A CONSERVATION THEORY OF GOVERNANCE FOR AUTOMATED LAW ENFORCEMENT

Gregory Conti, Woodrow Hartzog, John Nelson, and Lisa A. Shay

Continued advances in robotic technology, distributed sensor networks, and computerized analysis have made possible the automation of the entire law enforcement process, from detection of a crime, to identification of the perpetrator, to imposition of punishment. While this augurs well for more efficient and lower cost systems as inefficient and relatively expensive manual labor is replaced by robots and computers, governments and citizens must look beyond these obvious savings to assess the more subtle, but arguably more important, costs to society. To facilitate better decision making about when, where, and to what extent a law enforcement process should be automated, we propose a conservation theory of governance for automated law enforcement (ALE).

While efficiency and determinacy are often lauded as advantages for employing computers and robots over humans, inefficiency and indeterminacy have significant value in ALE systems and should be preserved in order to prevent severe societal harms. The conservation theory of governance for ALE states that those introducing or increasing automation in one part of the ALE system should evaluate the entire system holistically and ensure that inefficiency and indeterminacy are explicitly preserved or increased in other parts of the system.

Confronting Automated Law Enforcement

Gregory Conti,[1] *Woodrow Hartzog,*[2] *John Nelson,*[3] *and Lisa A. Shay*[4]

TABLE OF CONTENTS

[1] Associate Professor, Department of Electrical Engineering and Computer Science, US Military Academy at West Point.

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

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

[4] Associate Professor, Department of Electrical Engineering and Computer Science, US Military Academy at West Point.

INTRODUCTION: THE RISE OF AUTOMATION

While it may sound like science fiction, the automation of law enforcement is already here. Knightscope, a Sunnyvale-based robotics company, has designed a robot to support law enforcement personnel. *USA Today* reporter Marco della Cava compares K5, a 300-pound robot, to a conflation of two other well-known Hollywood robots: R2-D2 and Wall-E.[5] In contrast to these popular cinema icons, however, Knightscope designed K5 for a specific law enforcement function--a hardwired and multi-wheeled Dirty Harry. Della Cava writes: "[T]he robot's friendly vibe masks the serious intent of the company's CEO, William Li: to develop an ever-growing army of K5s that would roam shopping malls, corporate campuses and other public places with a mission to collect and analyze data, and tip off law enforcement to potential issues."

K5, which can travel up to 18 mph, has the capacity to scan 1,500 license plates a minute, a vast improvement in speed and efficiency over its human counterpart. While this seemingly benign mission of data collection and analysis--performed in the appealing trappings of a space-aged mall cop--might sound like a positive trend in leveraging technology to enhance public welfare and efficiency while decreasing cost (its estimated cost is $6.25 per hour of operation), we must consider the legal implications and social impact of such an endeavor.[6] Addressing what he calls "robophobia," Knightscope CEO William Santana Li writes in his blog, "Although it may be natural for folks to fear what lies ahead, it can more be exciting and productive to imagine the possibilities – and make them happen for the benefit of society as a whole. That is exactly what we are doing at Knightscope – an honorable mission to reduce crime by

---

[5] Marco della Cava. "Change Agents: William Li's robot wants to police you." http://www.usatoday.com/story/tech/2014/01/26/knightscope-k5-police-robot/4018047/. 26 January 2014. See also, Masahiro Mori's "Uncanny Valley," originally published in 1970 and officially translated into English in 2012 which explores the positive and sometimes repulsive aspects of robot aesthetics due to their similarity to humans. M. Mori (et al), "The Uncanny Valley," *IEEE Robotics & Automation Magazine*, June 2012, Vol: 19, No: 2, pp. 98-100.

[6] As a point of comparison, $6.25 per hour for K5 is less than the current $7.25 per hour Federal minimum wage in the United States. See United States Department of Labor, "Minimum Wage Laws in the States - January 1, 2014." http://www.dol.gov/whd/minwage/america.htm, last accessed 19 February 2014.

50%."[7] The benefits that robotic technology will bring to law enforcement--particularly in the areas of efficiency and cost savings--are theoretically impressive; however, employment of these technologies without careful consideration poses a distinct danger to our civil liberties and can have detrimental effects on society.[8]

Enhanced automated capability raises some important questions. What, if anything, is novel about automated law enforcement systems? How much authority should we bestow upon these automated systems? To what extent are technologists and policy makers capable of producing a system capable of exercising discretion and accounting for context in the same way humans can? Even if an automated law enforcement system is capable of achieving total legal compliance by the populous, is perfect enforcement of a law ever desirable? Prudence is therefore necessary as we embrace seemingly inevitable force multipliers in our brave new world of enhanced automated law enforcement.

Enforcement of the law has thus far been largely a manual process, one moderated by the discretion of human judgment and finite human resources, which were focused on priority offenses. Relatively speaking, this process is inefficient. Increasingly however, portions of, and in some cases the entire, law enforcement process from surveillance to punishment can be automated. Red light cameras and speeding tickets automatically issued by drones display the potential for automated enforcement in its early stages. The ubiquity of networked sensor devices, increases in processing power at lower cost, demands for revenue, and desires to increase public safety and security are seemingly leading to an era of productized automated law enforcement systems. If we want, inefficiency can be a thing of the past.

Yet, policy makers are unsure how to properly regulate automated systems. This is a problem because it seems that automated law enforcement systems will inevitably become more powerful and effective. If left unchecked, automated law enforcement systems could cause significant social harm despite attempting to improve public welfare.

---

[7] William Santana Li. "Why Are We Robophobic?" http://knightscope.com/why-are-we-robophobic/. 7 February 2014.

[8] We note that a society where everyone is surveilled is a society where everyone is presumed guilty at the outset. Mr. Li wants to "prevent" crime, but in reality he is just developing a means to more efficiently "detect" crimes. Will the one result in the other?

Anecdotes of partially or fully automated law enforcement, such as license plate readers and crowd-control robots, are becoming increasingly common. The implementation of these systems has sometimes been haphazard and seemingly always atheoretical. There is no guiding principle for policy makers and enforcement officers to ensure that automated law enforcement systems fulfill their objective in a way that respects privacy and civil liberties. Yet these same systems continue to proliferate in our day-to-day lives.

This article aims to remedy the dearth of guidance by developing a conservation theory of governance for the automated enforcement of the law. The central premise of this theory is that inefficiency and indeterminacy (usually in the form of human actors with free will) are vital components within the law enforcement process and should be conserved in some form. When one aspect of a law enforcement process (surveillance, analysis or action) is automated to increase efficiency and determinism, inefficiency and indeterminacy should generally be proportionally and explicitly preserved elsewhere in the process to prevent harms from automation. In short, we argue that inefficiency and human intervention should be conserved in automated enforcement systems through reallocation.

Making the discrete aspects of an automated system of law enforcement symbiotic through this conservation principle has at least two advantages. First, it forces policymakers to consider enforcement systems holistically, which will reduce internal conflict and unintended consequences. Additionally, it designates indeterminacy and inefficiency as necessary and desirable components of any automated law enforcement process, not weaknesses in the system, as they first might appear. Rather, they are essential checks and balances to maintain a civil and sustainable rule of law system.

In order to help develop this theory of conservation, this article also imposes order on the seemingly haphazard milieu of unmanned regulation by providing an end-to-end analysis of automatic law enforcement systems. In Part I of this article, we propose a revised taxonomy of three discrete aspects of an automated law enforcement system, conceptualized as surveillance, analysis, and action. A deeper understanding of each sub-component, and the larger process as a whole, allows for more effective analysis of automated law enforcement

proposals. In Part II of this article, we delineate specific, undesirable societal outcomes stemming from unchecked, ungoverned automation of surveillance, analysis and action. In Part III, we develop our conservation theory of automated law enforcement by explicating the value of inefficiency and indeterminism and the possible harms from automation to be avoided through conservation. We then explore how the theory might be applied using several scenarios. This article concludes that while increases in automation seem inevitable, law enforcement agencies should carefully maintain checks and balances with appropriate applications of inefficiency or indeterminism.

It is critical that those who implement and administer automated law enforcement systems have a theory of governance. Otherwise, scholars, technologists, law enforcement officials, privacy and civil liberty advocates, policy makers, purveyors of ALE systems, and individual citizens risk not being able to fully understand the potential for both efficiency and harm that automation poses to law enforcement, judicial systems, and public welfare. The importance of understanding, shaping incentives, and appropriately constraining current and future automated law enforcement systems is clear--failure to do so risks creating systems that undermine the system of laws and the free societies in which we live.

I. A REVISED TAXONOMY OF AUTOMATING LAW ENFORCEMENT

We have used the concept of "automating laws" as shorthand in previous research for the automation of various parts of the legal process.[9] 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. In order to apply conservation theory to ALE, each aspect of the legal process must be broken down into its constituent parts and critically examined to determine the risks and rewards of automation.

[9] Lisa Shay, Woodrow Hartzog, John Nelson, Dominic Larkin, and Gregory Conti, "Confronting Automated Law Enforcement" presented at the We, Robot Inaugural Conference on Legal and Policy Issues Relating to Robotics at the Miami School of Law, Coral Gables, FL, 21-22 April 2012.

At the highest level of abstraction we define three major actors interacting in three major parts of a process. 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. In a perfect case, the interplay among these actors results in criminals being caught, accurately judged, and fairly punished. In reality, the results are far messier.[10] Automation anywhere in these three areas can trigger the considerations listed later in this article.

Figure 1 shows a revised taxonomy that focuses on a three-stage process: surveillance, analysis, and action.

