data from GPS receivers already in a suspect's possession or data from other systems already in place such as E-Z Pass or traffic cameras.

d. Velocity

Like tracking, velocity is an attribute that can be derived by measuring successive locations at known time intervals. It can also be measured directly, such as by a vehicle's speedometer or radar. Vehicular velocity, combined with location, can be used to determine if speeding laws have been violated. Radar systems currently determine vehicular speed and can be connected to systems that automatically send tickets to the owner identified from the photograph of the license plate. This process could be even more automated. A database could be developed that listed the posted speed limit for each section of every road. A car's onboard computer tracks the car's velocity and many have GPS sensors. If the car's onboard computer has access to the database of speed limits, it could determine that the driver was violating the law and either warn the driver, alert the police, or both.

e. Identification

A key objective of automated law enforcement systems is the ability to identify the subject or subjects who may be breaking, or about to break, the law. Modern technology often makes this process relatively straight forward. Automated law enforcement systems that are connected to large databases of identity information and sensor data can run algorithms to determine the identity of the subject with some degree of accuracy.

[31] United States v. Jones. 565 U.S (Slip Opinion) (2012) http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.

Depending on the type of information collected, the reliability of the identification could be very good or very poor.[32] The specific performance depends on the underlying technology. Some systems, particularly digital systems, are specifically designed for accurate automated identification. As examples, RFID tags and bar codes are designed to be read with high accuracy over short distances with little error. Both RFID tags and bar codes are very flexible and low cost technologies that may be used to identify physical objects and living things, including people, as long as the mapping of RFID tag number to the individual's identity is accurate.

Software constructs, such as web browsing software, may also be uniquely identified, as in the case of cookies issued by websites to web browsers to uniquely identify a given browser or the use of cryptographic hashing algorithms to uniquely identify computer programs and data files.[33] In some cases, systems cannot uniquely determine an individual or object, but may be able to partially identify them[34] and determine a number of potential identities.

The computer security access control literature provides a useful model for identification, which considers some combination of something you know (such as a password), something you have (such as a physical token like a key or ATM card), and something you are (such as a given subject's facial characteristics or fingerprint).[35] Single factor authentication that considers one category is often employed, but multi-factor authentication which considers two or more categories is considered significantly stronger. We see each of these categories, particularly something you

[32] Biometric systems which measure attributes of individuals, including facial features, fingerprints, gait, and hand geometry, and compare these measurements against databases of enrolled individuals have widely varying accuracy which may be very accurate under controlled conditions and highly inaccurate in practice due to environmental noise, injury or stress. *See* BIOMETRICS.GOV http://www.biometrics.gov/NSTC/Publications.aspx, for detailed specifics.

[33] Communities of malicious software researchers often band together and create registries of such hashes as a means to determine if a given malicious software sample is new or has been already discovered. *See* TEAM-CYMRU.ORG, http://www.team-cymru.org/Services/MHR/ and MALWAREHASH.COM, http://www.malwarehash.com/ for two examples of such registries.

[34] One such technique is web user profiling which seeks to observe user behavior and serve targeted advertising. *See* PHORM.COM, http://www.phorm.com/.

[35] SHON HARRIS. ALL IN ONE CISSP (2011) (describing numerous well established access control and identity management frameworks).

have (e.g. a smart-card, license plate, etc.) and something you are (e.g. biometrics) as identification strategies relevant to automated law enforcement.

Identification of physical or software objects may be loosely or tightly coupled with actual human suspects. For example, a license plate reader may accurately identify a license plate, which, if it has not been switched, leads to the specific car. Through a database lookup of motor vehicle records, the owner of the car may be determined. The specific driver at a given time is only loosely coupled given this process, but may be assumed to be the owner or relative. The linkage to the correct driver is strengthened if supported by other evidence such as a photograph of the driver taken at the same time as the license plate reading.

In the case of red light cameras, many courts have determined that only the vehicle need be identified in order to issue a citation to the owner, with lesser concern to identify the driver, who does not receive a citation. However, we note that many such systems take photographs of drivers at the time of the offense, as additional supporting evidence.

There are numerous risks associated with identity systems that are extremely relevant to automated law enforcement systems. Systems may incorrectly identify a suspect, leading to Figure 1's "False Positive" error based on mis-identification. If the identified individual actually committed the offense, he or she may escape punishment personally, but deliberately or unintentionally frame another individual in the process. Moreover, if an innocent subject is incorrectly identified as someone with a criminal record or as a terrorist they may receive harsher handling and punishment during the law enforcement process. There are multiple instances of law abiding citizens being detained at airports and border crossing check points due to similar individuals being on a watch list.[36] Both cases are undesirable, as an innocent is detained and possibly

[36] *See* Drew Griffin & Kathleen Johnston, *Airline captain, lawyer, child on terror 'watch list'*, CNN.com (Aug. 19, 2008), http://articles.cnn.com/2008-08-19/us/tsa.watch.list_1_terror-watch-list-airline-pilot-terrorist-screening-database?_s=PM:US; Thomas C. Green, *Database snafu puts US Senator on terror watch list*, THE REGISTER (Aug. 19, 2004), http://www.theregister.co.uk/2004/08/19/senator_on_terror_watch/. Such newsworthy, high-profile false positives are likely just the tip of the iceberg when considering far less empowered average citizens.

punished without cause, while a truly dangerous person is allowed to roam freely.

Subjects may also take measures designed to increase the likelihood of errors, especially sensor errors that prevent the automated system from detecting their crime (the "False Negative" situation in Figure 1). For example, users may employ license plate covers designed to prevent photography, or use special wallets or clothing to block the transmission of RFID signals. The use of many defensive strategies frustrates automated law enforcement systems, but may be employed for entirely legitimate purposes such as protecting against identity theft.[37]

Subjects may also take measures that actively seek to spoof, or steal, the identity of another or to create a false identity. A simple example is that of simply swapping license plates, but high tech sniffing and cloning of identity information, often at a distance and without the target's knowledge, is frequently possible.[38] Some technologies designed for one task, such as inventory management[39] or tire pressure monitoring[40] may also be re-purposed[41] by automated law enforcement systems to assist in

[37] An excellent example of a legitimate technology to protect against identity theft are wallets designed to block sniffing of RFID enabled passports. *See* *RFID Blocking Passport Billfold*, THINKGEEK, http://www.thinkgeek.com/gadgets/security/910f/ (last accessed March 30, 2012).

[38] *See* Melanie Rieback, *A Hacker's Guide to RFID Spoofing and Jamming*, DEFCON 14, 2006; Kim Zetter, *Feds at DefCon Alarmed After RFIDs Scanned*, WIRED THREAT LEVEL BLOG (Aug. 4, 2009), http://www.wired.com/threatlevel/2009/08/fed-rfid/.

[39] The use of RFID tags by manufactures and retailers to uniquely identify stock is a common practice. *See* Miguel Bustillo, *Wal-Mart Radio Tags to Track Clothing*, WALL STREET JOURNAL (July 23, 2010) as a representative example. Significant privacy concerns arise if the tag is not disabled or removed after purchase. Due to the small size of the RFID tag the purchaser may be unaware of the existence of the tag.

[40] Tire pressure monitoring systems are now mandatory for new passenger cars in the United States. *See* U.S. Department of Transportation's Federal Motor Vehicle Safety Standard (FMVSS) No. 138, http://www.nhtsa.gov/cars/rules/rulings/TPMS-FMVSS-No138-2005/part1.html Tire pressure monitoring systems contain numeric identifiers ranging from 2^{32} to 2^{128} bits, allowing for unique identification of every tire on the planet. Because tire pressure monitoring systems operate wirelessly these unique identifiers may be intercepted from a distance by law enforcement or government entities and spoofed by attackers. See Mike Metzger, *Letting the Air Out of Tire Pressure Monitoring Systems*, DEFCON 18, 2010.

