9-2017

Digital Surveillance and Preventive Policing

Manuel A. Utset
Florida State University College of Law

ARTICLE CONTENTS

Digital Surveillance and Preventive Policing

MANUEL A. UTSET*

INTRODUCTION

Modern police departments use "Big Data" technologies[1] to collect digital information about almost every aspect of our public and private lives,[2] storing it in large data banks,[3] and processing it, as needed, to extract actionable knowledge,[4] used to solve and prevent crimes.[5] For example, police departments routinely feed data about past crimes into sophisticated learning algorithms to help them "predict" the timing and location of future crimes.[6] This Article refers to law enforcement's use of

---

* William & Catherine VanDercreek Professor and Associate Dean for Academic Affairs, Florida State University College of Law. I would like to thank Richard Borden, Hillary Greene, Mariko Hirose, Justin Hurwitz, and Harvey Rishikof for their comments.

[1] "Big Data" is a catchall term used to refer to a variety of tools and methods for acquiring, storing, and processing large data sets to extract useful knowledge. *See* Andrea De Mauro, Marco Greco, & Michele Grimaldi, *What is Big Data? A Consensual Definition and a Review of Key Research Topics*, 13 AIP CONFERENCE PROCEEDINGS 97, 101–03 (2016) (setting forth various uses of the term Big Data); Andrew McAfee & Erik Brynjolfsson, *Big Data The Management Revolution*, HARV. BUS. REV. 60, 62–63 (October 2012) (describing advances in using large datasets to make business decisions, including advancements in storage capacity, real-time capture of large amounts of data, and increase in variety of data available).

[2] *See, e.g.*, Susan Landau, *Making Sense from Snowden What's Significant in the NSA Surveillance Revelations*, IEEE SEC. & PRIVACY 54, 57–59 (July–August 2013) (describing collection of metadata and actual content data by U.S. intelligence agencies); Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327, 353–69 (2015) (describing growth in collection and use of large volume of data by police departments); Elizabeth E. Joh, *Policing by Numbers Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 42–55 (2014) (describing various ways in which police use surveillance data).

[3] *See* Mél Hogan and Tamara Shepherd, *Information Ownership and Materiality in an Age of Big Data Surveillance*, 5 J. INFO. POL. 6, 9–11 (2015) (discussing the NSA's Utah Data Center, a 100,000 square-foot facility built to store surveillance intercepts).

[4] *See infra* Section II.G. (discussing machine learning algorithms used to extract patterns from big data sets and make predictions).

[5] Growing concerns about terrorism have led intelligence agencies and law enforcement to invest heavily in surveillance technologies aimed at preventing terrorist attacks. *See e.g.*, David Lyon, *Surveillance, Snowden, and Big Data Capacities, Consequences, Critique*, BIG DATA & SOC. 1, 2 (2014) (stating that urban policing and anti-terrorism, along with consumer marketing and health care are four main areas that make use of Big Data).

[6] *See* Ric Simmons, *Quantifying Criminal Procedure How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 952–68 (2016) (providing a detailed overview of how predictive policing algorithms work). For example, PredPol, a popular machine learning program for "predictive policing," uses historical data about crime type, crime location, and crime date and time, to provide "crime predictions for the places and times that crimes are most likely

Big Data as "digital policing."

With the continued growth of digital policing, policymakers and commentators have focused their attention on a plethora of privacy and criminal procedure issues.[7] But digital policing has other, less obvious, effects on the criminal justice system: on police practices, deterrence policy, and substantive criminal law. These collateral effects of digital policing, largely overlooked by commentators and policymakers, are the focus of this Article.

Digital policing helps reduce the criminal justice system's overall complexity, creating economies of scale in law enforcement and allowing police departments to better deploy their limited resources.[8] After a crime has occurred, digital policing gives the police quick access to evidence from multiple sources,[9] including repositories of historical data, helping them to identify offenders and make arrests.

Increased worries about terrorist attacks have led policymakers to focus increasingly on preventing crimes rather than solving them after the fact. This shift in enforcement focus, which we will refer to as "preventive policing," has been aided and complicated by the proliferation of information available to law enforcement. The shift towards preventive policing has implications for substantive criminal law, since it leads the police to give greater attention to inchoate crimes, such as criminal attempt, conspiracy, and solicitation, and increases the risk of inappropriate entrapment.

Section I describes the general economics approach to criminal law, which posits that offenders are rational actors and that lawmakers design legal rules and punishment schemes so as to maximize social welfare. The Article adopts this general approach to analyzing criminal misconduct, enforcement policies, and deterrence schemes.

Section II begins by examining the complexity of the criminal justice

---

to occur." *See How PredPol Works We Provide Guidance on Where and When to Patrol*, PREDPOL, http://www.predpol.com/how-predpol-works/.

[7] *See e.g.*, Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317 (2008); Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CAL. L. REV. 805 (2016); David Alan Sklansky, *Too Much Information How Not to Think About Privacy and the Fourth Amendment*, 102 CAL. L. REV. 1069 (2014); Ferguson, *supra* note 2; Joh, *supra* note 2.

[8] Los Angeles Police Chief Charlie Beck's testimonial on the website of the predictive policing software company, PredPol, makes the point: "I'm not going to get more money. I'm not going to get more cops. I have to be better at using what I have, and that's what predictive policing is about. . . . If this old street cop can change the way that he thinks about this stuff, then I know that my [officers] can do the same." PREDPOL, http://www.predpol.com/.

[9] For example, during the investigation of a crime on a subway platform, the police may review CCTV camera footage. *See* Manal Al-Rawahi & E.A. Edirisinghe, *Video Forensics in Cloud Computing The Challenges & Recommendations*, 3 J. INFO. SCI. & COMPUTING TECH. 201, 205–07 (2015) (providing an overview of practical and legal issues in using CCTV footage for evidentiary purposes).

process. It then shows that digital policing techniques help reduce the complexity of law enforcement and create economies of scale. It continues by showing that ex ante preventive policing is a more complex undertaking than ex post investigative policing. In particular, by reducing the complexity of law enforcement, digital policing has allowed society to shift its enforcement focus from investigative policing to preventive policing, which is a much more complex undertaking. Section II concludes by discussing the various social costs and benefits associated with digital policing.