Surveillance includes all actions to detect that a crime has been committed, such as eyewitness or victim reports, observations by police officers (or private security personnel), and electro-mechanical sensors (such as cameras, radar guns, GPS trackers) which may or may not be operated by law enforcement agencies. The technology and systems we suggest provide data readily available to law enforcement, however, other systems that might require judicial approval may also provide significant surveillance data, such as smart homes,[11,12] private CCTV systems, or mobile devices. A comprehensive listing of all surveillance measures is beyond the scope of this paper, but the defining characteristics we suggest: speed (human or machine), unique subject identifier, and

[10] The problem is compounded by the use of automation in an attempt to gain efficiencies at various points in the process. Such automation can be a single step in a given process, as in the case of a speed gun used by a police officer to identify the speed of a passing motorist, after which largely manual processes are used to proceed. However, an end-to-end automated system may be constructed in an attempt to automate virtually all aspects of law enforcement for a given law or set of laws with little to no human oversight. As an example, consider a red light camera system that identifies violations, performs license plate recognition, conducts driving record retrieval, employs algorithmic adjudication, and automatically prints and mails citations to vehicle owners, all with only a cursory inspection performed by a human law enforcement official to limit errors.

[11] For one example of a smart home package, see AT&T's Digital Life offering. https://my-digitallife.att.com/learn/, last accessed 15 January 2014.

[12] "Why Google Bought Next for $3.2 Billion" http://www.elp.com/articles/print/volume-92/issue-1/columns/why-google-bought-nest-for-3-2-billion.html last accessed 3 March 2014

location information may be applied to other technologies, as desired. In previous research, we identified location, time, tracking, velocity, and identification as all being subject to automated surveillance.[13] We also suggest study of future candidate attributes, including more accurate time and location measurements, accuracy identification rates, and percent coverage of a given area. Surveillance ends with the determination that a crime may have been committed. This determination and all evidence is passed to the next stage: analysis.

The analysis stage consists of actions taken to identify the alleged perpetrator and/or to determine guilt or innocence of the suspect. These actions can include human investigation, human interrogation of suspects or witnesses (possibly augmented with technology), computer analysis of surveillance data, and manual or automated "mining" of multiple datasets to establish connections between individuals or between an individual and an action in the crime ("data mining"). The analysis stage also includes a determination as to whether the case should proceed to trial and if so, includes the trial itself. The end of the analysis stage is a determination of guilt or innocence for each defendant and a sentencing decision.

The action stage consists of carrying out the sentence or administrative action, via embarrassment/shaming,[14] delivering a ticket, manual or automatic monitoring of probation (e.g. using a GPS bracelet), incarceration, or in extreme cases, execution.

Consider this taxonomy in the context of red-light cameras. Sensors in the form of cameras are activated when a vehicle enters an intersection after the light has turned red (often with a "grace period" of 0.1 to 0.2 seconds). "These pictures document the date, time, and speed of the vehicle. Red light cameras also typically capture a picture of the vehicle entering the intersection and a picture of the vehicle in the intersection,

[13] Lisa Shay, Woodrow Hartzog, John Nelson, Dominic Larkin, and Gregory Conti, "Confronting Automated Law Enforcement" presented at the We, Robot Inaugural Conference on Legal and Policy Issues Relating to Robotics at the Miami School of Law, Coral Gables, FL, 21-22 April 2012.

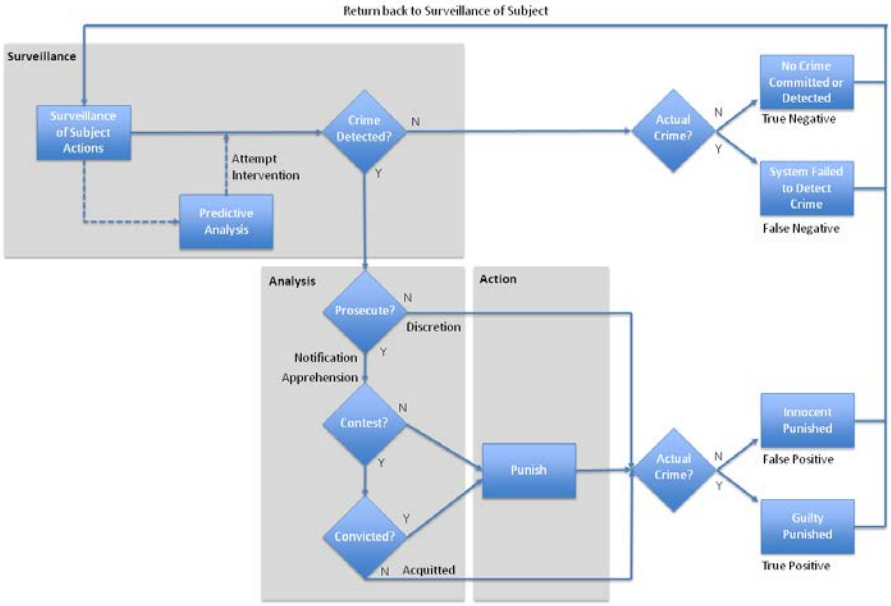
[14] See Lynn DeBruin, "'Shame' Punishments Increasing: Judges Order Ponytail Cutting, Sleeping In Doghouse, Wearing Embarrassing Signs," Associated Press, 24 June 2012. Consider also the use of offender registries such as the National Sex Offender database, http://www.nsopr.gov/, and online arrest search systems, e.g. Broward County Florida - https://www.sheriff.org/apps/arrest/, both of which are easily automated.

both during the red phase. Individual jurisdictions or camera vendors then process the pictures and issue the citation to the owner of the offending vehicle."[15]

Depending on the specific law the system attempts to enforce, each of these stages in the taxonomy is amenable to automation to varying degrees ranging from effectively impossible using today's technology to easily accomplished. In some cases, the entire process from start to finish may be automated, for example red light cameras (automated surveillance) triggering on a car crossing the intersection when the light is red and looking up the license plate number to find the address of the registered owner (automated analysis), and printing and mailing a ticket to the registered owner's address (automated action).

[15] Kimberly Eccles, Rebecca Fiedler, Bhagwant Persaud, Craig Lyon, Glenn Hansen, "Automated Enforcement for Speeding and Red Light Running," National Cooperative Highway Research Program Report #729, 2012. http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_729.pdf (accessed 8 March 2014), pp. 3-4

Figure 1: Overview of Automated Law Enforcement Model. The model has three major sections: surveillance, analysis (resulting in a determination of guilt or innocence), and action (resulting in punishment or freedom).



We anticipate such systems will increase in efficiency over time as sensing, networking, and processing technologies improve. The rate at which such systems are fielded, employed, and upgraded in practice will depend on several factors, including financial cost (and potentially financial incentives), performance, usability, and acceptability, but we believe the ultimate driver will be demands of national, regional, and local policy makers, law enforcement officials, or the public for greater use, efficiencies, and cost savings.

The degrees of automation will vary between contexts, but there are examples of how levels of automation might be created. For example, consider the Society of Automotive Engineer (SAE) International's Levels of Driving Automation for On-Road Vehicles.[16] From Level 0 (No Automation) to Level 5 (Full Automation), the model plots four different

[16] Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems, SAE International, http://standards.sae.org/j3016_201401/ .

variables: 1) Execution of Steering and Level of Acceleration/Deceleration; 2) Monitoring of Driving Environment; 3) Fallback Performance of Dynamic Driving Task; and 4) System Capability (driving modes).

Summary of Levels of Driving Automation for On-Road Vehicles

This table summarizes SAE International's levels of *driving* automation for on-road vehicles. Information Report J3016 provides full definitions for these levels and for the italicized terms used therein. The levels are descriptive rather than normative and technical rather than legal. Elements indicate minimum rather than maximum capabilities for each level. "System" refers to the driver assistance system, combination of driver assistance systems, or *automated driving system*, as appropriate.

The table also shows how SAE's levels definitively correspond to those developed by the Germany Federal Highway Research Institute (BASt) and approximately correspond to those described by the US National Highway Traffic Safety Administration (NHTSA) in its "Preliminary Statement of Policy Concerning Automated Vehicles" of May 30, 2013.

Level	Name	Narrative definition	Execution of steering and acceleration/ deceleration	Monitoring of driving environment	Fallback performance of *dynamic driving task*	System capability (*driving modes*)	BASt level	NHTSA level
Human driver **monitors the driving environment**								
0	**No Automation**	the full-time performance by the *human driver* of all aspects of the *dynamic driving task*, even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a	Driver only	0
1	**Driver Assistance**	the *driving mode*-specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	Human driver and system	Human driver	Human driver	Some driving modes	Assisted	1
2	**Partial Automation**	the *driving mode*-specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the *human driver* perform all remaining aspects of the *dynamic driving task*	**System**	Human driver	Human driver	Some driving modes	Partially automated	2
Automated driving system **("system") monitors the driving environment**								
3	**Conditional Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task* with the expectation that the *human driver* will respond appropriately to a *request to intervene*	System	**System**	Human driver	Some driving modes	Highly automated	3
4	**High Automation**	the *driving mode*-specific performance by an *automated driving system* of all aspects of the *dynamic driving task*, even if a *human driver* does not respond appropriately to a *request to intervene*	System	System	**System**	Some driving modes	Fully automated	3/4
5	**Full Automation**	the full-time performance by an *automated driving system* of all aspects of the *dynamic driving task* under all roadway and environmental conditions that can be managed by a *human driver*	System	System	System	**All driving modes**		

Levels of automation might look similar for surveillance, analysis, or enforcement of traffic laws. Levels of automation could be based on variables such as humans surveilling, processing data, analyzing data, reviewing decisions, whether any of this is done in "real time" or asymmetrically, and whether humans are physically present at the location of surveillance, analysis, or enforcement.