[41] Such re-purposing may require minor modifications to the underlying technology. An excellent example was the addition of unique microdot patterns to the output of many

identifying suspects.[42] In other areas we see technologies being developed to integrate analog-based identification systems, such as license plates, into automated law enforcement processes, such as automated license plate readers, speeding up processing.

However, the conversion between analog data and digital identity can be error prone, which has spurred the development of entirely digital systems, such as electronic license plates[43] and RFID-enabled passports that eliminate the need for analog to digital conversion. However, in both co-opted analog or entirely digital technology, enhanced mass identification of individuals[44] and objects[45] is becoming increasingly realistic and should be assumed to be a capability of automated law enforcement systems in the near future.

modern computer printers, in an alleged attempt to frustrate counterfeiters. *See Is Your Printer Spying on You*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/issues/printers (last accessed Mar. 24, 2012).

[42] There is a growing appreciation for building privacy into the design of technologies which will likely be in tension with automated law enforcement advocates seeking increased ways to accurately find and identify law breakers. *See* Kashmir Hill, *Why 'Privacy By Design' Is The New Corporate Hotness*, Forbes (July 28, 2011). Such design considerations include minimizing data collection and retention, avoiding unique identifiers, and frustrating data utilization by unauthorized third parties. *See* Adam Barth, *HTTP State Management Mechanism*, Request for COMMENTS 6265, Internet Engineering Task Force, 2011.

[43] See U.S. Patent 6404327, "Electronic License Plate," for one such example.

[44] Augmented reality systems overlay digital data onto the physical world using technologies such as search engines and smart phones. Such advances will likely be incorporated into fully automated and human-machine hybrid law enforcement regimes of the future. *See* Paul Marks, *Augmented reality iPhone helps police track suspects*, NEW SCIENTIST (Feb. 21, 2011); Google Googles, www.google.com/mobile/goggles. Crowdsourcing is another means of identifying large numbers of people, *See Using Crowdsourcing To Identify Vancouver Rioters*, SLASHDOT (June 26, 2011), http://yro.slashdot.org/story/11/06/16/2327228/using-crowdsourcing-to-identify-vancouver-rioters. In general, there is much research and development seeking to identify individuals from a photograph or single video frame. *See* Rob Waugh, *Big Brother just got scarier: Japanese CCTV camera can scan 36 million faces per second - and recognise anyone who has walked into its gaze*, MAIL ONLINE (Mar. 23, 2012), http://www.dailymail.co.uk/sciencetech/article-2119386/Could-governments-recognise-ANYONE-instantly-CCTV-Japanese-camera-scan-36-million-faces-second.html.

[45] One such system is Cordon which can simultaneously identify and follow up to 32 vehicles at one time across four lanes of traffic. *See* Amar Toor, *Cordon multi-target photo-radar system leaves no car untagged*, ENGADGET, (Oct. 31, 2011).

Effective automated law enforcement systems will depend upon accurate and high speed sensor system performance. The future portends the ability to perform mass identification of suspects and average citizens, enhanced by technology.[46] However, inaccurate identification either through failings in technology,[47] countermeasures employed by subjects, or identity theft, remains a significant disadvantage. Every such error targets an innocent person, leading to significant burdens on the court and administrative appeals processes. At the extreme, it might seem a compelling idea to uniquely identify every man, women, and child using digital identity systems, perhaps through the use of DNA or biometrics registries or national identification cards[48] to reduce errors by law enforcement systems, but we believe such sweeping regimes will bring significant personal and societal risks.

2. Analysis

A key characteristic of automated law enforcement systems is their ability to process and analyze information at speeds far beyond human capabilities. Where a single police officer may take 15-30 minutes for a simple engagement, such as a traffic stop, automated systems can monitor many subjects in parallel and make decisions in milliseconds.[49] Today's enforcement systems are relatively simple, performing basic identification tasks, such as license plate recognition, accurate measurement of some physical characteristics, such as location or velocity, and performing crosschecking against databases, such as motor vehicle registration

[46] Consider the many ways technology users disclose information to third-parties. For example, Google Voice, https://www.google.com/voice/, and Apple’s Siri, http://www.apple.com/iphone/features/siri.html, collect voice samples of users on a global scale and combine it with identity information such as phone numbers and user accounts.

[47] We note that purveyors of identification systems are likely not incentivized to acknowledge shortcomings of their technologies, but instead will highlight optimistic levels of performance, enhanced by marketing puffery.

[48] *See, e.g., A Time Bomb For Civil Liberties*’*: France Adopts a New Biometric ID Card*, ELECTRONIC FRONTIER FOUNDATION, (Mar. 8, 2012), https://www.eff.org/deeplinks/2012/03/french-national-assembly-proposes-new-alarming-biometrics-bill; *India to Compile ‘World’s Biggest ID Database*, BBC NEWS SOUTH ASIA (Sept. 29, 2012), http://www.bbc.co.uk/news/world-south-asia-11433541.

[49] *See, e.g.,* Ping Jian, et. al., *A Mosaic of Eyes,* 18 ROBOTICS & AUTOMATION MAGAZINE, IEEE 104 (2011).

lookups.[50] However, advances in sensing technologies, high speed processors, and networking combined with emerging artificial intelligence, data mining, and facial and voice recognition advances portend a future when subjects may be targeted, judged, and punished by automated systems for a broad and ever-increasing range of offenses, at an ever-decreasing transaction time and with potentially no human intervention.[51]

3. *Aggregation*

Automated law enforcement systems are not constrained to a single flow of sensor data. In many cases, isolated flows of data are insufficient to determine if an offense has been committed and by whom.[52] Automated systems can easily aggregate data from multiple sensors and sensor systems to create a more comprehensive view of a subject's activities.[53] Importantly, such data aggregation may combine data collected over long time periods from diverse and geographically disparate sources, including information from existing licensing, registration, law enforcement, and other governmental and commercial databases.[54] Even if an individual consented to having some data collected in exchange for a desired benefit (such as ease in traversing bridges and toll roads), the data could be kept for years, resold to another organization, and used for an entirely different purpose. It is possible that these follow-on transactions will occur without the knowledge or consent of the individual.

[50] *See, e.g.*, Jenna Ray Glasson, Note, *Technology Outpacing Due Process: Analysis of Kentucky's Financial Institution Data-Match Program and a Proposed Solution*, 48 U. Louisville L. Rev. 399 (2009); Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 17 (2005)..

[51] *See, e.g.*, Elizabeth Joh, *Discretionless Policing: Technology and the Fourth Amendment*, 95 CAL. L. REV. 199, 203-04 (2007); Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008); Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2011); Mathew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581 (2011).

[52] *U.S. Still Mining Terror Data*, WIRED.COM (Feb. 24, 2004), http://www.wired.com/politics/law/news/2004/02/62390 .

[53] *See, e.g.*, GREG CONTI. SECURITY DATA VISUALIZATION (2001).

[54] *See* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2011).

4. Punishment

The ability to punish perceived offenders distinguishes an automated law enforcement system from a surveillance system. Depending on societal norms and legal guidelines, governments empower their law enforcement agents and judicial systems to examine evidence, judge whether an offense occurred, and mete out appropriate punishments. The same holds true for automated law enforcement systems. Some punishments are currently in use by automated systems, others are within the current capability of today's systems, and additional capabilities will soon be available given reasonable assumptions about technological development, as shown in Figure 2 below.

