2016

Inefficiently Automated Law Enforcement

Woodrow Hartzog
Boston University School of Law

Gregory Conti

John Nelson

Lisa A. Shay

INEFFICIENTLY AUTOMATED LAW ENFORCEMENT

Woodrow Hartzog,[*] *Gregory Conti,*[**] *John Nelson,*[***] *& Lisa A. Shay*[****]

2015 MICH. ST. L. REV. 1763

ABSTRACT

For some crimes the entire law enforcement process can now be automated. No humans are needed to detect the crime, identify the perpetrator, or impose punishment. While automated systems are cheap and efficient, governments and citizens must look beyond these obvious savings as manual labor is replaced by robots and computers.

Inefficiency and indeterminacy have significant value in automated law enforcement systems and should be preserved. Humans are inefficient, yet more capable of ethical and contextualized decision-making than automated systems. Inefficiency is also an effective safeguard against perfectly enforcing laws that were created with implicit assumptions of leniency and discretion. This Article introduces a theory of inefficiently automated law enforcement built around the idea that those introducing or increasing automation in one part of an automated law enforcement system should ensure that inefficiency and indeterminacy are preserved or increased in other parts of the system.

A theory of governance is critical for those who implement and administer automated law enforcement systems. Without it, systems become unmoored from ethics. Ironically, failure to responsibly automate law enforcement risks creating systems that actually undermine law and democracy. One way to preserve ethics in

* Associate Professor, Cumberland School of Law at Samford University; Affiliate Scholar, Center for Internet and Society at Stanford Law School.

** Associate Professor, Department of Electrical Engineering and Computer Science, U.S. Military Academy at West Point.

*** Assistant Professor, Department of English and Philosophy, U.S. Military Academy at West Point.

**** Associate Professor, Department of Electrical Engineering and Computer Science, U.S. Military Academy at West Point. The authors would like to thank Mary Anne Franks and the participants of the 2014 We Robot Conference for their feedback.

automated law enforcement systems is to preserve ethical actors, inefficiency and all.

TABLE OF CONTENTS

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.[1] *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.[2] In contrast to these popular

1. *See* KNIGHTSCOPE, http://www.knightscope.com/about.html (last visited Jan. 14, 2016).

2. Marco della Cava, *Change Agents: William Li's Robot Wants to Police You*, USA TODAY (Jan. 26, 2014, 12:16 AM), http://www.usatoday.com/story/tech/

cinema icons, however, Knightscope designed K5 for a specific law enforcement function—a hardwired and multi-wheeled Dirty Harry.[3] 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."[4]

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.[5] 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[6]), we must consider the legal implications and social impact of such an endeavor.[7] Addressing what he calls "robophobia," Knightscope CEO William Santana Li writes in his blog:

> [A]lthough it may be natural for folks to fear what lies ahead, it can [be more] 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 50%.[8]

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.[9]

2014/01/26/knightscope-k5-police-robot/4018047. 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. Masahiro Mori, *The Uncanny Valley*, IEEE ROBOTICS & AUTOMATION MAG., June 2012, at 98 (Karl F. MacDorman & Norri Kageki trans.).

3. *See* della Cava, *supra* note 2.

4. *Id.*

5. *Id.*

6. *Id.*

7. 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 Minimum Wage Laws in the States - January 1, 2016*, U.S. DEP'T OF LAB., http://www.dol.gov/whd/minwage/america.htm (last visited Jan. 14, 2016).

8. William Santana Li, *Why Are We Robophobic?*, KNIGHTSCOPE, http://knightscope.com/media.html (last visited Jan. 14, 2016).

9. 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

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 able to produce 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, the law enforcement process can be automated partially (and, in some cases, completely) from surveillance to punishment. 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.[10] If we want, inefficiency can be a thing of the past.

Yet, policy makers are unsure how to properly regulate automated systems.[11] 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

---

reality he is just developing a means to more efficiently "detect" crimes. Will the one result in the other?