From the perspective of law enforcement and government officials, improvements to automated law enforcement systems are not guaranteed. Citizens may petition for the limitation or removal of automated law enforcement systems, and many have already done so.[17] Subjects or their supporters may employ a wide range of countermeasures, especially technical and policy countermeasures, that reduce efficiency of a system.[18] Technical countermeasures would strive to deny, degrade, deceive, corrupt, usurp, or destroy sensing, networking, storage, and processing capabilities of the system.[19] Policy countermeasures undermine the legal authorities which allow use of the system by legitimate entities.[20]

It is important to conceptualize law enforcement as a process with discrete parts for purposes of automation. Key stakeholders with the power to implement law enforcement systems might not be aware of the ripple effects automating one aspect of a system might have on the other aspects. For example, if surveillance is automated, much more information can be gleaned from that surveillance at a reduced transaction cost. Should analysis of this dramatically larger pile of information also be automated in order to keep up? If the decision-making process is automated and flag a significantly higher number of legal violations, should action also be automated in order to avoid a systemic apathy to identified crimes? In the section below, we explore potential social costs of automation at each point in an automated law enforcement system as well as holistically.

---

[17] Cyrus Farivar, "Iowa City to ban red-light cameras, drones, and license plate readers too, Ars Technica," http://arstechnica.com/tech-policy/2013/06/iowa-city-to-ban-not-only-red-light-cameras-but-drones-license-plate-readers-too/.

[18] Lisa Shay, Gregory Conti and Woodrow Hartzog. "Beyond Sunglasses and Spray Paint: A Taxonomy of Surveillance Countermeasures," Invited Presentation IEEE International Symposium on Technology and Society, 27-29 June 2013, Toronto, Ontario, Canada.

[19] Noah Shachtman, "'Degrade, Disrupt, Deceive': U.S. Talks Openly About Hacking Foes," Wired Danger Room Blog, 28 August 2012. http://www.wired.com/dangerroom/2012/08/degrade-disrupt-deceive/

[20] See Rachel Weiner, "Cuccinelli to work on NSA class-action lawsuit," Washington Post, 6 January 2014 http://www.washingtonpost.com/local/dc-politics/cuccinelli-to-work-on-nsa-class-action-lawsuit/2014/01/06/1832ee22-7720-11e3-8963-b4b654bcc9b2_story.html and James Warren, "White House task force report on NSA spying recommends sweeping reforms," New York Daily News, 18 December 2013. http://www.nydailynews.com/news/politics/white-house-release-report-reforms-nsa-spying-article-1.1551792.

II. SOCIAL COSTS OF AUTOMATED LAW ENFORCEMENT SYSTEMS

1. Surveillance

The social cost of automated surveillance is potentially profound, but our society has already been subjected to it with increasing scope and depth over the past several years. Until relatively recently, significant and collective outcry has failed to emerge. Certainly social activists and "robophobes," to borrow Samuel Jackson's term, have always raised concern at the potential Orwellian turn of ALE in our everyday lives; these voices normally have fallen on society's margins, however, and rarely have they voiced a collective sentiment. This passive acceptance seems to have changed recently with the intense media focus on Edward Snowden's leaked classified information about the National Security Agency's global automated surveillance system. The body politic the system was designed and employed to protect now turns against it for its deep invasiveness and troubling secrecy.

Consider the recent report that the UK's Government Communications Headquarters (GCHQ) allegedly conducted a vast, comprehensive surveillance and recording of Yahoo webcam users' online activities in an aptly titled operation named Optic Nerve. Reporters Spencer Ackerman and James Ball, pulling from Snowden's leaked NSA documents, reported the following: "GCHQ files dating between 2008 and 2010 explicitly state that a surveillance program codenamed Optic Nerve collected still images of Yahoo webcam chats in bulk and saved them to agency databases, regardless of whether individual users were an intelligence target or not ... In one six-month period in 2008 alone, the agency collected webcam imagery – including substantial quantities of sexually explicit communications – from more than 1.8 million Yahoo user accounts globally."[21] This automated surveillance, ostensibly conducted in the interest of national security, violated the privacy of millions of law-abiding citizens across the globe. The digital gaze--previously limited by the human eye in scope and duration--now has the potential for deepening and widening penetration as well as increasingly long-term archivability for future law enforcement analysis and deployment.

21 "Yahoo webcam images from millions of users intercepted by GCHQ," The Guardian, 27 February 2014. See http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

Director of National Intelligence James Clapper equated the controversial archiving of private internet communication to the collection of books in a library; most of those books will never be opened, he stated, just as most of the archived email traffic will never be directly read by a human analyst. "So the task for us in the interest of preserving security and preserving civil liberties and privacy," says Clapper, "is to be as precise as we possibly can be when we go in that library and look for the books that we need to open up and actually read."[22]

2. Analysis

Removing the human element from the analysis phase is likely the most troubling to critics of a completely automated law enforcement system. For it is human discretion--the intrinsic value of mitigation and extenuation--that would be missing without a human-in-the-loop.

Philosophers have long asserted that a law, no matter how well-intentioned or clearly stated, cannot be appropriate for all people in all circumstances. Consider Plato's analysis of government in The Statesman, "a law would never be capable of comprehending with precision for all simultaneously the best and most just and enjoining the best, for the dissimilarities of human beings and of their actions and the fact that almost none of the human things is ever at rest do not allow any art whatsoever to declare in any case anything simple about all and over the entire time."[23]

Given that laws must be adapted, interpreted, and even replaced, as times and circumstances change, it is clear that analysis leading to decisions of guilt or innocence should not be left entirely to an automated inflexible system. Humans are ideally suited for performing this adaptation and interpretation, since humans are the beings whose actions are affected and regulated by these laws. In contrast, the actions of computers or robots are governed by deterministic programs which are rarely designed to adapt or change and who receive neither benefit nor

22 "NSA robots are 'collecting' your data, too, and they're getting away with it," The Guardian, 27 February 2014. http://www.theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier

23 Plato. "The Statesman." Trans. Seth Benardete. The Being of the Beautiful: Plato's Theaetetus, Sophist, and Statesman (Chicago: University of Chicago Press, 1984) sec. 294.

harm from a law, whether just or unjust or whether applied fairly or unfairly. While ultimately these algorithms are designed by humans, they require all contextual decisions to be made ex ante, thus limiting the ability for human discretion to mitigate seemingly unjust or excessive enforcement of a particular law. Therefore, the analysis portion of the ALE system, which concludes with a determination of guilt or innocence, must at some point be tempered ex ante or simultaneously with automation by human judgment.

3. Action

As automated surveillance increases in power and scope and crime detection is further perfected, is our legal system justified tolerating criminality by intentionally ignoring known violations of the law? Does perfect detection obligate perfect enforcement or risk undermining the rule of law, an essential component of our social fabric? Or should flexibility or a level of toleration be engineered into the automated system so that illegal behavior isn't detected and then purposefully ignored? If so, what principles allow designers to shape this forgiveness ex ante? At the root of these questions is the legitimacy of toleration within our legal system. As we will argue below, perhaps simply preserving inefficiency and indeterminacy as a matter of design and procedure will help avoid these social costs without having to set principles of forgiveness in stone.

Slovenian Marxist philosopher and cultural critic Slavoj Žižek asserts in *The Plague of Fantasies* that "far from undermining the rule of the Law, its 'transgression' in fact serves as its ultimate support. So it is not only that transgression relies on, presupposes, the Law it transgresses; rather, the reverse case is much more pertinent. Law itself relies on its inherent transgression, so that when we suspend this transgression, the Law itself disintegrates."[24] While Žižek may overstate the importance of transgression, or disobedience, for the stability of our legal system, the capacity to transcend judicial boundaries is inarguably essential to the establishment of those constraints in the first place. Why else would legal restrictions exist? They would be unnecessary and redundant in a world in which automation prevents transgression. Intent, criminal or not, would thereby be trumped preemptively and always. Such a world strips

24 Slavoj Žižek. The Plague of Fantasies, (London: Verso, 1997), pp.77.

human agency from us by disallowing deviancy and rebellion, risk-taking and that justified, isolated breach. A safer, more docile world we would have perhaps, but absent the free will that necessitates governance in the first place, we should question the foundation of those very systems that strip away our ability to challenge codified legal constraints.

Equally important to this need to be free to disobey--to transgress if you will--is, of course, is our desire and, indeed, our innate need to *choose to obey*. If compliance as a forced function reaches its fully-automated capacity of total enforcement, then we can no longer be deemed a "law-abiding society," for instead we would be imprisoned--not abiding by choice--within an artificially-constrained world, potentially constrained in both our public and private spheres. What then of responsible citizenry?

In his book *Liars and Outliers: Enabling the Trust that Society Needs to Thrive*, Bruce Schneier echoes many social advocates before him when he writes that law breaking is at times necessary for social change. In fact, law breaking under certain circumstances might be just as critical to our social fabric as abiding by the law. We might consider such famous and morally-justified breaches of the law by noted activists like Martin Luther King, Jr., and Mahatma Ghandi. In his highly-influential essay "Civil Disobedience," Henry David Thoreau writes, "If the machine of government is of such a nature that it requires you to be the agent of injustice to another, then, I say, break the law."[25] Thoreau was responding, in part, to his moral outrage against slavery and the Mexican-American War. Imagine a society in which morally-justified civil disobedience like Thoreau's is made impossible by perfected surveillance and enforcement, when transgression rises to the level of a moral imperative yet is stymied by the totality of our brave new system, an unchallengeable "machine of government." How might this affect our individual and collective ability--and obligation--to confront, in full, government-sanctioned abuses or missteps?

The benefits of automated law enforcement in the form of increased efficiency and consistency are readily apparent and discussed below. In theory, better enforcement reduces crime by increasing the likelihood of punishment, among other things. More consistent decisions through automation can mitigate the harmful effects of enforcement bias and

25 Henry David Thoreau. Civil Disobedience and Other Essays, (Digireads.com, 2005).

related abuse of discretion harms. Citizens are, in theory, all held to a more consistent standard, resulting in a harmonization regarding the particular boundaries and interpretation of the law.

But it is critical to consider carefully the long-term and nuanced implications of ceding human decision-making to human-derived but computer-driven algorithms that seemingly streamline, simplify, and reduce the cost of more traditional methods but reduce human agency at all junctures. We examined this in our previous study. The imperfections of current automated law enforcement systems most certainly are considerable and should cause the prudent critic to pause; the perfected system, if even possible and whatever that "ideal" system may look like, can be equally troubling, however, since we naturally cringe at the concept of omniscient governmental control due to the value we place on freedom and privacy.