Figure 2 depicts a range of punishments from least severe (green) to most severe (red). The rows indicate maturity and use of technology from technologies currently in use (top row) to capabilities that could be developed using current technology (middle row) to capabilities that could be developed in the near future (bottom row). The entries are only exemplars-for some cells there are many more entries than there was room to list. The check marks simply indicate that the entry in the previous row is still valid.

Figure 2: Spectrum of Punishments available in an Automated Law Enforcement System

	Notice	Warning	Embarrassment	Citation/Points	Arrest	Prosecution	Confinement	Execution
	7	6	5	4	3	2	1	0
Currently Implemented	Signs & websites warning about sensors	"Flash" when camera activates at speed trap or intersection	Listing on a website or database	Red Light Cameras, Radar speed traps			Ankle bracelets for house arrest	
Current Capability not yet Implemented	✓	✓	✓	✓			✓	Lethally-armed robots
Future Capability	✓	✓	✓	✓	Robots could disable and drag crime suspects	?	More sophisticated location control-better enforcement of restraining orders, for instance	More advanced lethally-armed robots that might even be autonomous

III. QUESTIONS NECESSARY TO CONFRONT AUTOMATED LAW ENFORCEMENT

Given that automated law enforcement has the potential to reduce manpower costs, increase revenue, and reduce human bias, what limits or constraints should be emplaced to protect the rights of ordinary citizens? This section relies on theoretical and empirical research in presenting several topics that should be addressed before any systems are implemented. Each of these topics must also consider whether the automated law enforcement systems comply with constitutional, statutory, administrative, and common law schemes such as the Fourth Amendment and crimes with a *mens rea* requirement.[55]

Indeed, the most basic or introductory question might be whether the law to be enforced is suitable for automation.[56] Crimes with scienter requirements are unlikely candidates for full automation given the heavy adjudicatory requirements typically required to legally determine an individual's state of mind. However, many other aspects of the crimes, such as surveillance and aggregation of the requisite activity, could still be automated.

1. *Method of Implementation*

Automated law enforcement systems might cause problems for the various parties involved if they are implemented too quickly or incorrectly. In some cases, individuals are compelled to use particular technologies such as GPS in cell phones or taxi cabs. Should governments mandate these technologies in a way similar to the "V-Chip?"[57] Or should they adopt the approach of many insurance companies and incentivize the adoption of automated law enforcement technologies?[58]

[55] *See, e.g.*, Jeffery A. Parness, *Beyond Red Light Enforcement Against the Guilty But Innocent: Local Regulations of Secondary Culprits*, 47 WILLAMETTE L. REV. 259 (2011). A full exploration of the potential legality of automated law enforcement schemes is beyond the scope of this article.

[56] Mulligan, *supra* note 6, at 5.

[57] *See, e.g.*, *V-Chip: Viewing Television Responsibly*, FEDERAL COMMUNICATIONS COMMISSION, http://transition.fcc.gov/vchip/ (last visited Jan. 7, 2012).

[58] *See, e.g.*, Karen Aho. *Will your car rat you out?*, MSN MONEY (Feb. 8, 2008), http://articles.moneycentral.msn.com/Insurance/InsureYourCar/WillYourCarRatYouOut.aspx.

Should governments use their own technology or simply commandeer existing technologies such as GPS devices?[59] Should an automated law enforcement system be used if less than a certain percentage of potential violators have adopted the necessary technology? How much testing should be required before implementation? The ultimate legality of automated law enforcement could hinge on of some of these highly factually specific determinations.

2. Control

Those who control automated law enforcement systems wield great power over the populace, even over those accustomed to privileged treatment.[60] Every automated law enforcement system will require many different individuals or organizations to design, implement, install, maintain, finance, operate, and audit it. We consider each of these entities to be an actor who has some control over how well the system ultimately works. In our framework, implementation translates a conceptual design into a collection of sensors and other hardware which are connected to computers (often via a data network) and the software that runs algorithms to determine if a crime has been or is about to be committed.

Many of the potential controllers will not be a part of the government. Rather, government contractors are likely to have a significant influence over the design, implementation, installation, maintenance and even use of automated law enforcement systems. To what extent should these contractors or ministerial government workers be allowed to control the system? What agency verifies that the system that is built accurately represents the system that was intended? If a computer program falsely

[59] This is also an issue of control. See Part III, 2, *infra*.

[60] We note that some law enforcement officers, who are often given informal warnings by their fellow police officers for traffic infractions as a professional courtesy instead of more severe punishments, are challenged by their loss of control to automated law enforcement systems. The Washington Post reported on police officers photographed making obscene gestures at speed cameras and that some police unions may be advising officers to not pay fines, because the owner of the vehicle, in this case the county government, is responsible, not the driver. *See* Ernesto Londono, *Montgomery's Finest Won't Pay Fines*, THE WASHINGTON POST (Mar. 8, 2008), http://www.washingtonpost.com/wp-dyn/content/article/2008/03/07/AR2008030703484.html. Some elected government officials might receive similar treatment and may be similarly challenged by automated law enforcement.

accuses an innocent person, who is at fault? The system owner? The installer? The programmer? Or the legislature that drafted and effectuated a law that cannot be adequately automated (as discussed in the introduction to this section)?

Additionally, the proliferation of surveillance devices in the private sector could render some government surveillance redundant. For example, from an efficiency and technological standpoint, the government would be duplicating efforts by installing a GPS device on cars that already utilize a commercial GPS service such as OnStar. The market for private drones appears to be rapidly increasing in light of a burgeoning framework which provides for their use.[61] Most smartphones are equipped with GPS technology and according to a recent statistic, 46% (and counting) of all mobile phone users in the US have smart phones.[62]

To what extent should governments leverage the adoption of these technologies for use in an automated law enforcement systems? Procedural safeguards and rights violations aside,[63] use of these systems might seem more efficient and could arguably lower the cost of automation by using already implemented technologies the government does not have to fund. Yet use of third-parties to aid in the collection and storage of information also cedes some or all control of this activity. To what extent is this cessation of control appropriate?

3. *Discretion*

The issue of how much human discretion to build into an automated law enforcement system may be one of the most difficult to resolve. Elizabeth Joh identified as the central dilemma of discretionless policing the predicament that “we cannot expect the police to fully enforce the law everywhere, yet their freedom to make choices in enforcing the law can

[61] *See, e.g.*, M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, http://www.stanfordlawreview.org/online/drone-privacy-catalyst; Kashmir Hill, *Would You Buy a Drone to Walk Your Child to School*?, FORBES, http://www.forbes.com/sites/kashmirhill/2012/03/20/would-you-buy-a-drone-to-walk-your-child-to-school/.

[62] *More US Consumers Choosing Smartphones as Apple Closes the Gap on Android*, NIELSEN WIRE (Jan. 18, 2012), http://blog.nielsen.com/nielsenwire/consumer/more-us-consumers-choosing-smartphones-as-apple-closes-the-gap-on-android.

[63] These concerns are addressed *infra,* Part III, 9.

have harmful effects because enforcement may be discriminatory and arbitrary."[64] In this way, the elimination of human discretion can be seen as a positive for automated law enforcement schemes.

Yet discretion also allows humans to overlook the letter of the law in favor of fairness, extenuating circumstances, or simply the "spirit of the law."[65] Additionally, police discretion at the local level allows departments to choose some "priorities of enforcement" over others. Joh stated, "These choices reflect social and political choices that prevent a police organization from 'full enforcement:' enforcing the law every time a violation is observed."[66] For example, the prosecution for the theft of a low-value item such as an iPod might not warrant the same zeal for enforcement as more serious violent crimes. For these and other reasons, courts and legislators have been reluctant to curb police discretion.[67] The implementation of an automated law enforcement system may force their hand.