Section III examines how digital policing affects deterrence policy. Given its economies of scale, digital policing allows police to increase their ex ante monitoring and ex post investigations. By increasing the efficiency of law enforcement, digital policing allows authorities to make more arrests and get more convictions. Digital policing, in short, allows society to increase the expected sanctions of crimes. This can lead to inefficient overdeterrence. This Section first shows that digital policing will increase the overall deterrence of offenders. It then examines a well-known puzzle in the economic literature—the fact that repeat offenders are punished more harshly—and shows that the proliferation of digital and preventive policing should lead to the opposite conclusion: that gross sanctions for repeat offenders should be *lower*. But society has failed to adjust gross criminal sanctions to account for the widespread adoption of digital policing. This Section continues by providing various explanations for the stickiness of gross sanctions. The Section also describes how digital policing can affect the likelihood of wrongful acquittals and wrongful convictions.

Section IV develops a number of other criminal law implications of digital and preventive policing. It examines the interaction between preventive policing and inchoate crimes, such as criminal attempt, conspiracy, and solicitation, as well as its relationship with the entrapment defense. It also examines the implications of digital and preventive policing on police searches, plea bargains, and police corruption.

I. THE LAW AND ECONOMICS APPROACH TO SUBSTANTIVE CRIMINAL LAW

This Section describes the general economics approach to criminal law. It begins by describing the way that rational offenders make decisions about whether to violate the law. It then provides a justification for assuming that offenders either act in a rational manner or, if they fall short, they do so notwithstanding a preference to act rationally. The Section then describes how a lawmaker whose goal is to maximize aggregate social welfare would go about determining and implementing a scheme of optimal criminal sanctions.

A. *Rational Offenders*

The economics approach to criminal law assumes that criminal offenders are rational. An actor acts "rationally" if, given a specific goal, she chooses the best means to achieve it.[10] This is a general statement, but it helps set up the framework of the type of rationality—instrumental rationality—that will be our focus.[11] A few comments will help clarify the approach.

Under instrumental rationality, we assume that people have specific goals—for example, to go to Chicago, rob a bank, or become a professional baseball player—which we take as givens and do not question.[12] We further assume that people with goals will take the requisite steps to bring them to fruition.[13] Given these assumptions, we judge an individual's behavior as "rational," if the individual, when choosing among the different courses of actions available to her, chooses the one best suited for achieving her stated goal.

1. *The Decision to Violate the Law*

Under the economics approach to criminal law, rational offenders are driven by a particular, rather generic, goal: to maximize their utility or overall happiness.[14] Rational offenders commit crimes that give them a net gain in utility,[15] or alternatively, crimes whose expected benefits exceed the expected costs.[16] An offender's benefits from misconduct may include increasing his wealth, retaliating against perceived social unfairness,

---

[10] *See* John C. Harsanyi, *Advances in Understanding Rational Behavior*, *in* RATIONALITY IN ACTION: CONTEMPORARY APPROACHES 271, 272 (Paul K. Moser ed., 1990).

[11] The concept of rationality in economics, however, is narrower; it assumes that actors make decisions using a well-defined preference relation to compare and order the various alternatives available to them. This preference relation is complete, in that every positive alternative in the relevant choice set is comparable; it also satisfies transitivity—if the individual prefers a over b and b over c, she prefers a over c. *See* ANDREU MAS-COLELL ET AL., MICROECONOMIC THEORY 6–7 (1995) (defining preference relations that are "rational").

[12] *But see* Aurel Kolnai, *Deliberation Is of Ends*, 62 ARISTOTELIAN SOC'Y 195, 196 (1962) (calling into question whether someone who has set for themselves a certain goal did not by necessity already engage in the same type of goal-driven deliberation).

[13] *See* Joseph Raz, *The Myth of Instrumental Rationality*, 1 J. ETHICS & SOC. PHIL. 13 (positing that one with stated ends who fails to take the proper means to achieve it acts irrationally).

[14] One may question whether utility maximization is an appropriate goal to have and whether society should take steps to help its members achieve this goal. But the economics approach to criminal law asks us to accept this utility maximizing goal as being a valid one, normatively speaking.

[15] *See* RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 219–20 (6th ed. 2003) (stating that under the economics approach to criminal law, offenders are assumed to be rational, and thus choose to commit crimes when they will yield expected benefits that are greater than the expected costs).

[16] *See* A. Mitchell Polinsky & Steven Shavell, *The Economic Theory of Public Enforcement of Law*, 38 J. ECON. LIT. 45, 47 (2000) (stating that offenders violate the law if and only if the expected utility from doing so, considering the expected benefits and sanctions, exceeds the utility that they would get from obeying the law).

getting accepted by his peers, or the mere act of hurting someone else.[17] An offender's costs may include monetary fines, imprisonment, social stigma, ostracism, lawyer's fees, anxiety, and numerous other tangible and intangible sources of disutility.

2. *The Goal of Acting Rationally*

Why would an offender want to behave rationally? Because the consequences of violating the law can be severe. They can lead to loss of liberty and, in some cases, loss of life. Rational offenders are more likely to succeed in their criminal endeavors. So even when their behavior falls short of full rationality, it is not for lack of trying or because they had a preference to behave in a non-rational manner.[18] Irrational offenders no doubt exist. But we will exclude them from consideration, since our concern is with instrumentally rational offenders who, by definition, deliberate about the best ways of achieving their goals.[19]

B. *Deterring Rational Offenders*

Under the economics approach, the goal of the criminal justice system is to maximize social welfare.[20] That is, to maximize the aggregate utility of all actors affected by criminal misconduct, particularly: actual and potential victims; taxpayers, who pay for the criminal justice system (which includes the police, prosecutors, public defenders, courts, and the prison system); and offenders. Including the offender's welfare in the

---

[17] *See* MICHAEL R. GOTTFREDSON & TRAVIS HIRSCHI, A GENERAL THEORY OF CRIME 89 (1990) (cataloguing immediate rewards of crime); JACK KATZ, SEDUCTIONS OF CRIME, MORAL AND SENSUAL ATTRACTIONS IN DOING EVIL 312 (1988) (arguing that criminals take "delight in deviance" and "take pride in a defiant reputation as 'bad'"). Offenders may also get immediate utility from using criminal activity as a form of retaliation against perceived injustice. *See* Vai-Lam Mui, *The Economics of Envy*, 26 J. ECON. BEHAV. & ORG. 311, 312 (1995) (exploring "the role of envy in provoking sabotage or retaliation against others" and stating that "envy plays an important role in social and economic life"); William Terris & John Jones, *Psychological Factors Related to Employees' Theft in the Convenience Store Industry*, 51 PSYCHOL. REP. 1219, 1225 (1982) (finding that revenge is one of the major motivators of employee theft).