III. A CONSERVATION THEORY FOR AUTOMATED LAW ENFORCEMENT

The central premise of our theory is that inefficiency and indeterminacy (in the form of human actors with free will) are vital components within the law enforcement process and should be conserved in some form. When one aspect of a law enforcement process (surveillance, analysis or action) is automated to increase efficiency and determinism, inefficiency and indeterminacy should generally be proportionally and explicitly preserved elsewhere in the process to prevent harms from automation. Automating surveillance, analysis, or action makes it important to ensure that inefficiency or indeterminism is correspondingly preserved or introduced into the rest of the system to protect social welfare and prevent harm. In short, we argue that inefficiency and human intervention should be conserved in automated enforcement systems through reallocation.

In previous research, we identified potential problems with automated law enforcement systems, including concerns about inaccuracy, bias, due process, privacy, inflexibility, over-enforcement, and abuse. Many of these concerns are viable because automation decreases the transaction cost of surveillance of individuals, the analysis of that surveilled data, and actions based upon that analysis. (See Figure 1). In other words, the elevated concern over automated law enforcement is primarily due to the fact that efficiency brings reduced transaction costs which, in turn, encourages

greater use of surveillance, analysis, and action (punishment), leading to reduced privacy, due process concerns,[26] and the specter of perfect enforcement culminating in an Orwellian police state.

It is important to note that we do not argue that automated technologies are inherently problematic. Robots and other automated technologies hold great promise to dramatically improve the lives of everyone on earth. Rather, it is at the intersection of automation and legal obligation where we urge caution. Automated systems enable at least two dramatic departures from the status quo. First, automated systems are highly efficient, which can reduce the cost of surveillance, analysis, and enforcement to negligible levels per incident. Manual surveillance, analysis, and enforcement requires manpower, money, and time. Automation can be centralized, cheap, and virtually instantaneous. Second, automated systems are completely predictable. They will react to the same input in the exact same way every single time. In this way, they are determinate because there is no room for choice in a given model.[27] Thus, automated law enforcement holds the promise of efficiency and consistency. We anticipate that these advantages will motivate and be used to justify the adoption of automated technologies.

We assert that inefficiency and indeterminacy in the form of human intervention and deliberate technological restriction are relative virtues of our current law enforcement system, not a drawback. Not only does inefficiency and indeterminacy allow for more contextualized, localized, and adaptive decision making, but they also help obviate the dilemma of the perfect enforcement of laws that were drafted with likely assumptions that enforcement would be resource intensive and, thus, optimize justified enforcement attempts.[28] Although this theory might seem regressive, both

26 The development of highly efficient automated law enforcement systems without corresponding efficiencies afforded to due process threatens subjects' ability to rebut accusations or appeal convictions, effectively pitting highly automated government systems against the human subject's personal time to resolve wrongs and provide self-defense. Asymmetries such as these are seen in voice mail systems that force users to navigate byzantine menus, wait on hold, and tolerate canned music to ultimately reach a human operator, effectively acting to shield bureaucracies against interaction with the public.

27 Harry Surden, The Variable Determinacy Thesis, 12 Columb. Sci. & Tech. L. Rev. 1 (2011).

28 For an exploration of the absurd results from developing code to enforce laws that failed to contemplate de minimus transaction costs for enforcement, *see* Lisa Shay,

inefficiency and indeterminacy humanize the automated law enforcement process and thus make it palatable for a free society. As a result, they should be accounted for and relatively conserved by those who would implement automated systems. In this part, we discuss the virtue of inefficiency and indeterminacy and the different ways in which they may be created and preserved.

1. Inefficiency

Law enforcement is, by and large, inefficient. It costs time and resources for most crimes to be detected, investigated, prosecuted, and punished. Many see this as a burden. The number of crimes committed is inevitably more than the number processed through to punishment. Standing alone, this innate inefficiency might appear as a flaw within the law enforcement system. However, we assert that it is an essential counter to the potential totality and flawlessness of a completely automated system. It necessarily disrupts and delays the rote, mechanical processing of pre-programmed procedures thereby allowing human intervention at critical points in the system.

Consider the issuance of a speeding ticket. In analog policing regimes, a police officer might wait in a concealed location and capture a vehicle's instantaneous speed as it passes by. If this speed crosses the officer's own particular enforcement threshold, the police office will stop the car, engage the driver, and potentially issue a ticket. However, an automated system could maintain a continuous flow of samples based on driving behavior and issue tickets accordingly. Our previous experiment demonstrated that a typical driver could be issued over five hundred tickets in a one hour trip, on a commuting route where there were at most two police cars stationed on a given day and often none at all. There are at least three different kinds of inefficiencies that can maintain the transaction cost of enforcement at desirable levels: 1) Human intervention in “the loop,” 2) countermeasures, and 3) technical governors.

Woodrow Hartzog, John Nelson, and Gregory Conti, “Do Robots Dream of Electric Laws? An Experiment in the Law as Algorithm” presented at We, Robot Getting Down to Business, at the Stanford University Law School, Stanford, CA, 8-9 April 2013.

a. Human Intervention in "The Loop".

The process of law enforcement has historically relied heavily on human police, investigators, judicial officials, and correction officers to function. Operating at human speed, rather than the much-faster machine speed, law enforcement systems traditionally possessed inherent inefficiencies and extensive human intervention that greatly limited the type, extent and duration of surveillance; prioritized enforcement of the law; contextualized decision making; and moderated the law's social impact. The bulk of laws on the books and the rich history of precedent on which today's legal decisions are based spring from this analog environment and assume this tradition of human intervention.

We are entering a new era when large portions of the law enforcement process may be automated, however, potentially with little to no human oversight or intervention. Enabling technologies--such as robotics, sensors, networking, and machine learning--are now removing these barriers, and important friction, from the process. These advances, which promise greater efficiency and accuracy at a greatly reduced cost (and sometimes increased profit[29]), are welcomed by officials in the quest for improved public safety through more efficient enforcement of the law. Emerging today are end-to-end Automated Law Enforcement (ALE) systems that include surveillance, crime detection, legal processing, and punishment of certain laws or classes of laws, for example, red light violations at intersections and violations of speed limits.[30]. Little has been done, however, to assess the social impact of human absence from the process.

b. Countermeasures.

We define countermeasures to mean actions taken in response to

[29] These systems can then be productized and sold. As an example, see Xerox's Photo Enforcement offerings. http://services.xerox.com/transportation-solutions/transportation-management-systems/photo-enforcement/enus.html.

[30] Kimberly Eccles, Rebecca Fiedler, Bhagwant Persaud, Craig Lyon, Glenn Hansen, "Automated Enforcement for Speeding and Red Light Running," National Cooperative Highway Research Program Report #729, 2012. http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_729.pdf (accessed 8 March 2014).

perceived threats from automation of some aspect of law enforcement.[31] Our previous analysis of automating enforcement of one type of law led to explorations of countermeasures of surveillance, the first necessary step in automating the law.[32] Few would tolerate receiving 500 tickets during a one-hour trip, as our study indicated. Evidence already shows that an overzealous approach to law enforcement encourages individuals and organizations to take (sometimes illegal) countermeasures.[33]

For instance, earlier this year as a protest against the European Police Congress held in Berlin, German activists created a real-world "game" awarding points to teams who destroyed or removed surveillance cameras in major German cities, with bonus points for creative techniques.[34] The likelihood and acceptability of countermeasures are far greater with the human actor removed from the process, for no longer is the citizen acting against the police officer, the investigator, the court official but instead against faceless technology employed against the populace, a far more palatable target of resistance.

Elizabeth Joh has called countermeasures to surveillance in certain contexts "privacy protests." She writes:

> Ordinary American life today cannot be easily lived without being targeted by government surveillance. Many, if not most, people acquiesce to these demands for information about them, either out of acceptance or resignation. But some people object. They take steps to *thwart* police surveillance, not because they are seeking to conceal criminal acts, but out of ideological belief or

[31] Lisa Shay, Gregory Conti and Woodrow Hartzog. "Beyond Sunglasses and Spray Paint: A Taxonomy of Surveillance Countermeasures," Invited Presentation IEEE International Symposium on Technology and Society, 27-29 June 2013, Toronto, Ontario, Canada.

[32] Lisa Shay, Woodrow Hartzog, John Nelson, and Gregory Conti, "Do Robots Dream of Electric Laws? An Experiment in the Law as Algorithm" presented at We, Robot Getting Down to Business, at the Stanford University Law School, Stanford, CA, 8-9 April 2013.

[33] Lisa Shay, Gregory Conti and Woodrow Hartzog. "Beyond Sunglasses and Spray Paint: A Taxonomy of Surveillance Countermeasures," Invited Presentation IEEE International Symposium on Technology and Society, 27-29 June 2013, Toronto, Ontario, Canada.

[34] Kim Zetter. "German Activists Punch Out Big Brothers Eyes." Wired Danger Room Blog, 31 January 2013.

> personal conviction. Advice on "surveillance defense" and counter-surveillance products is readily available on the internet: Use Tor to surf the internet. Encrypt your digital communications. Use disposable "guerilla email" addresses and disposable phone numbers. Avoid ordinary credit cards and choose only cash, prepaid debit cards, or bitcoins to make a financial trail harder to detect. Avoid cell phones unless they are "burners" (prepaid phones), "dumb phones," or "freedom phones" from Asia that have had all tracking devices removed. Alternatively, hide your smartphone in an ad hoc Faraday cage, like a refrigerator, to avoid being tracked. Use photoblocker film on a license plate or a ski mask to thwart a red-light camera. Use a Spyfinder camera detector to see if someone is watching you. Use "spoof cards" that mask your identity on caller identification devices. Burn your garbage to hamper investigations of your financial records or the collection of your genetic information. Hire a professional to alter your digital self on the internet by erasing data or posting multiple false identities. At the extreme end, you could live "off the grid" and cut off all contact with the modern world.[35]

Countermeasures could play a critical role in conserving both inefficiency and indeterminacy in an automated system. By their very nature, countermeasures aim to frustrate enforcement efforts. If effective, they render these efforts inefficient because greater resources will be required to make them work. Countermeasures also preserve indeterminacy, at least for the surveilled, by helping ensure that surveillance, analysis, and enforcement is not guaranteed.