4. *Perfection of Enforcement*

The consideration of the perfection of enforcement is related to the issue of discretion, but directly asks "How many violations of the law should be explicitly forgiven or ignored?" Where discretion focuses on the preservation or elimination of individual contextual judgment, the perfection of enforcement question requires system-level determinations of when to ignore legal violations. Should any or all laws be perfectly enforced? If not, what is the proper "tolerance" for the system? Defining these criteria will ultimately reflect difficult policy decisions and can be fraught with bias or unintended consequences.

For example, in any given trip in a car, a motorist might violate the speed limit at numerous points. Should the motorist be given a ticket for

[64] *See, e.g.,* Elizabeth Joh, *Discretionless Policing: Technology and the Fourth Amendment,* 95 CAL. L. REV. 199, 203-04 (2007).

[65] *See, e.g.,* Lior Jacob Strahilevitz, *"How's My Driving?" For Everyone (and Everything),* 81 N.Y.U. L. REV. 1699 (2006) (noting the advantages of a system for traffic regulation where "existing laws and rules are modified by social expectations and aspirations to form a body of law that is used to reward the cooperators and punish the deviants.").

[66] Joh, *supra* note 18, at 207.

[67] *See, e.g,.,* Joh, *supra* note 18, at 202.

every violation, or just once per trip or per speeding "zone"? Should trespassers be punished only upon their initial unauthorized entry, or should they continue to receive graduated punishments based upon how long they remain trespassers?[68] If the trespasser exits the property and then re-enters, should the graduated punishment reset, or should punishment resume at the level where it left off?[69] If merely briefly touching private property without authorization is forgiven, how much time must elapse or what activity must occur before the briefly encroaching individual is deemed to have "trespassed"? If a subject violates the law unintentionally, because her own sensor malfunctions (such as the speedometer in the car or her own GPS incorrectly reports her location), or because the sensor is simply not accurately calibrated, should there be a mechanism to reconcile this problem?

This factor also includes the question of to what tolerance must personal sensors be calibrated and display their data? If an individual's car only displays the speed to the nearest mile per hour and the individual is traveling 55.01 miles per hour it will likely display 55mph. The individual's impression is that she is abiding by the law, but if she is in a 55mph zone, she is technically speeding.

5. *Legal Integration of Algorithms*

Computer code is at the heart of automated law enforcement systems. This code may be implemented in an attempt to capture the purpose and intent, perhaps exactly as written, of a law or laws. However, the law is rarely written with such algorithmic precision in mind. Therefore those who specify and implement the code base of a system will likely make their own interpretations of legal and illegal behavior, perhaps without any legal training.

Many questions arise when implementing automated law enforcement systems. Consider the following hypothetical that builds upon the previous consideration regarding the perfection of enforcement. David is driving his car across rolling terrain. He sets his cruise control at the

[68] See the punishment scale *supra* Part II, 4. An initial response could be a notice, then a warning, then a small citation, then a fine.

[69] In other words, if the trespasser exists the property after the punishment has risen to a "fine," should the response for re-entering the property be another fine or merely a warning?

speed limit, but the steep hills cause his vehicle to alternate between a few miles per hour below the speed limit when going uphill and perhaps as many as five or more miles per hour above the speed limit going downhill. Over the course of 30 minutes of this behavior, he has technically exceeded the speed limit many times, sometimes for just a few seconds and sometimes for a minute or more. An example of this type of speed variation is shown in Figure 3.

Given that technology allows recording and communication of this data, should David be issued a dozen citations? If not, what is the minimum duration above the speed limit that constitutes an offense? What is the minimum duration required between periods where he exceeded the speed limit to constitute two distinct infractions? Is travelling 0.001 MPH above the speed limit a violation of the law? What if the accuracy of his car's speedometer is +/- 3 MPH, should this limitation of the sensor be factored into the determination? Should there be a grace period in terms of offense duration, inter-offense time, or even an allowance for travel above the speed limit without triggering the system?

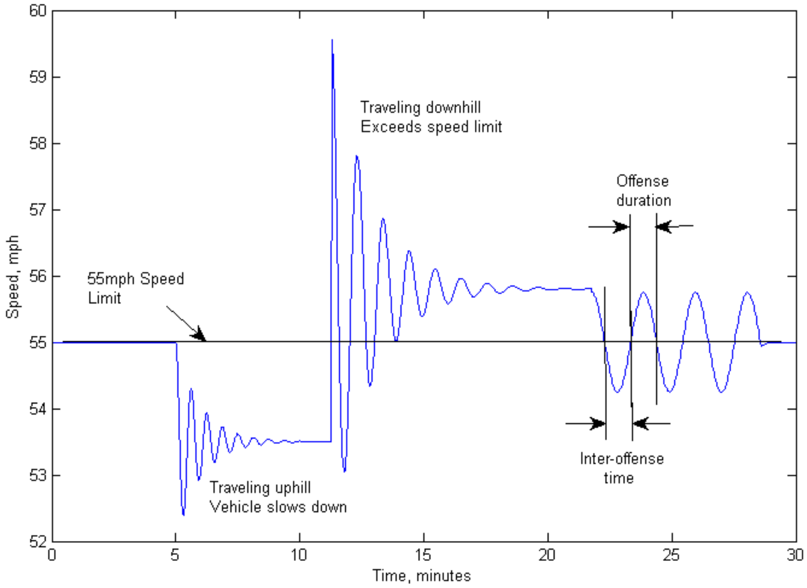
The law isn't written with these distinctions in mind, leaving programmers and systems designers to make their own assumptions in the form of code and algorithms. In the analog world of manual law enforcement, David might be pulled over once during his drive. Even this is unlikely since, with his cruise control set at the speed limit, he is traveling at the prevailing traffic speed (if not slower). Police would likely be concerned with those travelling above the prevailing traffic speeds and driving aggressively.

However, in the world of scalable, accurate, and persistent automated law enforcement David could, technically, receive a dozen citations, lose his license, and become uninsurable, all despite a good faith effort to obey the speed limit. Without proper restraint, automated law enforcement systems risk creating an environment where it is all but impossible[70] to follow the law without massive changes to a society's culture and norms. Might algorithms, which are increasingly employed to predict and

[70] Some drivers with sensory or physical limitations, such as the elderly, may find it essentially impossible to follow the law when driving despite all their best attempts, if automated law enforcement systems strictly enforce today's traffic laws as written.

regulate behavior, be used to ease the tension caused by perfect enforcement?

Figure 3: Illustration of possible variation vehicle speed during a 30-minute trip



Automated law enforcement systems can accommodate various algorithms, allowing for personalization of the law or punishment only above some algorithmically determined threshold. For example, systems could be designed such that if a driver has only one speeding infraction, he or she is allowed to slightly exceed the speed limit more than those who have a history of speeding infractions, traffic violations, or DUIs. Speeding limits could become dynamic and fluctuate based on the amount and speed of traffic or other risk factors.

Of course, the law is typically generalized and most algorithms require extreme precision. This dissonance might be hazardous when automated system vendors and coders are asked to make assumptions about the law, which would become embedded in the system hardware and software.[71]

[71] *See, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

Yet as algorithms become more accurate at predicting behavior, [72] law enforcement officials might find it increasingly difficult to justify ignoring an algorithm's recommendation in favor of human discretion.