10. *See* LISA SHAY ET AL., CONFRONTING AUTOMATED LAW ENFORCEMENT (2012), http://robots.law.miami.edu/wp-content/uploads/2012/01/Shay-EtAl-ConfrontingAutomatedLawEnf.pdf; *see also* Cyrus Farivar, *Perfect Enforcement: On the Ground in the Red Light Camera Wars*, ARS TECHNICA (Dec. 16, 2013, 9:00 PM) [hereinafter Farivar, *Perfect Enforcement*], http://arstechnica.com/tech-policy/2013/12/perfect-enforcement-on-the-ground-in-the-red-light-camera-wars; Cyrus Farivar, *Arizona Town Mounts Dozens of New License Plate Readers in Fake Cactuses*, ARS TECHNICA (May 8, 2015, 1:20 PM), http://arstechnica.com/tech-policy/2015/05/arizona-town-mounts-dozens-of-new-license-plate-readers-in-fake-cactuses.

11. For an example of the general uncertainty, see Farivar, *Perfect Enforcement*, *supra* note 10.

attempting to improve public welfare. 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 been haphazard and 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 theory of inefficiently automated law enforcement. 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 policy makers 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 of this Article, 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.

A theory of governance is critical for those who implement and administer automated law enforcement systems. Without it, systems become unmoored from ethics in the pursuit of efficiency. Failure to responsibly automate law enforcement risks creating systems that undermine law and democracy.

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.[12] We define automated law enforcement (ALE) 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.

At the highest level of abstraction, we define three major actors interacting in three major parts of a process. That model consists of (1) a subject, the person monitored who may or may not commit a crime; (2) law enforcement agencies that conduct surveillance, analysis, and enforcement; and (3) a judicial system that determines guilt and imposes punishment in certain cases. There are also feedback mechanisms that relay warnings and 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

12. *See* SHAY ET AL., *supra* note 10.

messier.[13] The three major components of automated law enforcement include (1) surveillance, (2) analysis (resulting in a determination of guilt or innocence), and (3) action (resulting in punishment or freedom). Automation anywhere in these three areas can trigger the considerations listed later in this Article.

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, and 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,[14] 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 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.[15] We also suggest the study of future candidate attributes, including more accurate time and location measurements, accuracy identification rates, and percent coverage of a given area.[16] Surveillance ends with the determination that a crime may have been committed. This determination and all evidence are passed to the next stage—analysis.

---

13. 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.

14. For one example of a smart home package, see AT&T DIGITAL LIFE, https://my-digitallife.att.com/learn (last visited Jan. 14, 2016). *See also* Tanya Bodell, *Why Google Bought Nest for $3.2 Billion*, ELEC. LIGHT & POWER (Feb. 25, 2014), http://www.elp.com/articles/print/volume-92/issue-1/columns/why-google-bought-nest-for-3-2-billion.html.

15. *See* SHAY ET AL., *supra* note 10.

16. *Id.*

The analysis stage consists of actions taken to identify the alleged perpetrator and 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").[17] 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 or shaming,[18] delivering a ticket, manual or automatic monitoring of probation (e.g., using a GPS bracelet), incarceration, or in extreme cases, execution.[19]

---

17. The NSA is a natural example. Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY (May 10, 2006, 10:38 AM), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm; Alexander Dryer, *How the NSA Does "Social Network Analysis*," SLATE (May 15, 2006, 6:33 PM), http://www.slate.com/articles/news_and_politics/explainer/2006/05/how_the_nsa_does_social_network_analysis.html. Other examples include Mudhakar Srivatsa & Mike Hicks, *Deanonymizing Mobility Traces: Using Social Networks as a Side-Channel*, *in* ACM SIGSAC, CSS'12: THE PROCEEDINGS OF THE 2012 ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 628 (2012), http://dl.acm.org/citation.cfm?id=2382262, and Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *in* IEEE COMPUTER SOCIETY, SP '08: PROCEEDINGS OF THE 2008 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 111 (2008), http://dl.acm.org/citation.cfm?id=1398064 (detailing the famous Netflix Prize dataset deanonymization). *See also* PREDPOL, https://www.predpol.com (last visited Jan. 14, 2016); Mark Gibbs, *Predicting Crime with Big Data . . . Welcome to "Minority Report" for Real*, NETWORK WORLD (Sept. 20, 2014, 12:01 PM), http://www.networkworld.com/article/2686051/big-data-business-intelligence/predicting-crime-with-big-data-welcome-to-minority-report-for-real.html.