[18] We will assume therefore that offenders have a second-order preference to act rationally and to hold rational beliefs. *See* Richard C. Jeffrey, *Preferences Among Preferences*, 71 J. PHIL. 377, 381 (1974) (discussing how people choose their preferred preferences).

[19] Individuals who go through life thoughtlessly acting according to whatever desire they happen to be feeling at the time would not be very effective as criminals. *See* HARRY G. FRANKFURT, THE IMPORTANCE OF WHAT WE CARE ABOUT, ESSAYS 47, 50 (1988) (arguing that the ability of people to form second-order preferences regarding what first-order desires they want to ultimately motivate them is an important part of what it means to be a person).

[20] *See* Gary S. Becker, *Crime and Punishment An Economic Approach*, 76 J. POL. ECON. 169, 180–81 (1968) (describing the goal of minimizing the social costs of crimes); Nuno Garoupa, *The Theory of Optimal Law Enforcement*, 11 J. ECON. SURVEYS 267, 269 (1997) (providing overview of the optimal law enforcement model); Richard A. Posner, *An Economic Theory of Criminal Law*, 85 COLUM. L. REV. 1193, 1194, 1196 (1985) (applying utilitarian approach to various areas of substantive criminal law).

social welfare calculus is controversial, particularly in the case of violent crimes. But under the economics approach, the goal is not necessarily to foreclose all criminal activity.[21]

Some crimes, like murder, rape, and armed robbery, require total deterrence because they produce harm that is so serious in nature that it trumps any plausible legitimate benefits to criminals.[22] However, there are a series of less harmful offenses, including regulatory crimes, that, while serious, do not necessarily call for total deterrence—at least not from an economic standpoint.[23]

1. *Optimal Deterrence*

When crimes do not call for total deterrence, a lawmaker will set the expected sanctions equal to the expected harm of the illegal behavior. This will assure that a rational offender will commit a crime only when it produces a net gain for society; that is, only when his net expected benefits (after taking the expected sanctions into account) are at least as great as the social harm. If a crime produces a social harm of $100, the expected sanctions will also be set at $100.[24] An offender who receives $300 from the crime will choose to offend, and by doing so, maximize social welfare; on the other hand, an offender who receives only $75 from the crime will choose to obey the law, which again maximizes social welfare.

2. *Total Deterrence*

Crimes, like murder, rape, and armed robbery, that call for total deterrence can be deterred by setting the expected sanctions at a level that greatly exceeds the benefits that offenders would hope to receive. While there is no danger of overdeterring offenders, a lawmaker must still make sure that the sanctions for these serious crimes are well-calibrated.[25] A lawmaker who punishes all of these crimes with the same maximal

---

[21] *See* Becker, *supra* note 20, at 180–81 (calculating aggregate welfare by taking into account the benefits offenders receive from their criminal activity).

[22] *See* Posner, *supra* note 20, at 1196–97, 1215–16 (discussing criminal activity, much falling under the rubric of common law crimes, that society has determined calls for total deterrence).

[23] In fact, the law and economics approach to criminal sanctions is based on the same general principles used to determine the optimal damages for torts, where the goal is to provide actors with the right incentives when choosing their activities and level of care, rather than completely dissuading them from engaging in those activities. *See* STEVEN SHAVELL, FOUNDATIONS OF ECONOMIC ANALYSIS OF LAW 474–79 (2004) (discussing analogous strict liability and fault-based rules in tort and criminal law contexts).

[24] The gross sanctions will often have to be higher, to account for the probability that an offender will escape prosecution. When an offense produces a harm, h, and the probability of detection is p, the optimal sanction is h/p. In our example, if the probability that the offender will be identified, arrested, and successfully prosecuted is 0.5, the optimal gross sanction is $200, assuming that offenders are risk neutral. This gross penalty would assure that the expected sanctions and expected harm both equal $100, the desired result.

[25] *See infra* Section III. F. (discussing marginal deterrence under a system of digital policing).

sanction—say, life in prison—can end up giving offenders perverse incentives. A bank robber who knows that robbery and murder both carry the same penalty will have an incentive to kill eyewitnesses. To avoid these marginal deterrence misincentives, less serious total deterrence crimes must be punished less severely than the more serious ones, like murder and rape.

3. *Fines and Imprisonment*

Society can punish offenders using monetary fines, prison sentences,[26] or some combination of both. All things being equal, fines impose fewer social costs than do prison sentences. Fines are a one-time wealth transfer from the offender to the state, and thus create few administrative or deadweight costs. Imprisonment, on the other hand, creates significant social costs, such as the costs of administering the prison system and of providing offenders with greater procedural safeguards. Imprisonment also creates opportunity costs: inmates are not as economically productive as their counterparts outside of prison.[27] Given the goal of maximizing social welfare, a lawmaker would first attempt to punish offenders with fines, resorting to prison sentences only in cases in which an offender is unable to pay the fine.[28]

C. *How Much Should Society Spend on Enforcement?*

When setting expected sanctions, a lawmaker has to decide how high to set the gross sanctions and how much to invest on law enforcement. All things being equal, the more that society invests on law enforcement, the higher the probability that offenders will be punished, and thus the higher the expected sanctions. But law enforcement is costly. Society must spend resources to determine that a crime occurred, and to identify the offender and bring him to justice. The second way to increase expected sanctions is to increase the gross sanctions. As a general matter, this will be a more economical option than trying to increase the probability of detection.

As a result, under the economics approach, if a crime is being punished with a fine, the lawmaker should first increase the fine as high as

---

[26] *See* A. Mitchell Polinsky & Steven Shavell, *The Optimal Use of Fines and Imprisonment*, 24 J. PUB. ECON. 89, 89–90 (1984) (discussing various ways of trading off monetary fines and prison terms).