6. *Preemptive/Post Hoc Enforcement*

Should automated law enforcement systems prevent crimes or simply enforce them post-violation? Given certain correlations between risky behavior and crimes, should systems police only illegal behavior or respond to behavior likely to lead to a crime? In some respect, the perfect prevention of crimes via an automated system might be seen as merely an extension of architecture to encourage or prevent behavior. For example, speed bumps and fences are attempts to preempt speeding and trespass. Perhaps the same could be said for an automatic inhibitor in vehicles preventing the driver from exceeding the speed limit on any given road.

Yet, in many ways automated systems as preemptive enforcers are different than fences and speed bumps. They ruthlessly efficient—in a word, perfect. Those wishing to speed over speed bumps may do so, perhaps sustaining great damage to his or her car. Yet that is a consequence of an action they freely chose. Those wishing to climb a fence (or destroy it), also, in theory, have that option. Automated systems likely will not offer the same flexibility. To what extent should this perfection affect the decision to preemptively enforce the law?

As driverless cars are introduced to the roads, should the law require them to ignore instructions to engage in any number of activities that could potentially violate the law, such as speeding, reckless driving, illegal parking, and trespassing? Given the possibility of "preemption" or "perfect prevention," government officials might find it hard to resist preventing crimes from occurring. Yet perfect prevention might violate numerous procedural safeguards for due process, inhibit necessary violations of the law to avoid more serious hardship as well as infringe upon individual autonomy and have a disruptive social cost, all of which are explored below.

[72] *See, e.g.*, Amazon was granted a patent that tracks users through their mobile devices and predicts where they are likely to go next Erik Sherman, *Amazon Big Brother patent knows where you'll go*, CBS MONEY WATCH (Dec. 14, 2011), http://www.cbsnews.com/8301-505124_162-57342567/amazon-big-brother-patent-knows-where-youll-go/.

7. System Error/Malfunction

No automated system is flawless.[73] Any automated law enforcement system must determine how much system error can be tolerated. It also must protect against inevitable system malfunctions and remain secure against unauthorized parties. Automated Law Enforcement errors can occur at the system or component level. At the system level, it is useful to consider four cases drawn from the computer security community's intrusion detection literature:[74]

- True Positive - The automated law enforcement system correctly identifies and acts upon a crime
- True Negative - The system correctly ignores offenses not within its purview.
- False Positive - The system incorrectly identifies and acts upon a crime.
- False Negative - The system fails to identify and act upon a crime within its purview.

The automated law enforcement system may function properly by correctly identifying offenses within its design parameters (True Positive) and correctly ignore other activity that does not constitute an offense (True Negative). However, the system may also incorrectly identify non-offenses as offenses (False Positive) or incorrectly ignore actual offenses (False Negatives). All four cases are captured in the model shown in Figure 1. A well designed automated law enforcement system will seek to maximize True Positives and True Negatives and minimize False Positives and False Negatives.

[73] Numerous examples abound which illustrate that even the most carefully designed automated systems may be flawed, such as NASA's Mars Climate Orbiter which crashed into Mars because of a mismatch between metric and English units. *See, e.g.,* Peter Neumann, *Illustrative Risks to the Public in the Use of Computer Systems and Related Technology*," STANFORD RESEARCH INSTITUTE (Oct. 2, 2001); Karen Aho. *Will your car rat you out?*, MSN MONEY (Feb. 8, 2008), http://articles.moneycentral.msn.com/Insurance/InsureYourCar/WillYourCarRatYouOut.aspx.

[74] Stegan Axelsson. *The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection*. RECENT ADVANCES IN INTRUSION DETECTION (RAID) (1999).

Error rates are extremely important. Even a relatively low False Positive rate on an active system could quickly overwhelm the administrative and court process for appealing a conviction. Consider that there are approximately 313 million people in the United States today.[75] Although the United States has more people in prison than any other country, only 2.3 million people in the United States are incarcerated.[76] If every person in the United States was under some sort of surveillance once per year, even a 0.7% False Positive rate would create as many false cases in one year as there inmates in the entire prison system.

A high False Negative rate threatens the actual and perceived value of the system.[77] However, in the context of automated law enforcement systems given the possibility of convicting innocents (False Positives) or ignoring actual offenses (False Negatives), is a design trade-off that may be faced by those seeking to tune an automated law enforcement system. We argue that the importance of minimizing False Positives outweighs the importance of minimizing False Negatives. For future work we recommend exploring the use of Receiver Operating Characteristic (ROC) curves, which graphically plot the True Positive rate against the False Positive rate, as a useful tool for those seeking to analyze the effectiveness of automated law enforcement systems.[78]

Errors may also occur at the individual component level. For example, spurious noise could cause errors in networked communications and sensors. In the case of digital networked communications, engineers have developed robust error correcting algorithms and protocols which identify and repair errors.[79] The same cannot be said for electronic components in

[75] U.S. Census Bureau http://www.census.gov/population/www/popclockus.html (accessed Mar. 27, 2012).

[76] The Sentencing Project News – Incarceration http://www.sentencingproject.org/template/page.cfm?id=107 (accessed Mar. 27, 2012)

[77] A good example of the False Negatives undermining the perceived value of a security system is that of current United States Transportation Security Agency's airport security program, criticized by some security experts as "Security Theater." *See* BRUCE SCHNEIER. "BEYOND FEAR: THINKING SENSIBLY ABOUT SECURITY IN AN UNCERTAIN WORLD(2003).

[78] *See* Tom Fawcett, *ROC Graphs: Notes and Practical Considerations for Researchers*, 27 PATTERN RECOGNITION LETTERS 882 (2004).

[79] *See* JAMES KUROSE & KEITH ROSS. COMPUTER NETWORKING: A TOP-DOWN APPROACH FEATURING THE INTERNET (2001) (describing numerous examples of error identification and correction techniques.)

general, and sensors in particular.[80] Each sensor has limitations in terms of accuracy that, by definition, induce some degree of error into a system. For example, the LeadTek LR9805ST GPS Module measures position to 10 meters, velocity to 0.1 meters/second, and time to 1 microsecond.[81]

Note that many errors only represent a single point of error in a long chain of potential errors. For example, the GPS module's stated accuracy of 1 microsecond is actually dependent upon the accuracy of the time provided by the GPS satellite, which in turn, has accuracy limitations of its own. The overall effect is cumulative. While this example may seem inconsequential, errors, sampling rate,[82] calibration dates, approved calibration labs, and system and component accuracy may play a significant role in the courtroom, particularly when the defendant may present evidence from one sensor system against the evidence generated by sensors in an automated law enforcement system, and the outcome may hinge on the relative accuracy of each system.[83] In our likely future of automated law enforcement we anticipate increasing defensive use of competing sensor systems by defendants, not just as a tool to identify law enforcement sensors as in the case of a radar detector, but instead as a reliable source of contradictory evidence for use as a defense.

[80] For an example of a technical data sheet clearing house, *see* ALLDATASHEET.COM, http://www.alldatasheet.com/ (last accessed March 30, 2012).

[81] LeadTek LR9805ST GPS Module Specification Sheet, Revision 0.9., ftp://ftp.leadtek.com/gps/9805st/LR9805ST_V0.9_052808.pdf (last accessed March 30, 2012). Note that specification sheets themselves may be inaccurate, due to errors or deceptive marketing practices. For example, the GPS accuracy depends on the number of satellites in view and their locations compared to the receiver. Also note that GPS position is only updated once per second, so a car traveling 60mph (88 feet per second) could have nearly an 88 foot error in position, which far exceeds the 10m (32.8 feet) specification.