Policy makers should be mindful of the availability and legality of countermeasures when automating a system. To the extent that countermeasures are desirable, they should not be explicitly prohibited. One notorious instance where perfect enforcement has been sought and countermeasures have been explicitly prohibited is the Digital Millennium Copyright Act's ban on circumventing technological copyright controls.

[35] Elizabeth E. Joh, Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion, 55 Ariz. L. Rev. 997, 1000-01 (2013)

The DMCA attempts to mandate respect for digital rights management (DRM)4 by instituting anticircumvention provisions into U.S. copyright law. These provisions are, in effect, a ban on the act of circumventing or trafficking in devices that circumvent certain DRM systems.[36]

In some instances, countermeasures should even be explicitly allowed.[37] Given the uncertainty in many computer crime laws, including the Computer Fraud and Abuse Act, it is not entirely clear when countermeasures may be deployed in response to government surveillance, analysis, and action.[38]

c. Technical and Procedural Governors.

Technical governors are mechanisms created by technologies or regulation that reduce the capability of a sub-system within the ALE framework. For instance, law enforcement officials must follow appropriate authorization process before they can install a wiretap.[39] The limit to the number of phone calls monitored is determined by law, not a limitation of the underlying technology. Law enforcement officials must follow the appropriate authorization process before installing a GPS tracker on a suspect's vehicle.[40] Again, the limitation on tracking cars is due to a constraint imposed by the law, not a limitation of the technology.

Paul Ohm has proposed that privacy and transparency goals can be simultaneously achieved by making information "hard but possible" to obtain.[41] Harry Surden has likewise recognized the value in high transactional costs to protect privacy, noting that "Society relies upon...latent structural constraints to reliably inhibit certain unwanted conduct in a way that is functionally comparable to its use of law. For example, society has frequently depended upon the search costs involved

[36] Woodrow Hartzog, Falling on Deaf Ears: Is the Digital Millennium Copyright Act Effective in Protecting Fair Use?, 12 J. Intell. Prop. L. 309, 312-13 (2005).

[37] A. Michael Froomkin, "Pets Must Be on A Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology, 74 Ohio St. L.J. 965, 966 (2013) ("A government concerned with protecting personal privacy and enhancing user security against ID theft and other fraud should support and advocate for the widespread use of [privacy enhancing technologies].").

[38] 18 U.S.C. § 1030.

[39] 18 U.S.C. §§ 2510–2522.

[40] Unites States v. Jones, 132 S. Ct. 945 (2012).

[41] Paul Ohm, Good Enough Privacy, 2008 U. Chi. Legal F. 1, 63 (2008).

in aggregating and analyzing large amounts of information to effectively protect anonymity."[42] These theories for protecting privacy by imposing artificial transaction costs could be expanded to protect against many different kinds of harm made possible through automation.

2. Indeterminacy

The second concept that automated systems should be designed to preserve is indeterminacy. As a term of art, if something is determinate then it has a constrained predictability. Consequently, indeterminate systems have fewer constraints on predictability and, as a result, are more random. Computer algorithms are usually implemented using deterministic state machines, systems where the transitions from state to state are uniquely determined.[43] In other words, the algorithm will always produce the same output for a given input under the same conditions: If a car is detected to exceed a speed limit, a traffic ticket will be issued.

While this predictability and repeatability is desirable in most software systems, it can be overly constraining in a legal system where the accused would like to account for extenuating and mitigating circumstances. In our previous research, we argued:

> Many crimes provide for a necessity defense for violators who can demonstrate that violation of the law was required to prevent harm. 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." 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

[42] Harry Surden, Structural Rights in Privacy, 60 SMU L. Rev. 1605 (2007).

[43] Frank Vahid, Digital Design, 2nd Edition, John Wiley & Sons: Hoboken, NJ, 201, p. 142.

restricted area.[44]

Indeterminacy, defined as the condition or quality of uncertainty, seems a strange characteristic to be desired within the rule of law spectrum, yet it illuminates an essential entry point for humans in the automated law enforcement system. In literary studies, indeterminacy requires readers to interpret their own meaning when faced with textual uncertainty, in a sense, to create meaning from those elliptical moments within a text based on personal experience and intuition. In other words, indeterminacy calls upon a reader to fill in meaning gaps. In law enforcement, indeterminacy recognizes that the data provided by a set of sensors might be incomplete and a decision based solely on that data would be inaccurate or invalid. Thus, the human-in-the-loop is a desired insertion at moments of legal indeterminacy in order to complete the narrative using intuition and an understanding and appreciation for the full range of human experience combined with legal knowledge. Indeterminacy ensures that the process of automated enforcement is extended and iterative in order to add meaning and certainty to the information collected, analyzed, and acted upon.

It is also worth noting that certain human characteristics, such as empathy, are difficult to program into systems. Thus, in the process of becoming determinate, they code intangibles like empathy out of the system. Perhaps one of the most vivid reasons to preserve uncertainty via humans is the preservation of these intangibles that can help produce outcomes that might be desirable even if they constitute a deviation from predictable standard protocol.

In practical terms, if automation is increased at one point in the ALE system, indeterminacy would be achieved by human intervention "downstream" or after the point at which the automation was increased. If surveillance is automated, keep "humans in the loop" to review or interpret the surveillance data, or at least data flagged as an indicator of suspicious activity. If analysis is automated, have a human review the analysis decision. If enforcement is automated, maintain a human-mediated appeals process.

---

[44] Lisa Shay, Woodrow Hartzog, John Nelson, Dominic Larkin, and Gregory Conti, "Confronting Automated Law Enforcement" presented at the We, Robot Inaugural Conference on Legal and Policy Issues Relating to Robotics at the Miami School of Law, Coral Gables, FL, 21-22 April 2012.

3. The Benefits of Conserving Inefficiency and Indeterminacy

a. Contextualized Decisions

One of the most difficult aspects of designing an automated system is that all decisions about how the system will respond in any given situation must be made ex ante. In our previous research, we stated "Despite the best intentions of designers, any model of the law and of the physical world is, by definition, a simplification. Environmental variables will fall outside the model, leading to error. Potholes develop, trees fall on the road, and streets become icy. Lack of context as well as absence of the traditional police officer's domain knowledge is likely, and in some cases inevitable, due to lack of appropriate sensor data or inability to process higher level cognitive functions in software."[45] We noted that "a robotic car might slide through a stop sign due to snow and possibly even decide it did stop because the wheels are not turning. Or the car may drive 15 MPH on a freeway because a repair crew forgot to take down an RFID-enabled construction zone sign."[46]

Fully-automated systems lack the ability to contextualize alleged crimes. For instance, violating speed limits and traffic signals might in some cases be not only morally justified but potentially even obligated, for the protection of life or limb perhaps.

In a very helpful essay, Professor Patrick Lin explored the limits of automated decision making and the importance of context in these decisions for driverless vehicles. Lin began, "If a small tree branch pokes out onto a highway and there's no incoming traffic, we'd simply drift a little into the opposite lane and drive around it. But an automated car might come to a full stop, as it dutifully observes traffic laws that prohibit crossing a double-yellow line. This unexpected move would avoid bumping the object in front, but then cause a crash with the human drivers behind it. Should we trust robotic cars to share our road, just

[45] Lisa Shay, Woodrow Hartzog, John Nelson, and Greg Conti, "Do Robots Dream of Electric Laws? An Experiment in the Law as Algorithm" presented at We, Robot Getting Down to Business, at the Stanford University Law School, Stanford, CA, 8-9 April 2013.

[46] *Id.*

because they are programmed to obey the law and avoid crashes?"[47] Lin argued, "Our laws are ill-equipped to deal with the rise of these vehicles...For example, is it enough for a robot car to pass a human driving test? In licensing automated cars as street-legal, some commentators believe that it'd be unfair to hold manufacturers to a higher standard than humans, that is, to make an automated car undergo a much more rigorous test than a new teenage driver."[48]

According to Lin, "there are important differences between humans and machines that could warrant a stricter test. For one thing, we're reasonably confident that human drivers can exercise judgment in a wide range of dynamic situations that don't appear in a standard 40-minute driving test; we presume they can act ethically and wisely."[49] Lin also sees the potential problem from automating legal compliance, stating, "because the legal framework for autonomous vehicles does not yet exist, we have the opportunity to build one that is informed by ethics. This will be the challenge in creating laws and policies that govern automated cars: We need to ensure they make moral sense. Programming a robot car to slavishly follow the law, for instance, might be foolish and dangerous."[50]

The classic example that has been put forward with respect to the difficulty of pre-programming decisions according to context is that programmers must eventually deal with the "Trolley Problem." Lin describes the problem, originally proposed by philosophers Philippa Foot and Judith Jarvis Thomson, as follows:

> Imagine a runaway trolley (train) is about to run over and kill five people standing on the tracks. Watching the scene from the outside, you stand next to a switch that can shunt the train to a sidetrack, on which only one person stands. Should you throw the switch, killing the one person on the sidetrack (who otherwise would live if you did nothing), in order to save five others in harm's way? A simple analysis would look only at the numbers: Of course it's better that five persons should live than only one person, everything

[47] Patrick Lin, http://www.theatlantic.com/technology/archive/2013/10/the-ethics-of-autonomous-cars/280360/.