[27] *See* POSNER, *supra* note 15, at 223 (arguing that imprisonment causes a depreciation of skills and a loss of contacts that impairs a convict's productivity post-parole and thus causes depreciation in the convict's human capital).

[28] *See* Polinsky & Shavell, *supra* note 16, at 51 (stating that sanctions via fines should be exhausted first before using prison sanctions because fines are wealth transfers and are generally cheaper to collect than the social costs of imprisonment); *see also* SHAVELL, *supra* note 23, at 482 (discussing underdeterrence when offenders do not have sufficient levels of wealth to pay fines necessary to properly deter them).

possible.[29] If the optimal expected sanctions are $1,000 and offenders can afford a fine of up to a $100,000, a lawmaker should set the probability of detection at 1% and the gross fine at $100,000. Assuming that the administrative costs of fines do not increase with the level of the fine (which will not always be the case because offenders facing higher fines may attempt to hide assets), any investment in enforcement that increases the probability of detection above 1% would be wasteful.

As we saw above, imprisonment is a costlier option than fines. In cases in which offenders are unable to pay fines, and imprisonment is the only option, a lawmaker will need to compare the added administrative costs from increasing the gross prison sentence with the added law enforcement expenditures needed to increase the probability of detection.[30]

II. COMPLEXITY, LAW ENFORCEMENT, AND DIGITAL SURVEILLANCE

This Section examines the complexities of law enforcement and of the criminal justice process. It begins with a brief overview of how individuals go about making decisions in complex environments. The Section continues by examining the overall complexity of the criminal justice process. It shows that complexity is exacerbated by the need of various law enforcement officials to coordinate their behavior. It then describes the relative complexity of ex ante preventive policing and of ex post investigative policing. It shows that, all other things being equal, preventive policing is a more complex undertaking than investigative policing. The Section then argues that the proliferation of digital policing techniques can be seen as a natural reaction to the growing complexity of the criminal justice process, in general, and of policing, in particular. While digital policing has a greater number of moving parts, they are deployed in manners that reduce the overall complexity of law enforcement. The Section concludes by examining the social benefits and costs associated with digital policing.

---

[29] This was one of the important insights in Gary Becker's work on optimal criminal deterrence. *See* Becker, *supra* note 20, at 190–93 (describing the trade-off between the magnitude of sanctions and enforcement expenditures to increase probability of detection); *see also* Lucian Arye Bebchuk & Louis Kaplow, *Optimal Sanctions When Individuals Are Imperfectly Informed About the Probability of Apprehension*, 21 J. LEGAL STUD. 365, 368–69 (1992) (describing the optimal trade-off between higher sanctions and enforcement costs when offenders are imperfectly informed of probability of detection).

[30] Not all increases in enforcement costs will provide a sufficiently high return in reducing the harm from misconduct; thus, to economize these costs, society will sometimes opt for underdeterrence. If there is underdeterrence, then it does not follow that when a criminal is observed in misconduct, social welfare is increased. *See* SHAVELL, *supra* note 23, at 488–89 (arguing if there is underdeterrence, the fact that someone engaged in misconduct does not signal that her expected benefit exceeds the expected harm).

A. *What Is "Complexity"?*

A complex system is one that is difficult for someone to quickly and fully comprehend. A system's complexity increases with the number of distinct parts that it has,[31] and the way those parts interact.[32] The less transparent those interactions, the greater the system's complexity. It follows that one can reduce complexity by making more salient and transparent how the various parts of a system interact. One can also reduce complexity by "hiding" the interaction between different parts of the system. For example, the value of a publicly traded security depends on the preferences and plans of thousands of potential traders. However, if the capital markets are efficient, the security's equilibrium market price encapsulates all information relevant to its valuation.[33]

B. *Why Complexity Matters: Bounded Rationality of Decision-Makers*

As we saw above, a rational actor in pursuit of a goal will choose the course of action best suited for achieving that goal. This means that a rational decision-maker will, at a minimum, process and use all information in her possession that would help reduce her decisional uncertainty. But a decision-maker facing a quick decision may not have the time or cognitive ability to process this information quickly enough.[34] When a decision-maker leaves information "on the table" due to time and cognitive constraints, she exhibits "bounded rationality."[35] Bounded rationality can lead to costly decisional mistakes that could be avoided if the decision-maker had the time and ability to fully use all of the information. Complex information by definition requires more time and

---

[31] *See* HERBERT A. SIMON, THE SCIENCES OF THE ARTIFICIAL 215 (3d ed. 1996) ("How complex or simple a structure is depends critically upon the way in which we describe it. Most of the complex structures found in the world are enormously redundant, and we can use this redundancy to simplify their description. But to use it, to achieve the simplification, we must find the right representation.").

[32] *See* SIMON, *supra* note 31, at 183–84 (explaining that a complex system is "one made up of a large number of parts that have many interactions," where its complexity will increase whenever, given "the properties of the parts and the laws of their interaction, it is not a trivial matter to infer the properties of the whole").

[33] *See* Sanford Grossman, *On the Efficiency of Competitive Stock Markets When Traders Have Diverse Information*, 31 J. FIN. 573, 573–74 (1975) (stating that in a competitive market the equilibrium price summarizes all relevant information in the market).

[34] *See* James G. March, *Bounded Rationality, Ambiguity, and the Engineering of Choice*, 9 BELL J. ECON. 587, 594 (1978) (stating that limits of rationality stem from the fact that "decision-making impose[s] demands on the scarce resources of a finite capacity human organism").

[35] Bounded rationality increases with the cognitive load or psychic cost that a decision-maker must expend to make sense of the decision environment. *See* HERBERT A. SIMON, MODELS OF THOUGHT 3 (1979) (stating that "human thinking powers are very modest" compared to the complexity of decision environments, and describing "satisficing" decisions due to deliberation using only a subset of the available and relevant information set); SIMON, *supra* note 31, at 29 (describing the rational decision-maker as "a satisficer, a person who accepts 'good enough' alternatives, not because less is preferred to more but because there is no choice").

cognitive effort to process and use. It follows that the costs associated with bounded rationality will tend to increase with the information's overall complexity.

C. *The Complexity of the Criminal Justice Process*

The complexity of the criminal justice process is due in part to the large number of different types of actors involved, as well as the overall complexity of the environment in which crimes play out.