18. *See* Lynn DeBruin, *'Shame' Punishments Increasing: Judges Order Ponytail Cutting, Sleeping in Doghouse, Wearing Embarrassing Signs*, HUFFINGTON POST (June 26, 2012, 9:59 AM), http://www.huffingtonpost.com/2012/06/26/shame-punishments-judge-orders-ponytail_n_1627010.html. Consider also the use of offender registries, such as the National Sex Offender Database, DRU SJODIN NAT'L SEX OFFENDER PUB. WEBSITE, http://www.nsopr.gov (last visited Jan. 14, 2016), and online arrest search systems, for example BROWARD SHERIFF'S OFF., https://www.sheriff.org/apps/arrest (last visited Jan. 14, 2016).

19. *See* Ralph Kirkland Gable & Robert S. Gable, *Electronic Monitoring: Positive Intervention Strategies*, 69 FED. PROB. J. 21 (2005), https://www.ncjrs.gov/App/publications/abstract.aspx?ID=210867. For a detailed walkthrough including

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, 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.[20]

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) might trigger on a car crossing the intersection when the light is red, which would then look up the license plate number to find the address of the registered owner (automated analysis) and then print and mail a ticket to the registered owner's address (automated action).

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. However, 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.

---

discussion of the ticket (notice of liability), see *City of Yonkers Red Light Camera Safety Program*, CITY OF YONKERS, NY, http://www.cityofyonkers.com/government/departments/parking-violations-bureau/red-light-cameras-how-it-works-locations (last visited Jan. 14, 2016). To be fair, much of the automation occurs at the lower end of the scale. However, autonomous weapon systems are technically feasible and examples have been in use since the Cold War, so execution is possible (more or less) to automate. *See* Michael Carl Haas, *Autonomous Weapon Systems: The Military's Smartest Toys?*, NAT'L INT., http://nationalinterest.org/feature/autonomous-weapon-systems-the-militarys-smartest-toys-11708 (last visited Jan. 14, 2016).

20. KIMBERLY ECCLES ET AL., TRANSP. RESEARCH BD. OF THE NAT'L ACADS., NCHRP REPORT 729: AUTOMATED ENFORCEMENT FOR SPEEDING AND RED LIGHT RUNNING 3-4 (2012), http://onlinepubs.trb.org/onlinepubs/nchrp/nchrp_rpt_729.pdf.

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 Engineers International's Levels of Driving Automation for On-Road Vehicles.[21] From Level 0 (No Automation) and Level 1 (Driver Assistance) to Level 4 (High Automation) and Level 5 (Full Automation), the model plots four different 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).[22]

Levels of automation might look similar for surveillance, analysis, or enforcement of traffic laws. Levels of automation could be based on variables such as whether humans conduct surveillance, process or analyze data, or review decisions; whether any of these actions are at fully automated machine speed or slower based on degrees of human involvement; 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.[23] Subjects or their supporters may employ a wide range of countermeasures, especially technical and policy countermeasures that reduce efficiency of a system.[24] Technical countermeasures would strive to deny, degrade, deceive, corrupt, usurp, or destroy sensing, networking, storage, and processing capabilities of the system.[25] Policy countermeasures undermine the legal authorities, which allow use of the system by legitimate entities.[26]

---

21. *Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems*, SAE INT'L, http://standards.sae.org/j3016_201401/ (last visited Jan. 14, 2016).

22. *Id.*

23. Cyrus Farivar, *Iowa City to Ban Red-Light Cameras, Drones, and License Plate Readers Too*, ARS TECHNICA (June 4, 2013, 7:45 PM), http://arstechnica.com/tech-policy/2013/06/iowa-city-to-ban-not-only-red-light-cameras-but-drones-license-plate-readers-too/.

24. Lisa A. Shay et al., *Beyond Sunglasses and Spray Paint: A Taxonomy of Surveillance Countermeasures*, *in* IEEE, 2013 IEEE INTERNATIONAL SYMPOSIUM ON TECHNOLOGY AND SOCIETY (ISTAS) 191 (2013).