[48] *Id.*

[49] *Id.*

[50] *Id.*

> else being equal. But a more thoughtful response would consider other factors too, including whether there's a moral distinction between killing and letting die: It seems worse to do something that causes someone to die (the one person on the sidetrack) than to allow someone to die (the five persons on the main track) as a result of events you did not initiate or had no responsibility for.[51]

Lin notes that this dilemma isn't just a theoretical problem, stating "Autonomous cars may face similar no-win scenarios...and we would hope their operating programs would choose the lesser evil. But it would be an unreasonable act of faith to think that programming issues will sort themselves out without a deliberate discussion about ethics, such as which choices are better or worse than others....Human drivers may be forgiven for making an instinctive but nonetheless bad split-second decision, such as swerving into incoming traffic rather than the other way into a field. But programmers and designers of automated cars don't have that luxury, since they do have the time to get it right and therefore bear more responsibility for bad outcomes."[52]

So too it is with automated law enforcement. Designers are charged with creating a system that responds appropriately to contextual variations. For the time being, these systems have a limited capacity to make such nuanced distinctions. Prioritizing human discretion through conserved inefficiency and indeterminacy will ensure that a partially-automated law enforcement system is adaptable and capable of fine-grained decisions based upon various contexts.

b. Mitigating Harm

In previous research, we documented the harm that can come from improperly automated law enforcement. We stated, "Any automated law enforcement system must be sure to institute procedural safeguards against automation bias and due process violations, as well as ensuring an opportunity to appeal punishment. Additionally, automated law enforcement systems should be designed to minimize their enormous

[51] *Id.*
[52] *Id.*

potential to commit egregious privacy violations under the Fourth Amendment, electronic surveillance regimes, and other privacy laws."[53]

Automation bias refers to the human tendency to irrationally trust automated decisions. Professor Danielle Citron has noted, "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."[54]

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, automated information analysis might also spark privacy concerns, particularly in the age of "big data," where algorithms comb through piles of information for hidden or surprising correlations and inferences.[55] Conserving inefficiency and indeterminacy will mitigate the harms from surveillance from a sheer reduction in scope and number of people surveilled. Inefficient surveillance requires prioritization about how to expend limited resources. Meanwhile indeterminacy will mitigate the harms from erroneous data analysis by allowing humans to make

---

[53] Lisa Shay, Woodrow Hartzog, John Nelson, Dominic Larkin, and Gregory Conti, "Confronting Automated Law Enforcement" presented at the We, Robot Inaugural Conference on Legal and Policy Issues Relating to Robotics at the Miami School of Law, Coral Gables, FL, 21-22 April 2012 (citing Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669 (2010) and Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008)).

[54] Citron (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)).

[55] Ira Rubinstein defines big data as "a problem-solving philosophy that leverages massive datasets and algorithmic analysis to extract "hidden information and surprising correlations." Ira Rubinstein, Big Data: The End of Privacy or a New Beginning?, 3 Int'l Data Privacy L. 65, 74 (2013). The term "big data" has no broadly accepted definition and has been defined many different ways. See Viktor Mayer-Schönberger & Kenneth Cukier, Big Data: A Revolution that Will Transform how We Live, Work, and Think 6 (2013) ("There is no rigorous definition of big data . . . . One way to think about the issue today . . . is this: big data refers to things one can do at a large scale that cannot be done at a smaller one, to extract new insights or create new forms of value . . . .")

sense of the complexity involved in understanding data and language. For example, IBM's Watson has difficulty understanding slang and distinguishing between polite and impolite language.[56]

Conserving inefficiency and indeterminacy will also help mitigate harms to the freedom of expression. For example, consider the importance of countermeasures against surveillance. In exploring anti-mask laws and online real name policies, Margot Kaminski asked "Can the government impose a blanket ban on anonymity to thwart the masked and uncatchable bank robber, at the expense of the mask-wearing protester?"[57] She concludes that "A blanket real-world ban on anonymity...chills protected expression; and physical anonymity is becoming increasingly important in today's surveillance society."[58] Kaminski reaches a similar conclusion with respect to real name policies. The power of anonymity has grown exponentially over the past decade with the government employment of facial recognition software within existing surveillance systems. The mask, then, becomes a powerful countermeasure by hiding the wearer's identity not only from the gaze of the police officer and the looming camera, but also from the probing software and its impressive searching and archiving capacities. Veiled identity on the internet likewise thwarts the gaze of the NSA and cyber law enforcers, but technology is increasingly capable of circumventing attempts at anonymity, as has been recently revealed by the release of the Snowden documents.

Consider, for instance, Seattle city officials' debate to use $1.6 million federal grant money to purchase a city-wide surveillance system that includes state-of-the-art facial recognition software. This grant, available under the Department of Homeland Security's Urban Area Security

---

[56]Canadian TV News, "IBM's computer wins 'Jeopardy!' but... Toronto?" Feb 15, 2011.

[56] Alexis Madrigal, IBM's Watson Memorized the Entire 'Urban Dictionary,' Then His Overlords Had to Delete It, The Atlantic (http://www.theatlantic.com/technology/archive/2013/01/ibms-watson-memorized-the-entire-urban-dictionary-then-his-overlords-had-to-delete-it/267047/; Michal Lev-Ram, Teaching IBM's Watson the meaning of 'OMG', CNN Money (Jan. 7, 2013), http://tech.fortune.cnn.com/2013/01/07/ibm-watson-slang/.

[57] Margot Kaminski, Real Masks and Real Name Policies: Applying Anti-Mask Case Law to Anonymous Online Speech, 23 Fordham Intell. Prop. Media & Ent. L.J. 815, 818 (2013).

[58] *Id.*

Initiative (UASI), would allow for enhanced surveillance across the Emerald City: "Those Department of Homeland Security dollars would let the Seattle police pay for software that digitally scans surveillance camera footage and then tries to match images of the individuals caught on tape with any one of the 350,000-or-so people who have been photographed previously by King County, Washington law enforcement."[59] Privacy advocates are understandably concerned about the potential harm of such an intelligent system. Other cities across the U.S, such as San Diego and Daytona Beach, have already successfully fielded software-enhanced surveillance systems. Whereas now humans are involved in the processing and screening of the captured images, the potential exists for the system to become fully automated in the not-so-distant future. The proliferation of countermeasures--masked and otherwise--is inevitable given this exponential increase in surveillance scope and power.

c. Social Development and Inhibitor of Perfect Enforcement

Deterministic law enforcement systems with negligible transaction costs per attempt raises the possibility of perfect enforcement of law--as a relatively attainable goal if not a reality. In previous research we noted that any automated system must ultimately confront the question of "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?

If perfect enforcement is possible, that is, an ex ante decision for zero tolerance for legal violations, the temptation to embrace perfection is strong. As Jonathan Zittrain noted, "Few would choose to tolerate a murder, making it a good candidate for preemption through design, were that possible."[60] In exploring "impossibility structures" for enforcing various laws, Michael Rich noted, "Preventing drunk driving is a low hanging fruit when it comes to making criminal conduct impossible. The crime requires technology for its completion and is essentially defined by

[59] "Seattle considering $1.6 million facial recognition surveillance system," RT, 20 February 2014. http://rt.com/usa/seattle-surveillance-dhs-grant-943/.

[60] Jonathan Zittrain, The Future of the Internet and How To Stop It (2008).

a technological measurement. Thus, adapting automotive technology to incorporate the measurement of the driver's BAL is intuitive, if not technologically simple. Moreover, the harms resulting from drunk driving are severe and widespread, making the [this] more politically feasible than other potential impossibility structures."[61]

Yet we caution strongly against a goal of perfect enforcement, particularly through a zero tolerance strategy of automated ex post punishment. Even impossibility structures are problematic. As Rich noted with respect to drunk driving, "even...a straightforward impossibility structure gives rise to a tangle of constitutional, legal, and policy issues. These issues likely will only multiply as the targets of impossibility structures migrate outward from this natural origin of technology-related crimes."[62]

Rich continued, "a few areas seem ripe for the introduction of impossibility structures. The first would be other offenses involving the operation of automobiles, such as speeding, running a red light, or failing to wear a seat belt, that can result in death and serious bodily harm. From a technological standpoint, these should be easy to make impossible, and much of the technology needed to do so is already under development....Crimes that take place over the Internet, such as cyberbullying and cyberstalking, hacking, distributing child pornography, and theft of intellectual property, may also be amenable to impossibility structures in that they require technology for their commission. Although such crimes are disparate in how they are committed, and thus how they might be rendered impossible, they give rise to some common concerns."[63]

Inefficiency and indeterminism are perhaps most important in light of the long-term implications of automated law enforcement. Beyond specific circumstances where legal violations might be excused, certain countermeasures and the ability to break the law are necessary for social growth and stability. Preventing perfect enforcement through inefficiency and indeterminacy preserves this necessary breathing space for society to thrive. In short, a perfected system does not necessarily equate to perfect

---

[61] Michael L. Rich, Should We Make Crime Impossible?, 36 Harv. J.L. & Pub. Pol'y 795, 846-47 (2013).

[62] *Id.*

[63] *Id.* at 847-48.

justice in our humane understanding of the concept.

d. The Cost of Conservation and Benefits of Automation

However, there are incentives that work against this principle, including the desire to reduce the cost of law enforcement (or even profit from it). Red-light cameras produce considerable revenue for cities which employ them. For example, Philadelphia earned $17 million in fines from red-light cameras in 2013.[64] And these cameras never take a day off, never get sick, have no need for medical insurance, and will never draw a pension when they are replaced.