1. *The "Relationships" Forged by a Crime*

When offenders violate the law, they create a number of explicit and implicit relationships with (and between): victims, witnesses, investigators, prosecutors, judges, juries, and innocent individuals who may be mistaken for the real offender. More specifically, when a crime is committed, the offender and the victim become a "pair" of components within a subsystem of the criminal justice system. An eyewitness is an additional component, one that is interconnected to the offender, the victim, and the offender-victim pair. When a police officer investigates the crime, she too becomes part of that crime's subsystem, with analogous interconnections to the other individual and group components. The same is the case for the prosecutor, defense attorney, judge, and jury.

Each of these actors will have to try to make some sense of the overall set of relationships and about specific relationships. A police officer, prosecutor, and jury will have to try to determine the reliability of an eyewitness. To the extent that the witness has a prior relationship with either the offender or the victim (or both), the undertaking will be more complex than in cases in which the witness is a total stranger. Similarly, the relationship between an offender and his victim may be simple or complicated to understand, depending on whether they had a prior relationship.

2. *The Complexity of Policing*

Law enforcement is a complex enterprise. Police officers must make quick decisions, often in the face of great uncertainty. These decisions, moreover, can have a great impact on victims, offenders, and third parties. Police decisions can prevent—or cause—injury or death, they can lead to rightful convictions, or to wrongful acquittals and wrongful convictions. Not surprisingly, the police are required to follow a set of procedural rules.

Given the large number of potential contexts in which these criminal procedure rules may apply, they have evolved into a set of complicated, often vague, prohibitions and directives. Police officers must often apply these rules on the fly, under time pressure, knowing that procedural mistakes can make it more difficult to effectively prosecute offenders and prevent wrongful convictions.

3. *Ongoing Interactions and Coordination*

The level of complexity is also affected by the way that these various actors interact after the crime is committed. Eyewitnesses and crime-scene investigators both interact with offenders, although at different times and through different modes of communication. Between the time that a witness observes a crime and her testimony, she will have occasion to interact with investigators and prosecutors. Complexity will increase with the number of these interactions. It will also increase to the extent that the nature of these interactions is not sufficiently transparent to third parties.

Complexity will also tend to increase when parties are required to coordinate with each other.[36] Coordination failures, even if temporary, can be costly. Coordination will become more difficult to the extent that actors have incomplete information about each other and their environment. The problem is further exacerbated if their behavior is guided by complex legal rules—for example, the complex set of rules that officers must follow in deciding whether they need a search warrant or whether they can make an arrest.[37]

Law enforcement, by necessity, requires multiple state actors to coordinate their behavior: legislators decide what conduct to outlaw; the police monitors, prevents, and investigates; prosecutors have broad discretion in deciding whether to bring a case; and judges make procedural rulings and pass sentences.[38] To fully coordinate, each of these law enforcement actors must try to predict how other enforcement personnel are going to act. They also need to assure that their behavior over time intersects[39] along a number of dimensions—not just physically and temporally but also at the epistemic level.[40]

---

[36] *See* DAVID LEWIS, CONVENTION: A PHILOSOPHICAL STUDY 8–10 (1969) (discussing general coordination problem).

[37] *See* Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 34 (1988) (describing the complexity of the Fourth Amendment and failure of cases to provide clear guidance to police).

[38] *See* JEAN HINDRIKS & GARETH D. MYLES, INTERMEDIATE PUBLIC ECONOMICS 585 (2d ed. 2013) (describing difficulty of making broad claims about an enforcement effort decision when enforcement is dispersed across various actors).

[39] Coordination complexity will increase to the extent that parties are required to coordinate their behavior over time. *See* George Loewenstein & Richard H. Thaler, *Intertemporal Choice*, 3 J. ECON. PERSP. 181, 181 (1989) (defining intertemporal choices as "decisions in which the timing of costs and benefits are spread out over time").

[40] *See* OLIVER E. WILLIAMSON, MARKETS AND HIERARCHIES: ANALYSIS AND ANTITRUST IMPLICATIONS 31–33 (1975) (discussing "information impactedness"—i.e., "when true underlying circumstances relevant to the transaction . . . are known to one or more parties but cannot be costlessly discerned by or displayed for others").

4. *Discretion and Complexity*

The greater the discretion[41] of the police, prosecutors, and judges, regarding enforcement activities and gross sanctions, the greater the amount of complexity faced by each of these actors, as well as potential offenders. For example, prosecutors have great discretion at the time of charging. They may choose to charge an offender with a single count or break down the offense into multiple counts, depending on the context. Prosecutors also have discretion in agreeing to a plea deal and a reduced sanction under such an agreement.[42]

D. *Accurate Policing*

Police officers make law enforcement decisions using information about the "crime environment" in which potential offenders and victims interact.[43] Before making an enforcement decision, an officer will determine the extent to which it makes sense to acquire information to reduce uncertainty about the crime environment.[44] Acquiring and using information, however, is costly.[45] Rational police officers will economize, investing in information only up to the point that a $1 investment produces

---

[41] Discretion is a difficult concept to define precisely, but at a minimum involves a person's ability or freedom to choose between two or more possible actions. For example, prosecutors may exercise discretion when deciding whether or not to charge a suspect, and judges, when sentencing defendants, although, in both cases, their discretion is subject to a number of procedural and legal constraints. *See* Albert J. Reiss, Jr., *Consequences of Compliance and Deterrence Models of Law Enforcement for the Exercise of Police Discretion*, 47 LAW & CONTEMP. PROBS. 83, 89–91 (1984) (defining discretion generally and applying definition to the context of police discretion).

[42] David Alan Sklansky, *The Nature and Function of Prosecutorial Power*, 106 J. CRIM. L. & CRIMINOLOGY 473, 498 (2016) (stating that growing complexity of criminal justice system helps explain rise of prosecutorial power).