25. Noah Shachtman, *'Degrade, Disrupt, Deceive': U.S. Talks Openly About Hacking Foes*, WIRED (Aug. 28, 2012, 5:00 AM), http://www.wired.com/dangerroom/2012/08/degrade-disrupt-deceive/.

26. *See* Rachel Weiner, *Cuccinelli to Work on NSA Class-Action Lawsuit*, WASH. POST (Jan. 6, 2014), http://www.washingtonpost.com/local/dc-politics/

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 that 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 flags a significantly higher number of legal violations, should enforcement actions also be automated in order to avoid a systemic apathy to identified crimes? In the Part below, we explore potential social costs of automation at each point in an automated law enforcement system as well as holistically.

II. SOCIAL COSTS OF AUTOMATED LAW ENFORCEMENT SYSTEMS

A. 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" have always raised concern at the potential Orwellian turn of automated law enforcement in our everyday lives; these voices normally have fallen on society's margins, however, and rarely have they voiced a collective sentiment.[27] This passive acceptance seems to have

---

cuccinelli-to-work-on-nsa-class-action-lawsuit/2014/01/06/1832ee22-7720-11e3-8963-b4b654bcc9b2_story.html; James Warren, *White House Task Force Report on NSA Spying Recommends Sweeping Reforms*, N.Y. DAILY NEWS (Dec. 18, 2013, 6:00 PM), http://www.nydailynews.com/news/politics/white-house-release-report-reforms-nsa-spying-article-1.1551792.

27. Relatively unknown groups such as the National Motorists Association provide information for red-light camera activists. *Red-Light Cameras*, NAT'L MOTORISTS ASS'N, https://www.motorists.org/issues/red-light-cameras/ (last visited Jan. 14, 2016). *About the National Motorists Association*, NAT'L MOTORISTS ASS'N, https://www.motorists.org/about/ (last visited Jan. 14, 2016). One recent success occurred in Arlington, Texas, where activists succeeded in collecting more than 11,000 signatures to force city leaders to put the issue on the ballot. *See* Anna A. Tinsley, *Red-Light Cameras May Soon Be Shut Off in Arlington*, THE STAR-TELEGRAM (May 9, 2015), http://www.star-telegram.com/news/politics-government/election/article20602842.html. Fifty-nine percent of voters supported banning the cameras. *See id.*; *see also Texas Tea Party Takes On Red Light Cameras, and $18-*

changed recently with the intense media focus on Edward Snowden's leaked classified information about the National Security Agency's global automated surveillance system.[28] 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 United Kingdom'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.[29] 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.[30]

This automated surveillance, ostensibly conducted in the interest of national security, jeopardizes the privacy of millions of citizens across the globe.[31] 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.

U.S. Director of National Intelligence, James Clapper, equated the controversial archiving of private Internet communication to the

---

an-Hour 'Supporters,*'* FOX NEWS (May 6, 2015), http://www.foxnews.com/politics/2015/05/06/texas-tea-party-leader-fights-for-amendment-that-would-ban-red-light-traffic/.

28. *Edward Snowden and the National Security Agency Leak*, WASH. POST, https://www.washingtonpost.com/world/national-security/edward-snowden-and-the-national-security-agency-leak/0033078e-d2c6-11e2-9f1a-1a7cdee20287_topic.html (last visited Jan. 14, 2016).

29. Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, THE GUARDIAN (Feb. 28, 2014, 5:31 PM), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo.

30. *Id.*

31. Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934 (2013).

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.[32] "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."[33]

B. 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 the 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.[34]

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 that receive neither benefit nor harm from a law, whether just or

32. Bruce Schneier, *NSA Robots Are 'Collecting' Your Data, Too, and They're Getting Away with It*, THE GUARDIAN (Feb. 27, 2014, 9:39 AM), http://www.theguardian.com/commentisfree/2014/feb/27/nsa-robots-algorithm-surveillance-bruce-schneier.

33. *Id.*

34. PLATO, THE BEING OF THE BEAUTIFUL: PLATO'S *THEAETETUS*, *SOPHIST*, AND *STATESMAN* 294e (Seth Benardete trans., 1984).

unjust or whether applied fairly or unfairly.[35] 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 automated law enforcement 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.