[82] Sampling rate is the frequency with which a sensor system captures and analyzes data. Higher frequency sampling typically suggests higher accuracy than lower frequency sampling. For example, consider the difference between a GPS that calculates location every second versus a a GPS that updates every minute. Related technologies are sensor systems, such as a speed sensors in a police radar gun, that need only calculate a single instance of velocity to be legally viable. For these technologies, numerous velocity samples over an extended time frame are not necessary.

[83] Relative sampling rates played a significant role in a 2008 case where a defendant argued that a speeding ticket was invalid due to conflicting GPS data he provided to the court showing that he was travelling below the speed limit. *See* L.A. Carter, *Teen tries GPS defense to fight speeding ticket*, PRESS DEMOCRAT (July 12, 2008), http://www.pressdemocrat.com/article/20080712/NEWS/807120355/1033&title=Teen_tries_GPS_defense_to_fight_speeding_ticket.

Tamper resistance is also a critical component of automated law enforcement systems. Such systems must prove to an admissible standard that an offense occurred and by whom. However, even systems designed to be highly secure, such as electronic voting systems have proven vulnerable.[84] Tampering with automated law enforcement systems opens up the possibility of both False Positives, framing someone for an offense they did not commit, and False Negatives, destroying or altering system function or evidence such that the system fails to correctly identify an offense or suspect.

8. Administrative Burden

Given that an automated system can sense, analyze and act within a few seconds and never takes a lunch break, an automated system could generate hundreds of citations per day. This pace could pose an enormous burden on manual aspects of legal systems that in some jurisdictions are already at or near capacity, even with a zero False Positive rate.[85] As a cost-saving measure, governments could reduce the size of the police force, reducing jobs and potentially reducing safety. And the burden falls on citizens as much as the legal system. Even a less than 1% error rate could generate hundreds of cases where suspects are cited for violations they did not commit.[86]

[84] Consider the election of the fictional Futurama cartoon character Bender by hackers to the Washington, DC school board. Kevin Lee, *Hackers Elect Futurama's Bender to the Washington DC School Board,* PCWORLD (Mar. 2, 2012), http://www.pcworld.com/article/251187/hackers_elect_futuramas_bender_to_the_washington_dc_school_board.html

[85] *See, e.g.,* Ian Ith, *Seattle University professor's report calls misdemeanor courts "alarming,"* THE SEATTLE TIMES (Apr. 28, 2009), http://seattletimes.nwsource.com/html/localnews/2009139412_webmisdemeanors28m.html; Jim Galloway, *Georgia chief justice: Court systems on 'edge of an abyss,* POLITICAL INSIDER BLOG, ATLANTA JOURNAL CONSTITUTION (Mar. 16, 2010), http://blogs.ajc.com/political-insider-jim-galloway/2010/03/16/georgia-chief-justice-court-systems-on-edge-of-an-abyss/.

[86] *See, e.g.,* Meghan, E. Irons, *Caught in a Dragnet,* BOSTON.COM (July 17, 2011), http://articles.boston.com/2011-07-17/news/29784761_1_fight-identity-fraud-facial-recognition-system-license (describing an incident where a driver had his license mistakenly revoked via an automated facial recognition system because he looked like another driver).

Some have recently pondered the extreme burden that would be placed on the criminal justice system if every person charged with a crime asserted their Sixth Amendment right to a trial.[87] A similar burden might befall the criminal justice system due to the sheer increase in those prosecuted under a regime of perfect surveillance and perfect enforcement. Failure to accommodate this burden before implementation of an automated law enforcement system could have disastrous consequences.

9. *Procedural Safeguards*

Any automated law enforcement system must be sure to institute procedural safeguards against automation bias[88] and due process violations,[89] as well as ensuring an opportunity to appeal punishment. Additionally, automated law enforcement systems should be designed to minimize their enormous potential to commit egregious privacy violations under the Fourth Amendment, electronic surveillance regimes, and other privacy laws.[90] Transparency in the process is also absolutely critical to ensure proper functioning of the system and respect for the rule of law.[91] This section explores the various interests threatened by automated law enforcement that could benefit from procedural safeguards.

a. Due Process

Automated law enforcement systems threaten the fundamental right of procedural due process, that is, notice and an opportunity to be heard.[92] Any automated law enforcement system should be replete with "fail-safes," redundancies, and mechanisms to ensure that proper notice is

[87] Michelle Alexander, *Go to Trial: Crash the Justice System*, http://www.nytimes.com/2012/03/11/opinion/sunday/go-to-trial-crash-the-justice-system.html?_r=1&ref=opinion.

[88] *See, e.g.*, Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669 (2010).

[89] *See, e.g.*, Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

[90] *See* M. Ryan Calo, *Robots and Privacy*, IN ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS (Patrick Lin, George Bekey, and Keith Abney, eds. 2011).

[91] *See, e.g.*, Danielle Keats Citron, *Open Code Governance*, 2008 U. CHI. LEGAL. F. 355 (2008).

[92] *See, e.g.*, Citron, *supra* note 17.

effectuated and that individuals can effectively appeal automatically issued penalties. Danielle Keats Citron observed how automation of the administrative state could have due process consequences because automation can defeat participatory rulemaking, increase the likelihood of inaccurate outcomes, and encourage the presumption of a computer system's infallibility.[93]

The need to preserve due process that is threatened by automated systems is no less dire in the law enforcement context than in the administrative arena. Given the potential for error and mistaken reliance on the infallibility of machines within an automated law enforcement system,[94] the possibilities for insufficient notice abound.[95] Citron suggested that, "[a]t a minimum, automated systems should generate audit trails that record the facts and rules supporting their decisions."[96] These trails might help individuals fight the presumption of the automated system's infallibility.[97]

Additionally, the opportunity to be heard might be threatened if an appropriate system of appeals is not implemented to respond to potential increases in the sheer number of increase in violations.[98] The reinforcement of the appeals infrastructure with humans is expensive and to automate the appeals process would implicate many of the same potential due process violations as the initial enforcement action.

Citron advocated affirmative responses to dispel automation bias, disclosure of source codes to the public, requirements to rigorously test a

[93] *Id.*

[94] *Id.* Citron observed:

> Studies show that human beings rely on automated decisions even when they suspect system malfunction. The impulse to follow a computer's recommendation flows from human 'automation bias'—the 'use of automation as a heuristic replacement for vigilant information seeking and processing.' Automation bias effectively turns a computer program's suggested answer into a trusted final decision.

Id. (citing Raja Parasuraman & Christopher A. Miller, *Trust and Etiquette in High-Criciality Automated Systems*, 47 COMM. OF THE ACM 51, 52 (Apr. 2004); Linda J. Skitka, *Automation Bias and Errors: Are Crews Better Than Individuals?*, 10 INT'L J. AVIATION PSYCHOLOGY 85, 86 (2000)).

[95] *Id.* at 1275 (noting that "Automated systems routinely send faulty notices.").

[96] *Id.* at 1305.

[97] *Id.*

[98] *See supra* Part III,8.

system's software, attempts to incorporate public participation in automated decision systems, and a general reluctance to automate policy that has not undergone formal or informal rulemaking procedures.[99]

b. Privacy

The privacy of individuals is potentially threatened by nearly every automated law enforcement system capability. While the most obvious threat to privacy might be the pervasive surveillance enabled by ubiquitous sensors,[100] proper data minimization and retention safeguards[101] are required to adequately contain the enormous amount of information gathered by those sensors. Additionally, data use restrictions are required to address the improper use and distribution of information collected by automated law enforcement systems.