[43] A decision environment includes everything that is relevant to the decision, including other actors, tangible objects, and intangible "things." *See* JON BARWISE, THE SITUATION IN LOGIC xiv (1989) (developing "situation logic" in which actors find themselves within a context or situation—i.e , "portions of reality"—at a specific point in time). Rational actors attach subjective probability assessments about their environment based on the beliefs they hold about it. They will, over time, update their beliefs, to the extent that they determine that they do not conform to the true state of the world. *See* Radu J. Bogdan, *The Manufacture of Belief*, *in* BELIEF: FORM, CONTENT AND FUNCTION 149, 160–61 (Badu J. Bogdan ed. 1986) (stating that beliefs "track" certain facts or information about the real world); ROBERT NOZICK, THE NATURE OF RATIONALITY 67–69 (1993) (discussing various reasons for privileging true beliefs, but stating that in some rare contexts having false beliefs can make someone better off).

[44] *See, e.g.*, JACK HIRSHLEIFER & JOHN G. RILEY, THE ANALYTICS OF UNCERTAINTY AND INFORMATION § 5.1–5.2 (1992) (discussing cost-benefit analysis used by decision-makers contemplating acquiring information to reduce uncertainty).

[45] *See* LOUIS PHLIPS, THE ECONOMICS OF IMPERFECT INFORMATION 23–24 (1988) (discussing costs of time spent by individuals searching for information); Herbert A. Simon, *Alternative Visions of Rationality*, *in* RATIONALITY IN ACTION: CONTEMPORARY APPROACHES 189, 197–200 (Paul K. Moser ed., 1990) (describing costs associated with processing information and role of bounded rationality in decision-making process).

at least a $1 benefit, such as learning of a crime's occurrence or an offender's identity.

Officers may also invest in making more accurate enforcement decisions, investments in information that can reduce the likelihood of wrongful convictions and wrongful acquittals.[46] As a general matter, a "fully accurate" decision is one the decision-maker would not change if she had additional information.[47] One would expect that rational police officers intent on making good law enforcement decisions will invest in increasing the accuracy of their observations up to the point that the marginal benefits equal the marginal costs of added accuracy.[48] Police officers, however, are agents of the state.[49] As such, their interests may diverge from those of a benevolent lawmaker who sets out to maximize social welfare.[50]

---

[46] These potential errors can be reduced by acquiring more accurate information. An observation is more "accurate" if it leads to a conclusion that is closer to the true state of the environment. *See* Louis Kaplow & Steven Shavell, *Accuracy in the Determination of Liability*, 37 J. L. & ECON. 1, 10–12 (1994) (stating that the greater the accuracy of information, the less likely that there will be an adjudication error).

[47] *See* John W. Payne & James R. Bettman, *Preferential Choice and Adaptive Strategy Use*, *in* BOUNDED RATIONALITY: THE ADAPTIVE TOOLBOX 123, 133–34 (G. Gigerenzer & R. Selten eds., 2001) (discussing various metrics used in the rationality literature to assess the "accuracy" of decisions).

[48] In designing a law enforcement system, it is necessary to take into account the tradeoff between the accuracy and usability of information gathered in the process. For example, in a nuclear power plant, it is important to get an accurate reading of the temperature inside the reactor's core; at the same time, greater accuracy will require more data and thus more computational resources and processing time. What ultimately matters is getting an accurate reading in a timely fashion. One way that designers have dealt with this type of problem is by taking measurements at set intervals, and if those measurements indicate that there is a potential problem, dynamically taking more extensive, "accurate" measurements. During the time that the more detailed measurements are being made and processed, the plant's operator may determine, given other threshold signals, that the reactor has to be shut down immediately—i.e., before getting a full, accurate reading. For a discussion of the multiple-tier safety procedures, see John A. Stankovic, *Real-Time and Embedded Systems*, *in* THE COMPUTER SCIENCE AND ENGINEERING HANDBOOK 1710–11 (Allen B. Tucker, Jr. ed., 1997) (reviewing the concepts of sensors, time correctness, timing constraints, and critical tasks in the context of real-time systems using examples of safety procedures for nuclear reactors, aircraft control, and automated factory floors).

[49] Agency relationships arise when one party agrees to act on behalf of another party. The Restatement of Agency defines agency as "the fiduciary relationship . . . arises when one person (a 'principal') manifests assent to another person (an 'agent') that the agent shall act on the principal's behalf and subject to the principal's control, and the agent manifests assent or otherwise consents so to act." RESTATEMENT (THIRD) OF AGENCY § 1.01 (AM. LAW INST. 2005).

[50] Agency relationships allow a principal to delegate certain tasks to the agent. This is beneficial, since it allows for the division of labor. It, however, comes at a cost. As a general matter, a principal will be unable to fully monitor their agent. One would expect that a bona fide, self-interested agent will act in a self-serving manner, at least to the extent to which the principal cannot observe its behavior. *See* John W. Pratt & Richard J. Zeckhauser, *Principals and Agents An Overview*, *in* PRINCIPALS AND AGENTS: THE STRUCTURE OF BUSINESS 1, 2 (John W. Pratt & Richard J. Zeckhauser eds., 1985) (stating that an agency problem can arise when "one individual depends on the action[s or behavior] of another"); Joseph E. Stiglitz, *Principal and Agent*, *in* THE NEW PALGRAVE: ALLOCATION,

Even if police officers were perfectly benevolent and wanted to choose the optimal level of accuracy, they may fail to do so. This is because more accurate decisions demand more information and thus lead to more complexity.[51] Given the bounded rationality of officers, it would not make economic sense to acquire additional information that will go unused. As a result, officers will underinvest in increasing the accuracy of their information—unless they can do so in a manner that does not increase their overall cognitive load. One way of doing this is by using surveillance technology that combines and presents data in a manner that reduces complexity.

E. *The Timing of Enforcement: Ex Ante Preventive Policing vs. Ex Post Investigative Policing*

Society can choose to focus its enforcement efforts to interrupt crimes before they occur ("preventive policing"),[52] or to investigate crimes after they have occurred ("investigative policing").[53] In preventive policing

---

INFORMATION AND MARKETS 241, 241–42 (John Eatwell et al. eds., 1989) (discussing the sources of agency problems and various approaches available to try to reduce agency costs).