C. 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.[36] 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:

> [F]ar 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.[37]

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

35. LISA SHAY ET AL., DO ROBOTS DREAM OF ELECTRIC LAWS?: AN EXPERIMENT IN THE LAW AS ALGORITHM 25 (2013), http://conferences.law.stanford.edu/werobot/wp-content/uploads/sites/29/2013/04/Shay-et-al_Lisa.pdf.

36. *See* Christina M. Mulligan, *Perfect Enforcement of Law: When to Limit and When to Use Technology*, 14 RICH. J.L. & TECH., Spring 2008, at 1, http://law.richmond.edu/jolt/v14i4/article13.pdf.

37. SLAVOJ ŽIŽEK, THE PLAGUE OF FANTASIES 77 (1997).

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 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—is, of course, our desire and, indeed, our innate need to *choose to obey*.[38] 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.[39] 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.[40] In his highly influential essay "Civil Disobedience," Henry David Thoreau writes, "[I]f [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."[41] 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

38. *See* Ian R. Kerr, *Digital Locks and the Automation of Virtue*, *in* "RADICAL EXTREMISM" TO "BALANCED COPYRIGHT": CANADIAN COPYRIGHT AND THE DIGITAL AGENDA 247 (Michael Geist ed., 2010).

39. BRUCE SCHNEIER, LIARS AND OUTLIERS: ENABLING THE TRUST THAT SOCIETY NEEDS TO THRIVE (2012).

40. *See* MAHATMA GANDHI, THE ESSENTIAL GANDHI: AN ANTHOLOGY OF HIS WRITINGS ON HIS LIFE, WORK, AND IDEAS (Louis Fischer ed., 2002); MARTIN LUTHER KING, JR., THE AUTOBIOGRAPHY OF MARTIN LUTHER KING, JR. (Clayborne Carson ed., 2001).

41. HENRY DAVID THOREAU, CIVIL DISOBEDIENCE AND OTHER ESSAYS 9 (Digireads.com 2005).

by the totality of our brave new system, an unchallengeable "machine of government."[42] 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 related abuse of discretion harms.[43] 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. 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 THEORY OF INEFFICIENTLY 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

42. GEORGE ORWELL, 1984 (Signet Classics 1961) (1949).

43. *See* Elizabeth Joh, *Discretionless Policing: Technology and the Fourth Amendment*, 95 CAL. L. REV. 199, 232-33 (2007).

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.[44] 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. 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,[45] 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.[46] Manual surveillance, analysis, and enforcement require manpower, money, and time. Automation can be centralized, cheap, and virtually instantaneous. Second, automated systems are

---

44. *See* SHAY ET AL., *supra* note 10; SHAY ET AL., *supra* note 35.

45. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249 (2008).

The development of highly efficient automated law enforcement systems without corresponding inefficiencies afforded to due process threatens subjects' abilities 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. Janie Emaus, *Help! I'm Stuck in Voicemail Hell*, HUFFINGTON POST, (Aug. 30, 2013, 5:15 AM), http://www.huffingtonpost.com/janie-emaus/help-im-stuck-in-voicemai_b_3481364.html; *see also* DIAL A HUMAN, http://www.dialahuman.com/ (last visited Jan. 14, 2016).

46. Maggie Clark, *Red-Light Cameras Generate Revenue, Controversy*, USA TODAY (Oct. 15, 2013, 3:07 PM), http://www.usatoday.com/story/news/nation/2013/10/15/stateline-red-light-cameras/2986577/ (discussing the significant efficiency and revenue).

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.[47] 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.[48] Although this theory might seem regressive, both inefficiency and indeterminacy humanize the automated law enforcement process and 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.

A. Inefficiency

Law enforcement is, by and large, inefficient. It costs time and resources for most crimes to be detected, investigated, prosecuted, and punished. These costs can burden law enforcement. 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

47. *See generally* Harry Surden, *The Variable Determinacy Thesis*, 12 COLUM. SCI. & TECH. L. REV. 1 (2011).

48. For an exploration of the absurd results, from developing code to enforcing laws that failed to contemplate de minimis transaction costs for enforcement, see SHAY ET AL., *supra* note 35.

capture a vehicle's instantaneous speed as it passes by. If this speed crosses the officer's own particular enforcement threshold, the police officer 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 500 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.