For example, can the driving information of motorists collected by local law enforcement be shared with federal agencies for purposes unrelated to enforcement of moving violations? Can this valuable information on driving habits be sold to insurance companies and marketers? If so, should some kind of verification process allow sharing only with responsible purchasers of data?

There is undeniable value that can result from this information, particularly for uses that might not be considered at the time of collection. Collected information can be used efficiently to enable private entities to uphold the law. For example, liquor stores may be encouraged to help participate in automated law enforcement schemes to curb the purchase

[99] Citron, *supra* note 17, at 1308-13.

[100] *See infra* Part III, 10.

[101] There is a constant tension between well-intentioned desires by government entities to retain data to facilitate enhanced analysis and the privacy rights of the populace. Recently the U.S. government issued new counterterrorism guidelines allowing the U.S. National Counterterrorism Center to retain data about U.S. citizens for five years, up from the previous limit of 180 days. *See* Sari Horwitz & Ellen Nakashima, *New counterterrorism guidelines permit data on U.S. citizens to be held longer*, WASHINGTON POST (Mar. 22, 2012), http://www.washingtonpost.com/world/national-security/new-counterterrorism-guidelines-would-permit-data-on-us-citizens-to-be-held-longer/2012/03/21/gIQAFLm7TS_story.html?wprss=; Eileen Sullivan, *Govt to keep info on Americans with no terror ties*, BOSTON.COM (Mar. 22, 2012), http://www.boston.com/news/nation/washington/articles/2012/03/22/govt_to_keep_info_on_americans_with_no_terror_ties/.

of alcohol by minors and, in return, be given a safe-harbor from local liquor laws for selling to anyone with a "verified" identity. Yet information collected with the best of intentions can still be used for improper purposes by others in other departments and future governments.[102]

Numerous scholars have addressed this issue. Danielle Keats Citron and Frank Pasquale have discussed the growing tendency of government and private entities to share information within what is known as "fusion centers."[103] Information collected by automated law enforcement systems would no doubt provide a substantial amount of information to these centers, but should they? And for what purpose? To what extent should information be allowed to be cross-referenced and added to our "digital dossiers?"[104]

M. Ryan Calo has discussed the many ways in which robots with sensors can implicate privacy concerns, particularly, the facilitation of direct surveillance, increased access to private spaces, and the unique social meaning of robots.[105] Calo posited that distinct privacy dangers flow from these attributes, like the ability to invade solitude, extract private information, and leverage the advantages of humans (e.g., praise, fear) in information gathering, without the burden of bad memory and fatigue.[106] Any automated law enforcement system taking advantage of robots should be mindful of these potential privacy harms and take steps to mitigate any potential abuse.

c. Freedom of Expression

In addition to violations of an individual's privacy, law enforcement surveillance can also potentially chill an individual's rights under the First Amendment, including the interests in promoting the freedom of speech,

[102] Mulligan, *supra* note 6, at 18.

[103] Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441 (2011).

[104] *See, e.g.*, DANIEL SOLOVE, THE DIGITAL PERSON (2006); Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2001); Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C.J. INT'L L. & COM. REG. 595 (2004).

[105] M. Ryan Calo, *Robots and Privacy*, in ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS (Patrick Lin, George Bekey, and Keith Abney, eds. 2011).

[106] *Id.*

association, thought, and belief.[107] The relationship between the First Amendment and the Fourth Amendment has been well documented.[108] The First Amendment right to anonymity has been seen as necessary to foster speech about unpopular views as well as a safeguard for intellectual inquiry.[109] Any law enforcement scheme must ensure that it is not unduly infringing upon the First Amendment rights of individuals.

d. The Necessity Defense

Many crimes provide for a necessity defense for violators who can demonstrate that violation of the law was required to prevent harm.[110] Specifically, the necessity defense has been recognized where "criminal action was necessary to avoid a harm more serious than that sought to be prevented by the statute defining the offense."[111] It is not difficult to imagine scenarios where activity in violation of the law is justified by necessity. For example, speeding might be justified to rush someone needing urgent medical care to the hospital. Reckless driving might be justified if the driver was avoiding obstructions in the road. Those under restraining orders might not be able to return home because the only route is via a bridge that lies within the restricted area.

Christina Mulligan noted, "In a system of 'perfect prevention,' technology could remove the ability to break laws in situations where the necessity defense would be applicable."[112] Indeed, any effective automated law enforcement system should accommodate necessary violations. This accommodation could be either built into the system itself or at least effectuated through the appeals system. Additionally, any system that relied upon "preemptive enforcement" should require stakeholders to decide whether to provide for an override in cases of necessity.

[107] *See, e.g.,* Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008).

[108] See, e.g., Daniel Solove, *The First Amendment as Criminal Procedure*, 82 N.Y.U. L. REV. 112 (2007).

[109] *Id.*

[110] Mulligan, *supra* note 6, at 29.

[111] United States v. Bailey, 444 U.S. 394, 410 (1980) (citations omitted).

[112] Mulligan, *supra* note 6, at 31.

e. Transparency

Transparency in the implementation and use of an automated law enforcement system is critical in order to avoid error and corruption of the system.[113] Citron stated, "The opacity of automated systems shields them from scrutiny. Citizens cannot see or debate these new rules. In turn, the transparency, accuracy, and political accountability of rulemaking are lost. Code writers lack the properly delegated authority and policy expertise that might ameliorate such unintentional policymaking."[114]

Yet many aspects of automated law enforcement systems might be withheld from public scrutiny for numerous alleged reasons such as national security, privacy, or, increasingly, intellectual property.[115] When third party contractors play a prominent and perhaps practically indistinguishable role from the government in automated law enforcement systems, how is the law to balance a contractor's claim of trade secrecy in the relevant proprietary information with the public's right to know? Here, it might be helpful to draw from similar transparency disputes involving third-party contractors, like voting machines and public Wi-Fi Internet access.[116] In any event, it is clear that without transparency, societal and legal doubts will likely plague the implementation and use of automated law enforcement systems.

10. The Social Cost of Automation

The increased intrusion of automated surveillance—both in depth and breadth—into the public and the private spheres of citizens' lives risks eroding the sacred trust between the citizen and the state and can dehumanize the governing process.[117] Automated law enforcement also

[113] *See, e.g.,* Danielle Keats Citron, *Open Code Governance,* 2008 U. CHI. LEGAL. F. 355 (2008).

[114] Citron, *supra* note 17, at 1254-55.

[115] *See, e.g.,* David S. Levine, *Secrecy and Unaccountability: Trade Secrets in Our Public Infrastructure,* 59 FL. L. REV. 135 (2007); David S. Levine, *The People's Trade Secrets?,* 18 MICH. TELECOMM. TECH. L. REV. 61 (2011); Citron, *supra* notes 17, 113.

[116] *Id.*

[117] *See, e.g.,* Daniel Solove, *I've Got Nothing to Hide' and Other Misunderstandings of Privacy,* 44 SAN DIEGO L. REV. 745 (2007) (noting that the chilling effects resulting from government surveillance "not only frustrate the individual by creating a sense of

threatens to degrade responsible citizenship, for it modifies behavior through fear of surveillance and reprisal rather than through a self-generated respect for the rule of law, an essential component of the social contract between citizen and state. Public reaction to dehumanized technology, particularly automation and robotics,[118] could result in unintended social consequences to automated processes.