[51] A perfectly accurate set of observations would lead to a transparent environment. Transparency refers to a decision-maker's level of access to information about her environment. An environment is transparent in real-time if the decision-maker comes to hold true beliefs about the relevant properties while she still has the ability to change her mind about a planned course of action. An environment is completely opaque if the decision-maker does not hold any true beliefs about any of its relevant properties at the time of acting. Real-time transparency and opaqueness lie in a continuum: at one end is complete real-time transparency, in which a decision-maker has access in real time to all of the information that she needs to make a fully informed decision; at the other end of the spectrum is complete opacity, in which the actor makes the decision completely blind—i.e., without access to any relevant information. More generally, a decision-maker starts with a goal, a set of beliefs, and a set of feasible actions that can help her achieve that goal. Among other things, she holds beliefs about certain aspects or properties of her environment, including its current state and way it may evolve. Suppose that the true state of the environment (or its expected state in the future) is defined by a set of properties (x, y, z, etc.); that environment is transparent if the decision-maker believes that all of these properties are true. The level of transparency will go down to the extent that the observer is mistaken about one or more of them. *See* STUART J. RUSSELL & PETER NORVIG, ARTIFICIAL INTELLIGENCE: A MODERN APPROACH 46 (1995) (drawing distinction between accessible environments, in which an agent is able to ascertain the true state of an environment by observing it, and non-accessible ones, in which observation provides only partial information of an environment's true state).

[52] *See* State v. Slater, 2010 WL 5419030, at *3 (N.J. Super. Ct. App. Div. 2010) (describing preventive policing in which police tries to prevent crimes from occurring); DAVID A. HARRIS, GOOD COPS: THE CASE FOR PREVENTIVE POLICING 4 (2005) (defining preventive policing as an approach in which police focus on preventing crime before it occurs as opposed to investigating crimes after the fact); Amna Akbar, *National Security's Broken Windows*, 62 UCLA L. REV. 834, 849 (2015) (describing preventive policing approach in national security context); Elizabeth E. Joh, *The New Surveillance Discretion Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL'Y REV. 15, 25–26 (2016) (describing Chicago preventive policing program).

[53] *See* Eric J. Miller, *Role-Based Policing Restraining Police Conduct "Outside the Legitimate Investigative Sphere,"* 94 CAL. L. REV. 617, 620 n.18 (2006) (drawing distinction between preventive and investigative policing, and defining latter as law enforcement activities aimed at "seeking out criminal activity or responding to crime" which includes "walking the beat or patrolling in a car to

regimes, the timing of enforcement actions matters much more: the police need to be constantly on guard to try to identify potential offenders and the date, time, and location when a crime may occur. In other words, police officers must not only make the right decision regarding whether a crime is occurring or is about to occur, but they must make that decision at the right time.[54] Preventive policing also requires the authorities to invest in enforcement-related information that may go stale before they get a chance to use it.[55]

In investigative policing regimes, on the other hand, the authorities can wait to start expending resources on enforcement until they know that a crime has occurred, at a particular location. At that point, they can focus fully on identifying and locating the offender. Importantly, in an investigative regime, law enforcement can wait until some of the uncertainty surrounding a crime has been resolved before they commit resources to enforcement.[56]

All other things being equal, investigative policing involves a smaller number of dimensions: there will be less uncertainty about the set of potential offenders, victims, types of crimes, and geographical locations.[57] Furthermore, the only material time constraint faced by investigators are statutes of limitations.[58] It follows, that preventive policing is a more complex undertaking. Given this complexity, the bounded rationality constraints faced by police officers will be more binding in preventive

---

setting up speed traps, [and] responding to 911 calls"); Dilip Mookherjee & I. P. L. Png, *Monitoring Vis-á-Vis Investigation in Enforcement of Law*, 82 AM. ECON. REV. 556, 556 (1992) (distinguishing between ex ante monitoring and ex post investigations).

[54] *See* Stankovic, *supra* note 49, at 1709 (stating that a real-time system is one in which the correctness of the system depends on both the result and the time in which the result is produced).

[55] *See* Stuart Anderson & Juliana Küster Filipe, *Guaranteeing Temporal Validity with a Real-Time Logic of Knowledge*, *in* IEEE COMPUTER SOCIETY, PROCEEDINGS OF THE 23RD INTERNATIONAL CONFERENCE ON DISTRIBUTED COMPUTING SYSTEMS 178, 178 (2003) ("The older the data gets the more unusable and unreliable it becomes."); Ben Kao et al., *Updates and View Maintenance in Soft Real-Time Database Systems*, 8 INT'L CONF. INFO. & KNOWLEDGE MGMT. 300, 300–01 (1999) (discussing the problems that can arise when using stale data).

[56] Investments in information are irreversible, so the greater the uncertainty regarding the future, the greater the potential value of delaying making an investment until some of that uncertainty is resolved. *See* AVINASH DIXIT & ROBERT PINDYCK, INVESTMENT UNDER UNCERTAINTY 3–4 (1994) (discussing the "option" value created by delaying making decisions that are costly to reverse, where a decision-maker has the ability to delay committing to a course of action, and some of the uncertainty will be resolved with the passage of time); *see also* ANDREU MAS-COLELL ET AL., MICROECONOMIC THEORY 690 (1995) (discussing role of passage of time in revealing true states of world and resolving uncertainty).

[57] All other things being equal, the complexity of a decision will increase with the number of future states of the world affected by that decision. *See* Karen Eggleston et al., *The Design and Interpretation of Contracts Why Complexity Matters*, 95 NW. U. L. REV. 91, 97–100 (2000) (arguing that complexity increases with uncertainty or equivalently with the number of future states of the world that a decision-maker must take into account).

[58] If it takes too long to solve the crime, other time constraints will become binding. For example, witnesses may die or their testimony become less accurate as they begin to forget certain facts.

regimes.

Under the economics approach to criminal law, society should focus on investigative, not preventive policing. Preventive policing will sometimes lead to pre-crime investigations and arrests of individuals who, if left to their own devices, would have decided not to go through with the crime in question. Preventing offenders from committing crimes imposes costs on the offenders who are prevented from committing the crime. An offender who is caught in a crime prevention scheme will bear additional costs, including the myriad tangible and intangible costs associated with being stopped, searched, and arrested.

F. *Inattentive Policing*

A number of studies have found that inattention can lead decision-makers to make systematic decision mistakes. Consumers are less likely to pay attention to hidden taxes, hidden shipping costs, and financial information revealed on Fridays.[59] All things being equal, inattentive decision-makers are more likely to pay attention to salient information, and overlook less salient, complex information. This is because when decision-makers face bounded rationality constraints, they must decide which pieces of information to include in their deliberations and which to ignore. A fully rational actor will use both salient and non-salient information, but inattentive, boundedly rational actors will give relatively more attention to salient information. Inattention, therefore, is more likely to lead to erroneous decisions when decision-makers must make decisions quickly.