1. *Human Intervention in "The Loop"*

The process of law enforcement has historically relied heavily on human police, investigators, judicial officials, and correctional 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),[49] 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 systems that include

49. *See* Christopher K. Walker, *Red-Light Cameras: How States Jeopardize Safety by Manipulating Yellow-Light Intervals to Earn a Quick Buck*, 7 J. LEGAL TECH. RISK MGMT. 222, 243, 259 (2014). These systems can then be productized and sold. As an example, see *Photo Enforcement Systems*, XEROX, http://services.xerox.com/transportation-solutions/transportation-management-systems/photo-enforcement/enus.html (last visited Jan. 14, 2016).

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.[50] Little has been done, however, to assess the social impact of human absence from the process.

2. *Countermeasures*

We define countermeasures to mean actions taken in response to perceived threats from automation of some aspect of law enforcement.[51] 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.[52] Few would tolerate receiving 500 tickets during a one-hour trip, as our study indicated.[53] Evidence already shows that an overzealous approach to law enforcement encourages individuals and organizations to take (sometimes illegal) countermeasures.[54]

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.[55] 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, or 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

50. ECCLES ET AL., *supra* note 20, at 37, 43.
51. Shay et al., *supra* note 24, at 191.
52. SHAY ET AL., *supra* note 35.
53. *See id.* at 17-20.
54. *See* Shay et al., *supra* note 24, at 191.
55. Kim Zetter, *German Activists Punch Out Big Brother's Eyes*, WIRED (Jan. 31, 2013, 5:22 PM), http://www.wired.com/2013/01/camover-targets-cctvs/.

> ideological belief or 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.[56]

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 are 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 (DMCA) ban on circumventing technological copyright controls.[57] The DMCA attempts to mandate respect for digital rights management (DRM) by instituting anticircumvention provisions into U.S. copyright law.[58] These provisions are, "in effect, a ban on the act of circumventing or trafficking in devices that circumvent certain DRM systems."[59]

---

56. Elizabeth E. Joh, *Privacy Protests: Surveillance Evasion and Fourth Amendment Suspicion*, 55 ARIZ. L. REV. 997, 1000-01 (2013) (footnotes omitted).

57. 17 U.S.C. §§ 1201-05 (2012).

58. *See id.*; Mulligan, *supra* note 36, at 26-27 (discussing digital rights management).

59. Woodrow Neal Hartzog, *Falling on Deaf Ears: Is the "Fail-Safe" Triennial Exemption Provision in the Digital Millennium Copyright Act Effective in Protecting Fair Use?*, 12 J. INTELL. PROP. L. 309, 312-13 (2005).

In some instances, countermeasures should even be explicitly allowed.[60] 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.[61]

3. *Technical and Procedural Governors*

Technical governors are mechanisms created by technologies or regulation that reduce the capability of a sub-system within the automated law enforcement framework.[62] For instance, law enforcement officials must follow the appropriate authorization process before they can install a wiretap.[63] 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.[64] Again, the limitation on tracking cars is due to a constraint imposed by the law, not a limitation of the technology.

Professor Paul Ohm has proposed that privacy and transparency goals can be simultaneously achieved by making information "hard but possible" to obtain.[65] Harry Surden has likewise recognized the value in high transactional costs to protect privacy, noting that "[s]ociety 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 in aggregating and analyzing large amounts of information to effectively protect

60. For example, being able to use a mask to thwart facial recognition technologies or a pseudonym to protect identity should be preserved in some settings to foster First Amendment values. *See* 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 (2013); *see also* 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].").

61. *See* 18 U.S.C. § 1030 (2012).

62. *See* SHAY ET AL., *supra* note 10.

63. *Id.* §§ 2510-22.

64. *See* United States v. Jones, 132 S. Ct. 945, 949 (2012).

65. Paul Ohm, *Good Enough Privacy*, 2008 U. CHI. LEGAL F. 1, 63.

anonymity."[66] 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.

B. 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.[67] 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 restricted area.[68]

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

66. Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605, 1605 (2007).