In a sense, automated law enforcement creates an arguably safer, more stable society—a self-restrained citizenry who, under the perception of continual surveillance and potential threat of reprimand, normalize their actions within legally-defined parameters. Indeed, a self-policing, crime-free society appears, on the surface, a utopian ideal. Yet, as so many intellectuals have argued, a utopia most often devolves into a dystopic rendition of its ideal. Science fiction writers, particularly those concerned with unrestrained techno-creep, have explored the potential impact of these changes to our social fabric. The illusion of social stability comes at a profound cost. As Daniel Solove notes, the chilling effects resulting from government surveillance "not only frustrate the individual by creating a sense of helplessness and powerlessness, but they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives."[119]

Commenting on the prevalence of governmental monitoring in modern society, French philosopher Michel Foucault explains that due to the uncertainty of the scope and duration of the surveilling gaze, the individual becomes complicit in his own policing. "He who is subjected to a field of visibility, and who knows it, assumes responsibility for the constraints of power," Foucault theorizes. "[H]e makes them play spontaneously upon himself; he inscribes in himself the power relation in which he simultaneously plays both roles; he becomes the principle of his

helplessness and powerlessness, but they also affect social structure by altering the kind of relationships people have with the institutions that make important decisions about their lives.").

[118] *See, e.g.*, M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN ST. L. REV. 809 (2010); M. Ryan Calo, *Robots and Privacy*, in ROBOT ETHICS: THE ETHICAL AND SOCIAL IMPLICATIONS OF ROBOTICS (Patrick Lin, George Bekey, and Keith Abney, eds. 2011).

[119] Daniel J Solove, *I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007).

own subjection."[120] Thus, the citizen becomes his own policing agent, the watched and the watcher.

The lack of human interface—a robotic governing force in its place—may seem at first blush to be a cost-saving, utilitarian move, but in a free society law enforcement must be an extension of the social body, with power invested to it by the citizenry itself. Rather than human mediation in the surveillance and judicial process by the police officer, judge, and jury, the individual himself become complicit in the enforcement mechanism, resulting in what Foucault characterizes as a modern citizenry of "docile bodies."[121]

These concerns deepen when the government allows private contractors, such as Redflex Traffic Systems and American Traffic Solutions, to profit from automated law enforcement due to their involvement in the policing process.[122] One need only look at the state of Arizona's recent decision to halt the use of photo enforcement on its highways due to widespread privacy concerns and public outrage.[123]

The traffic cameras, previously located at dozens of locations throughout the state, resulted in wide-ranging civil disobedience by privacy groups and individual citizens, from refusal to pay the assessed fines, to petty vandalism of the cameras, to the tragic roadside murder of Doug Georgianni, a photo van operator working for Redflex Traffic Systems.[124] In the end, only about one third of the 1.2 million tickets were paid, indicating widespread discontent with the practice of photo enforcement.[125] State representative Sam Crump summarized the sentiment of many of his constituents when he stated, "Arizona has a

[120] MICHEL FOUCAULT. DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON. 202-03 (1995).

[121] *Id.* at 135.

[122] Ryan Randazzo, *Traffic Cameras Not Profitable for Arizona Cities,* THE ARIZONA REPUBLIC (July 3, 2011), http://www.azcentral.com/business/articles/2011/07/03/20110703traffic-camera-arizona-city-profit.html.

[123] Randall C. Archibald, *Arizona Halts Photo Enforcement of Speed Laws,* THE NEW YORK TIMES (July 15, 2010), http://www.nytimes.com/2010/07/16/us/16camera.html.

[124] Archibald, *supra* note 123; Jerry Garrett, *Speed Camera Operator Is Shot in Arizona*, THE NEW YORK TIMES, WHEELS BLOG (May 4, 2009) http://wheels.blogs.nytimes.com/2009/05/04/speed-camera-operator-is-shot-in-arizona/.

[125] Chris Matyszczyk, *Arizona to Remove Its Highway Cameras,* CNET NEWS (May 8, 2010), http://news.cnet.com/8301-17852_3-20004508-71.html.

proud heritage of leaving its citizens alone to the greatest sense possible, and I find that the photo radar speed cameras are really a violation of that heritage."[126]

These concerns grow exponentially as technological advances and an increasingly accepting public allow the scope of automated surveillance to weave its way deeper into our daily lives. Consider, for instance, the recent announcement by Hitachi Hokusai Electric that its new biometric surveillance camera can scan 36 million faces per second and will be available to governments within the next year, significantly enhancing existing facial recognition capabilities.[127] While speed cameras arguably impede our civil liberties to a limited degree, existing technologies foretell potential intrusions that will manifestly deepen the divide between the citizenry and the state only hinted at in the Arizona controversy. The damage to the trust, freewill, and sense of liberty essential to the functioning of a free society could be profound.

CONCLUSION

The prospect of widespread automated law enforcement, particularly for minor infractions, is no longer remote. The ubiquity of sensors,[128] advances in computerized analysis and robotics, and widespread adoption of networked technologies have paved the way for the combination of sensor systems with law enforcement algorithms and punishment feedback loops. Yet, socially, politically, and legally, we are unprepared for the automated enforcement of law.

No regulatory scheme currently exits to ensure that automated law enforcement systems are properly implemented and restricted. Indeed,

[126] *Lawmakers Propose Ban on Arizona Highway Speed Cameras*, AZCENTRAL.COM (Jan. 14, 2009), http://www.azcentral.com/news/articles/2009/01/14/20090114speed-cameras0114-ON.html.

[127] Rob Waugh, *Big Brother just got scarier: Japanese CCTV camera can scan 36 million faces per second - and recognise anyone who has walked into its gaze*, MAIL ONLINE (Mar. 23, 2012), http://www.dailymail.co.uk/sciencetech/article-2119386/Could-governments-recognise-ANYONE-instantly-CCTV-Japanese-camera-scan-36-million-faces-second.html.

[128] In addition to law enforcement interest, the current and growing ubiquity of sensors has not gone unnoticed by the intelligence community. *See* Spencer Ackerman, *CIA Chief: We'll Spy on You Through Your Dishwasher*, WIRED DANGER ROOM BLOG (Mar. 15, 2012), http://www.wired.com/dangerroom/2012/03/petraeus-tv-remote/.

there is no generally accepted conceptualization for what automated law enforcement even is, much less a unifying theoretical framework to guide the implementation of such automated systems.

This article examined the potential scope of automated law enforcement in an attempt to refine automated law enforcement as a concept capable of being effectively implemented and properly constrained. To that end, this article provided a framework for analysis of automated law enforcement systems that includes a conceptualization of automated law enforcement as the process of automating some or all aspects of surveillance, analysis, and enforcement in an iterative feedback loop.

This article demonstrated how intended and unintended consequences can result from the automation of any stage in this process and provides a list of issues that must be considered in any automated law enforcement scheme. Technological failures, administrative burdens, algorithmic encoding of the law, loss of discretion, threats to our civil rights, and the social cost of perfect enforcement are all potential consequences of automation that must be adequately addressed for any system to be successful.

There are undeniable benefits that can result from the use of automated law enforcement systems. Lower costs, more efficient enforcement, reduction of the impact of human bias in enforcement, and many other advantages over human enforcement will undoubtedly result in increased pressure and zeal to adopt these automated systems. Yet those deploying automated law enforcement schemes should be extremely cautious to ensure that the necessary calculus has been performed and adequate safeguards have been incorporated to minimize the potential for public harm.

Once adopted, automated schemes become entrenched and difficult to modify. That is why it is imperative to adequately explore the issue of automated law enforcement before its inevitable adoption. Given the effect automated law enforcement systems can have on our core interests of freedom, autonomy, due process, and privacy, there is simply too much at stake to fail to confront this issue.

***