A conservation approach will often mean preserving police discretion, which has acknowledged harmful effects.[65] Elizabeth Joh has noted that "While harboring stereotypes is not a characteristic peculiar to the police, the authority delegated to the police makes stereotyping especially dangerous in that profession....As many have observed, the harms of this abuse of police discretion extend beyond the wasted time and annoyance of minority drivers. It is a demoralizing experience for an individual to be singled out primarily due to race or ethnicity. When repeated hundreds or thousands of times against members of a particular racial or ethnic group, however, these experiences alienate the entire affected community."[66]

Joh explored the value of automating away police discretion, stating "[t]he effects of a widespread automated enforcement regime would be dramatic."[67] As an example, Joh noted that "[t]raffic stops are often pretextual, a means for discovering evidence of other crimes unrelated to the justification for the initial stop. Thus, if traffic stops were eliminated through widespread automated enforcement, the nature of policing could be drastically different."[68] Thus, those applying the conversation theory to automated enforcement should be mindful of the advantages of

---

[64] Emily Babay, "Grace Period Ends for West Oak Lane Red-Light Cameras" Philly.com news site, http://www.philly.com/philly/news/Grace_period_ends_for_West_Oak_Lane_red-light_cameras.html (accessed 8 March 2014)

[65] Elizabeth E. Joh, Discretionless Policing: Technology and the Fourth Amendment, 95 Cal. L. Rev. 199, 208 (2007).

[66] *Id.*

[67] *Id.* at 202.

[68] *Id.*

eliminating discretion in certain areas or in certain ways.

VI. APPLYING THE THEORY

When this ideal system is decomposed into its component parts—the iterative steps of an automated legal process—room does of course exist at certain carefully-considered points for the precision, comprehensiveness, and rigor offered by automated technology. These questions then arise: Where in the process could or should automation trump human decision? To what extent can it go unchecked, if at all? And, how do we keep techno-creep from overriding what is necessarily a human-designed and governed system controlled through continually-regulated checks and balances?

The theory of governance for the automated enforcement of the law proposed here aims to answer these questions by focusing on reallocation of inefficiency and indeterminism. When one aspect of a law enforcement process (surveillance, analysis or action) is automated to increase efficiency and determinism, inefficiency and indeterminacy should generally be explicitly preserved elsewhere in the process to prevent harms from automation. Automating surveillance, analysis, or action makes it important to ensure that inefficiency or indeterminism is correspondingly preserved or introduced into the rest of the system to protect social welfare and prevent societal harm.

Where inefficiency and indeterminism are reallocated will entirely be dependent upon context, making this a general theory that is broadly applicable but in need of refinement in specific circumstances. Generally speaking, inefficiency and indeterminism can be conserved instantaneously at the point of surveillance, analysis, or action, or after the fact as a backstop.

Consider red light cameras. In Cyrus Farivar's in-depth exploration into red light cameras for *Ars Technica*, he investigated the installation and use of red light cameras by the commercial vendor Redflex in Modesto, California. He interviewed a police officer who reviewed the tickets, writing "Modesto Police officer Steve Silva, a 34-year police veteran who personally approves each ticket, denies about 20 percent of the cases that the Redflex system presents to him. 'I have to see a good violation,' he told me. 'If I can't identify the driver, the picture is too bad quality... sometimes there's a big vehicle blocking the limit line,

sometimes it's just real close, and I'll dismiss it because any doubt goes to the citizens, 100 percent.' Each morning when Silva arrives at work, Redflex usually has data on 40 cars that might have run the cameras. Line by line, day by day, Silva checks each entry on the Redflex website. Was the car over the line? Was the light red? Was the photo clear? Does the photo of the driver match DMV records? This task takes him a few painstaking hours each day to go through completely."[69]

In some instances, a regulatory response can be used to conserve inefficiency and indeterminacy. For example, Iowa City drafted a municipal ordinance that reads "The City shall not:...Use any automatic traffic surveillance system or device, automatic license plate recognition system or device, or domestic drone system or device for the enforcement of a qualified traffic law violation, unless a peace officer or Parking Enforcement Attendant is present at the scene, witnesses the event, and personally issues the ticket to the alleged violator at the time and location of the vehicle."[70] Iowa City embraced the conservation theory by injecting both inefficiency and indeterminacy not simply "in the loop," but at the geographic locus of surveillance, action, and enforcement.

CONCLUSION

As red-light cameras and radar speed traps have demonstrated, technology already exists for automating all parts of the Automated Law Enforcement process outlined in this article: surveillance, analysis and action. Fortunately, these examples impose only relatively minor civil penalties—they are a far cry from the fictional character, "Robocop." Failures in the system will be annoying to the innocent victim, but not catastrophic. However, robots are used in law enforcement applications, and as Knightscope's "K5" robot demonstrated, this is just the initial entry point into a potentially large and lucrative market. As we have seen, automation of surveillance has become widespread and automation of analysis and action are increasingly common. The improvements in

[69] Cyrus Farivar, Perfect Enforcement: On the Ground in the Red Light Camera Wars, Ars Technica (Dec. 16, 2013), http://arstechnica.com/tech-policy/2013/12/perfect-enforcement-on-the-ground-in-the-red-light-camera-wars/2/.

[70] Cyrus Farivar, Iowa City to ban red-light cameras, drones, and license plate readers too, Ars Technica (June 4, 2014), http://arstechnica.com/tech-policy/2013/06/iowa-city-to-ban-not-only-red-light-cameras-but-drones-license-plate-readers-too/.

[70] *Id.*

technology and the economic incentive to replace people with computers and robots form powerful arguments in favor of completely automated law enforcement systems. But arguments based on greater efficiency, reduced cost, and even reduced bias must be evaluated holistically, especially with regard to the overall effect of ubiquitous ALE systems on society.

This article examined the societal harms from over-reliance on automation at any stage in the ALE process, and especially the full automation of the entire process. Writers from Plato to Patrick Lin warn against rigid enforcement of laws that were never intended to cover every possible contingency in every situation.

This article proposed a theory to govern the automation of the law enforcement process. The theory states that whenever automation is introduced or expanded in one part of the ALE process in order to increase efficiency and determinacy, inefficiency and indeterminacy should generally be proportionally and explicitly preserved elsewhere in the process to prevent harms from automation. Although perhaps counterintuitive, we assert that indeterminacy and inefficiency are necessary and desirable components of any automated law enforcement process, not weaknesses in the system.

Once adopted, automated systems become entrenched and difficult to modify, so the initial design and implementation of ALE systems must preserve an adequate amount of indeterminacy and inefficiency. 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 place cost and efficiency above all other concerns.

***

APPENDIX: TABLES FOR AN EXPLICATED ALE TAXONOMY

Surveillance, whether conducted by human or machine, is a requisite first step of any law enforcement system. It is through this surveillance that violations of laws can be detected by government officials. However, while the cost of human police officers has continued to increase dramatically, the cost of automated surveillance continues to decline.[71]

In our model, surveillance is observation conducted by a law enforcement organization or its proxy, either directly or indirectly, of an individual's or group's activities. Table 1 provides representative examples of surveillance technology. Among these, there are several distinguishing characteristics. The first is the speed at which they operate. By this we mean, whether they are capable of feeding data consumable by machine processing or humans. Compared to machine processing, which can happen at millisecond speeds, human processing is inherently slow, taking minutes or hours, a difference of several orders of magnitude.

The second defining characteristic is that of a unique identifier of an object, such as a person, car, or cell phone. Some surveillance systems exploit a unique identifier, such as RFID or a GPS location. Others, like Closed Circuit Television require significant additional processing, to derive a unique identifier, which may suffer from high error rates.

For example, facial recognition technology is an active research area, but is currently not mature enough for widespread use. It is also heavily dependent upon a well-defined database of identities to perform a match. In contrast, recognition of license plate numbers from photos or video is largely a solved problem, as in the case of K5, because of the highly constrained problem - identify standardized alpha-numeric characters.

Because generalized facial recognition has not proved effective in practice, law enforcement is less likely to employ it to a significant degree,

[71] Ailsa Chang, "Crime-Ridden Camden To Dump City Police Force," National Public Radio - NPR.org, 6 December 2012, provides an excellent example in Camden, New Jersey's decision to eliminate its police force due to skyrocketing costs of employment benefits. The falling cost of surveillance is analyzed by Kevin S. Bankston and Ashkan Soltani in "Tiny Constables and the Cost of Surveillance: Making Cents Out of United States v. Jones, Yale Law School Journal Online, 9 January 2014. Bankston and Soltani illustrate that the human costs of law enforcement surveillance remain effectively constant at $50-$250/hour, while technological surveillance solutions quickly enjoy economies of scale, dropping costs several orders of magnitude over a period of 28 days.

at least in the near-term. Officials may require the use of complementary technologies to more easily identify subjects in an automated manner, such as RFID passports or compulsory biometrics enrollment.[72] An important aspect of unique identification is mapping an object (e.g. a car or cell phone) to a given individual. This would require corroborating evidence, such as that often used by red light camera systems that photograph the driver in addition to performing license plate recognition and a database look-up of the registered owner of the vehicle via motor vehicle department registries. This corroboration works to limit the chances of mistaken identity.

Our third characteristic is whether the technology remotely provides location information. This information is crucial for identifying whether an individual is present in a specific legal jurisdiction. Examples include GPS and cell phone surveillance systems. Of course, fixed location systems, or mobile systems such as police cars with known locations that are carrying surveillance technologies, also provide location data.

[72] Such use may be compulsory, see Pankaj Mishra, "Inside India's Aadhar, The World's Biggest Biometrics Database," Tech Crunch, 6 December 2013 and Charlie Osborne, "Student expelled for refusing to wear RFID tracking chip badge," ZDNet, 21 November 2013 or a near necessity, such as the E-ZPass system to avoid long lines at toll booths, see Kashmir Hill, "E-ZPasses Get Read All Over New York (Not Just At Toll Booths)," Forbes, 12 September 2013.

Table 1: Representative Surveillance Technologies

System	Speed	Unique ID	Location Info.	Notes
Closed Circuit Television (CCTV)	Human/ Machine	No	No	CCTV systems are in wide-spread use, but suffer from limitations in facial recognition software and typically require human analysis. However, character recognition, such as reading a license plate number, can be handled with today's machine processing technology, handling thousands of plates per minute.[73]
RFID	Machine	Yes	No	Widely used in RFID-enabled passports[74] and tracking of people.[75]
GPS	Machine	Yes	Yes	Can be used to track vehicles via attachable tracking devices[76] or humans via ankle or wrist bracelets,[77] among numerous other techniques.