67. FRANK VAHID, DIGITAL DESIGN WITH RTL DESIGN, VHDL, AND VERILOG 142 (2d ed. 2011).

68. SHAY ET AL., *supra* note 10, at 38 (footnotes omitted).

and intuition.[69] 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, programmers 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 those outcomes constitute a deviation from predictable standard protocol.

In practical terms, if automation is increased at one point in the automated law enforcement 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.

C. The Benefits of Conservation

1. *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:

---

69. "Indeterminacy" is a relatively common literary term (at least for specialists in literature). *See* CHRIS BALDICK, *Indeterminacy*, THE OXFORD DICTIONARY OF LITERARY TERMS (3d ed. 2008).

> 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 and lead to error. Potholes develop, trees fall across roads, 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.[70]

We noted that "[a] robotic car . . . might slide through a stop sign due to snow and possibly record that it did stop because the wheels stopped turning. Or the car might drive 15 MPH on a freeway because a repair crew forgot to take down an RFID-enabled construction zone sign."[71]

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 because they are programmed to obey the law and avoid crashes?[72]

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.[73]

According to Lin,

> [T]here are important differences between humans and machines that could warrant a stricter test. For one thing, we're reasonably confident that

70. SHAY ET AL., *supra* note 35, at 25.

71. *Id.*

72. Patrick Lin, *The Ethics of Autonomous Cars*, THE ATLANTIC (Oct. 8, 2013), http://www.theatlantic.com/technology/archive/2013/10/the-ethics-of-autonomous-cars/280360/.

73. *Id.*

> 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.[74]

Lin also sees the potential problem from automating legal compliance, stating:

> [B]ecause 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.[75]

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.[76] 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.

2. *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 potential to commit egregious privacy violations under the Fourth Amendment, electronic surveillance regimes, and other privacy laws.[77]

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

74. *Id.*

75. *Id.*

76. *See generally* Farivar, *Perfect Enforcement*, *supra* note 10; Matt Richtel & Conor Dougherty, *Google's Driverless Cars Run into Problem: Cars with Drivers*, N.Y. TIMES (Sept. 1, 2015), http://www.nytimes.com/2015/09/02/ technology/ personaltech/google-says-its-not-the-driverless-cars-fault-its-other-drivers.html?_r=0.

77. SHAY ET AL., *supra* note 10, at 34 (citing Kenneth A. Bamberger, *Technologies of Compliance: Risk and Regulation in a Digital Age*, 88 TEX. L. REV. 669 (2010); Citron, *supra* note 45.

> 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.[78]

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.[79] 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 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.[80]

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

---

78. Citron, *supra* note 45, at 1271-72 (citing Raja Parasuraman & Christopher A. Miller, *Trust and Etiquette in High-Criticality Automated Systems*, 47 COMM. ACM 51, 52 (2004); Linda J. Skitka et al., *Automation Bias and Errors: Are Crews Better than Individuals?*, 10 INT'L J. AVIATION PSYCHOL. 85, 86 (2000)).

79. 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 S. Rubinstein, *Big Data: The End of Privacy or a New Beginning?*, 3 INT'L DATA PRIVACY L. 74, 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 . . . .").

80. *IBM's Computer Wins 'Jeopardy!' but . . . Toronto?*, CTV NEWS (Feb. 15, 2011, 11:15 PM), http://www.ctvnews.ca/ibm-s-computer-wins-jeopardy-but-toronto-1.608022; Alexis C. Madrigal, *IBM's Watson Memorized the Entire 'Urban Dictionary,' Then His Overlords Had to Delete It*, THE ATLANTIC (Jan. 10, 2013), 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,'* FORTUNE (Jan. 7, 2013, 10:00 AM), http://fortune.com/2013/01/07/teaching-ibms-watson-the-meaning-of-omg/.

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?"[81] 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."[82]

Kaminski reaches a similar conclusion with respect to real-name policies.[83] The power of anonymity has grown exponentially over the past decade with the government employment of facial recognition software within existing surveillance systems.[84] 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.[85]

Consider, for instance, Seattle city officials' debate to use $1.6 million of federal grant money to purchase a city-wide surveillance system that includes state-of-the-art facial recognition software.[86] This grant, available under the Department of Homeland Security's Urban Area Security Initiative, 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.[87]

---

81. Kaminski, *supra* note 60, at 818.

82. *Id.*

83. These are policies that websites like Facebook place in their terms of use agreements that prohibit users from using a pseudonym or require them to use their legal name. *Id.* at 879.