[73] You are Being Tracked: How License Plate Readers are Being Used to Record Americans' Movements," American Civil Liberties Union. https://www.aclu.org/alpr, last accessed 15 January 2014.

[74] Anne Broache, "RFID passports arrive for Americans," CNET, 14 August 2006. See http://news.cnet.com/RFID-passports-arrive-for-Americans/2100-1028_3-6105534.html.

[75] Wendy Grossman, "Is UK college's RFID chip tracking of pupils an invasion of privacy?," The Guardian, 19 November 2013, http://www.theguardian.com/technology/2013/nov/19/college-rfid-chip-tracking-pupils-invasion-privacy.

[76] Unites States v. Jones, 132 S. Ct. 945 (2012).

[77] "The New Generation III Alcohol and Marijuana Sensing House Arrest Ankle Bracelet With Active GPS Is Now Available for only $3.50 per day!," HouseArrestBracelet.com.

[77] *Id.*

Barcode	Machine	Yes	No	Potential use in barcode license plates being explored.[78]
Cell Phone Intercept	Human/ Machine	Yes	Yes	Wiretaps have long allowed law enforcement intercept of telephonic communications, but automated processing of voice communication is not entirely a solved problem, particularly for low density languages. Cell phones, as broadcast devices, can also be geolocated.[79] Cell phones have also been remotely activated by law enforcement officials and used as a bugging device.[80]
Biometrics	Machine	Yes	No	Biometric measure characteristics of human subjects (such as retina, voice, gait, or hand geometry) and have proved accurate enough to identify registered subjects in practice.
Social Media	Machine /Human	Maybe	Maybe	Social media users publicly disclose significant sensitive information online, some of it exposing illegal activities, personal identities, and locations.[81]

[78] In 2012, the Virginia Department of Motor Vehicles Conducted a study exploring the use of RFID and barcode-based license plates, see http://leg2.state.va.us/DLS/h&sdocs.nsf/5c7ff392dd0ce64d85256ec400674ecb/db715763b38b14da85257ad200653d0d?OpenDocument.

[79] Ryan Gallagher, "FBI Files Unlock History Behind Cellphone Tracking Tool," Slate, 15 February 2013.

[80] Declan McCullagh and Anne Broache, "FBI taps cell phone mic as eavesdropping tool," CNET, 1 December 2006, http://news.cnet.com/2100-1029-6140191.html.

[81] "Surprise Guests at Teen Parties! Police Using New Tricks to Bust Teen Social Gatherings," ABC News, 10 January 2014. See http://abcnews.go.com/WNT/video/surprise-guests-teen-parties-police-tricks-bust-teen-21495591.

Table 2: Automated Means of Suspect Apprehension

Directive	Direct the subject to submit to apprehension.	Technically feasible today, but requires subject's compliance.
Trap the subject	Use electronically accessible elements of the environment to capture the subject.	Possible in limited circumstances, such as locking a victim in an automobile[82] or facility with electronic locks.
Trap and move the subject	Physically trap and use transportation device to move the subject.	Unrealistic with today's technology, but may be feasible by overriding programming of a near-future self-driving car.[83]
Disable subject	Forcibly subdue unwilling subject	Technically possible, but requires use of a non-lethal weapon.[84]

[82] Overriding a vehicle's locking system may require law enforcement backdoor access to control systems. Similar access would not be without precedent, consider Communications Assistance for Law Enforcement Act (CALEA), https://www.fcc.gov/encyclopedia/communications-assistance-law-enforcement-act which requires telecommunications carriers and manufactures to design their systems with surveillance capabilities. Absent official law enforcement backdoor options it may still be possible to break into automobile control systems. Recent research suggests such hacking is possible, see Andy Greenberg's "Hacker's Reveal Nasty New Car Attacks -- With Me Behind The Wheel," Forbes, 24 July 2013

[83] For a popular self-driving car example see Adam Fisher's "Inside Google's Quest to Popularize Self-Driving Cars," Popular Science, 18 September 2014. Self-driving cars are largely experimental and have not been subject to public scrutiny, this suggests security vulnerabilities may be present in fielded systems, especially early models. In addition, government officials could dictate CALEA like access to their control systems.

[84] To see a catalog of non-lethal weapons see the U.S. Department of Defense's Non-Lethal Weapons Program website, http://jnlwp.defense.gov/, last accessed 16 January 2014.

Disable vehicle	Forcibly disable subject's vehicle	Technically possible against many modern vehicles.[85]
Mental control of subject	Override or prevent subject's mental ability to control their actions.	Unrealistic, may be possible at some point in the mid to far-future.

[85] "Vehicle Disabling Systems," U.S. Department of Transportation Federal Motor Carrier Safety Administration, http://www.fmcsa.dot.gov/facts-research/systems-technology/product-guides/vehicle-disabling.htm, last accessed 16 January 2014. See also Victoria Woollaston, "Engineers Use Radio Beams to Remotely Disable Vehicle Engine," InfoWars, 4 December 2013. http://www.infowars.com/engineers-use-radio-beams-to-remotely-disable-vehicle-engine/, Keven Poulsen, "Hacker Disables More Than 100 Cars Remotely," Wired Threat Level Blog, 17 March 2010. http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/ and OnStar "Helping You Get Your Vehicle Back, Safely," https://www.onstar.com/web/portal/securityexplore?g=1, last accessed 16 January 2014.

Table 3: Potential technological advances and policy changes and their impact on future automated law enforcement.

Objective	**Analysis**	**Conclusion**
Identification[86]	Vehicle: Automobiles already possess unique identifiers which include license plates, Vehicle Identification Numbers (VIN), tire pressure sensor serial numbers,[87] RFID toll payment systems such as E-ZPass, and potentially Event Data Recorders (i.e. "black boxes") and subscription based integrated communication systems such as OnStar.[88]	Remote sensing and highly accurate identification of automobiles is possible now.[89]
	Human: People may be identified by something they are (biometrics), something they have (such as an identity card or subcutaneous RFID implant), or something they know (such as a PIN number or password).[90] Generalized identity systems require pairing with identity databases to map the given	Generalized automated identification of individuals from a distance and tied to existing identity registries such as driver's license databases has been attempted but is currently highly inaccurate. We anticipate technical breakthroughs in the next ten years that would allow such

[86] While identification of the subject is often an important part of an ALE system, it is not an absolute requirement. Punishment may be meted out without knowledge of the identity of the individual. Consider red-light cameras that ticket vehicle owners, not drivers based on motor vehicle records, and robots capable of killing intruders at the border of North and South Korea. See "South Korea deploys robot capable of killing intruders along border with North," The Telegraph, 13 July 2010.

[87] Mike Metzger. "Letting the Air Out of Tire Pressure Monitoring Systems," Defcon 18, 2010.

[88] Author Cory Doctorow eloquently describes automobiles as computers which humans ride inside. See Cory Doctorow, "Beyond the War on General Purpose Computing," Defcon 20, 2012.

[89] We believe the only thing preventing widespread employment of widespread license plate tracking systems is policy, not technology. See Ellen Nakashima and Josh Hicks, "Homeland Security is seeking a national license plate tracking system," Washington Post, 18 February 2014.

[90] These three aspects are a common methodology for performing identification of individuals. See Shon Harris, *CISSP Exam Guide*, 5ed., 2010, pp. 156-160.

	identifying information to a specific individual.[91]	techniques to be broadly employed in the context of ALE systems.[92]
Sensor Coverage and Accuracy	Sensors provide the eyes and ears of automated law enforcement systems. Improvements in sensor technology will provide increased resolution and transaction speed. Additional sensors provide coverage of new areas or more coverage of existing areas.	Government and privately owned sensors are already widespread in many areas and are sufficient to feed emerging automated law enforcement systems.[93] We anticipate coverage and accuracy will only increase over time, bolstered by the rise of sensors embedded in personal, household, and business technology.[94]
Access and Control	Fully automated law enforcement systems require access to sensor data, perhaps from third parties, in order to function. Access to identity and other forms of contextual information, such as digital maps, would provide for additional ALE system capability. Control includes law enforcement ability to not just access data, but to control sensors and electronic devices directly.	Law enforcement systems would be enhanced by increased ability to access other government and private sector data sources. Access to government data sources are limited by bureaucratic inertia and data sharing policies. Access to many private data sources requires navigating the friction of court oversight or administrative procedures. Removing or degrading these barriers, ideally with increased control over the devices themselves, is often a sought after goal by law enforcement officials due to a desire to

[91] As an example, India is building a nationwide database of identities based on biometric information. See Saritha Rai, "Why India's identity scheme is groundbreaking," BBC Online, 5 June 2012.

[92] We believe facial recognition systems combined with existing identity registries to be the most likely approach used by ALE systems. Accuracy could be rapidly improved by gathering biometric information from the populace, as is the case of India. Creation of such registries, however, raise important questions regarding records accuracy as well as data collection, destruction, and correction policies.

[93] For example the UK has approximately 5.9 million closed-circuit television cameras in the country and 750,000 in schools and hospitals. See David Barrett, "One surveillance camera for every 11 people in Britain, says CCTV survey," The Telegraph, 10 July 2013.

[94] Greg Conti, "Our Instrumented Lives: Sensors, Sensors, Everywhere," Defcon 18, 2010.

		increase the performance of their mission.[95]

[95] One example is an update to the Communications Assistance to Law Enforcement Act which would allow government access to online communications. See Mark Jaycox and Seth Schoen, "The Government Wants a Backdoor Into Your Online Communications," EFF Deep Links Blog, 22 May 2013. For an example of potential control see, Martin Robinson, "How police could soon be able to turn cars off remotely 'at the flick of a switch' under secret new EU plans," Mail Online, 30 January 2014.