84. *Id.* at 890.

85. *See generally* GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014).

86. *Seattle Considering $1.6 Million Facial Recognition Surveillance System*, RT (Feb. 20, 2014, 6:37 PM), http://www.rt.com/usa/seattle-surveillance-dhs-grant-943.

87. *Id.*

Privacy advocates are understandably concerned about the potential harm of such an intelligent system.[88] Other cities across the U.S., such as San Diego and Daytona Beach, have already successfully fielded software-enhanced surveillance systems.[89] 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.

3. *Social Development and Inhibitor of Perfect Enforcement*

Deterministic law enforcement systems with negligible transaction costs per attempt raise 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: "How many violations of the law should be explicitly forgiven or ignored?"[90] 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."[91] 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 a technological measurement. Thus, adapting automotive technology to incorporate the measurement of

88. *Id.*

89. *See* Dave Maass, *Going to San Diego Comic-Con? Put On Your Mask for the Surveillance Camera Network*, ELEC. FRONTIER FOUND. (July 22, 2014), https://www.eff.org/deeplinks/2014/07/operation-secure-san-diego; THE CITY OF DAYTONA BEACH, OFFICE OF THE PURCHASING AGENT, REQUEST FOR PROPOSALS: INVITATION 10 (2014), http://purchasing.codb.us/documents/RFP%200415-3630%20Video%20Surveillance.pdf.

90. *See* SHAY ET AL., *supra* note 35.

91. JONATHAN ZITTRAIN, THE FUTURE OF THE INTERNET AND HOW TO STOP IT 120 (2008).

> the driver's BAL is intuitive, if not technologically simple. Moreover, the harms resulting from drunk driving are severe and widespread, making [this] more politically feasible than other potential impossibility structures.[92]

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, "[E]ven . . . 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."[93] 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.[94]

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 justice in our humane understanding of the concept.

4. *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

92. Michael L. Rich, *Should We Make Crime Impossible?*, 36 HARV. J.L. & PUB. POL'Y 795, 846-47 (2013).

93. *Id.* at 847.

94. *Id.*

cities that employ them.[95] For example, Philadelphia earned $17 million in fines from red-light cameras in 2013.[96] 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 problems.[97] Elizabeth Joh has noted:

> 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.[98]

Joh explored the value of automating away police discretion, stating that "the effects of a widespread automated enforcement regime would be dramatic."[99] 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."[100] Those applying the conservation theory to automated enforcement should be mindful of the advantages of eliminating discretion in certain areas or in certain ways.

D. 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

---

95. *See* Walker, *supra* note 49, at 243; Clark, *supra* note 46.

96. Emily Babay, *Grace Period Ends for West Oak Lane Red-Light Cameras*, PHILLY.COM (Mar. 6, 2014, 6:24 AM), http://www.philly.com/philly/news/Grace_period_ends_for_West_Oak_Lane_red-light_cameras.html.

97. Joh, *supra* note 43, at 208.

98. *Id.* at 208, 211 (footnote omitted).

99. *Id.* at 202.

100. *Id.* (footnote omitted).

or should automation trump human decision? To what extent can it go unchecked, if at all? And how do we keep techno-creep—our slow but steady relinquishment of control to technology[101]—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 in the appeals process, for example.

Consider red-light cameras. In journalist 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.[102] 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

101. *See generally* Thomas P. Keenan, TECHNO CREEP: THE SURRENDER OF PRIVACY AND THE CAPITALIZATION OF INTIMACY (2014).

102. Farivar, *Perfect Enforcement*, *supra* note 10.

> 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.[103]

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.[104]

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 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 automated law enforcement systems on society.

This Article examined the societal harms from overreliance on automation at any stage in the automated law enforcement process and especially the full automation of the entire process. Writers from

---

103. *Id.*
104. Farivar, *supra* note 23.

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 automated law enforcement 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 automated law enforcement 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.