Inattention can lead police officers to make mistakes when confronting offenders or investigating crimes.[60] As with bounded rationality, the likelihood of such a mistake increases as the complexity of the crime

---

[59] *See* Raj Chetty et al., *Salience and Taxation Theory and Evidence*, 99 AM. ECON. REV. 1145, 1165 (finding that consumers are less likely to pay attention to hidden taxes); Tanjim Hossain & John Morgan, . . . *Plus Shipping and Handling Revenue (Non) Equivalence in Field Experiments on eBay*, 6 B.E.J. ECON. ANALYSIS & POL'Y: ADVANCES IN ECON. ANALYSIS & POL'Y 1 (2006) (finding that to the extent that those charges are bundled with the price of the item being sold, purchasers in eBay auctions are less likely to incorporate the shipping charges into their decision process, as opposed to being presented as an independent cost); David Hirshleifer et al., *Driven to Distraction Extraneous Events and Underreaction to Earnings News*, 64 J. FIN. 2289, 2323 (finding greater inattention when too much information about different companies is released on the same day); Lauren Cohen & Andrea Frazzini, *Economic Links and Predictable Returns*, 63 J. FIN. 1977, 1978–79 (2008) (finding slow reaction by investors in company A of incorporating information from company B that has an indirect effect on the future value of company A).

[60] Let v be the benefit to a police officer from taking an enforcement action and let c be the costs. A rational officer will take that action only if: $v - c > 0$. One way of modeling inattention, and parsing out its various components is by introducing an additional parameter, θ, that captures the officer's level of inattention. Let o be information about the action in question that is opaque. The officer would then make a decision based on the following cost-benefit calculus: $[v + (1 - \theta) \times o_v] - [c + (1 - \theta) \times o_c] > 0$. This means that if, $\theta = 1$, the officer is fully inattentive; and if $\theta = 0$, he is fully attentive.

environment increases, and whenever officers must make decisions quickly. Preventive policing requires officers to make a larger number of quick decisions than does investigative policing. Moreover, the costs associated with preventive policing mistakes tend to be higher—e.g., wrongfully arresting someone or inappropriately resorting to the use of deadly force.

G. *Preventive Policing and Machine Learning*

Police departments that have embraced preventive policing make great use of machine learning algorithms to help identify crime hot spots and deploy enforcement personnel. It is thus helpful to provide a brief overview of how machine learning works. Machine learning algorithms process data in order to identify patterns and make predictions.[61] Under the most common type of machine learning, supervised learning, historical data is used to train the learning algorithm to identify a set of descriptive features and a target feature, and settle on a prediction model that is consistent with the training data. A model is consistent if it makes a correct prediction for every record in the training dataset.[62]

The goal of machine learning is to use training data to find predictive models that generalize well, so that they can be used to make accurate predictions when new data is used.[63] Two types of generalization problems can arise. In the first, the "overfitting" problem, the person using the algorithm fits the training data so well that the predictive model, understandably, makes very accurate predictions using that training data.[64] On the other hand, a predictive model suffers from "underfitting" when the model is not complex or expressive enough to capture the underlying relationship between the descriptive features and the target feature.[65]

For example, in credit-default machine learning programs, the descriptive features may include the borrower's age, occupation, income, and credit history, and the target feature would be a "yes" or "no" answer

---

[61] *See* JOHN D. KELLEHER ET AL., FUNDAMENTALS OF MACHINE LEARNING FOR PREDICTIVE DATA ANALYTICS 3 (2015) (defining machine learning as "an automated process that extracts patterns from data").

[62] *See* KELLEHER ET AL., *supra* note 62, at 4–6 (describing models that are consistent with data and some of the problems with relying solely on consistency when judging models).

[63] Pedro Domingos, *A Few Useful Things to Know About Machine Learning*, 55 COMM. OF THE ACM (2012) ("The fundamental goal of machine learning is to generalize beyond the examples in the training set.").

[64] *See* Vineet Chaoji et al., *Machine Learning in the Real World*, 9 PROCEEDINGS VLDB ENDOWMENT 1597, 1598 (2016) (describing "overfitting" problem in which a predictive model fits the training data well but fails to properly generalize to new data).

[65] *See id.* (describing underfitting problem, where the model is not expressive enough to capture the underlying relationship).

to the question: did the borrower default?[66] Historical training data is used to come up with a generalizable prediction model. One possibility is the model: if the borrower is under the age of 30, is an industrial worker, makes under $50,000, and has a credit rating of under 700, then the borrower defaults.

Preventive policing using machine learning casts a wide net. Its goal is to gather large amounts of data in order to learn about the crime environments in which potential offenders operate.[67] Historical data about past crimes, geographical locations, and other predictive features are used to train the algorithms. As new data is fed into the trained algorithms, the programs will make predictions about geographical areas in which particular types of crimes are likely to occur within set time periods.[68] This allows police departments to deploy personnel in anticipation.[69] There are well known problems with predictive policing learning algorithms, including certain biases that can creep into the algorithms over time.

In addition to machine learning, digital policing uses other Big Data technologies to collect and mine surveillance data to help reduce the bounded rationality constraints[70] faced by law enforcement personnel. Even though digital policing systems greatly increase the amount of information available to officers, they do so using well-designed interfaces[71] that "hide" irrelevant information[72] from police officers

---

[66] *See* Amir E. Khandani et al., *Consumer Credit-Risk Models Via Machine-Learning Algorithms*, 34 J. BANKING & FIN. 2767, 2772–73 (2010) (discussing descriptive features in credit card default model).

[67] *See* Lawrence W. Sherman, Patrick R. Gartin, & Michael E. Buerger, *Hot Spots of Predatory Crime Routine Activities and the Criminology of Place*, 27 CRIMINOLOGY 27, 37–42 (1989) (early study finding crime "hotspots" and providing explanation for observed geographic concentrations); George Mohler, *Marked Point Process Hotspot Maps for Homicide and Gun Crime Prediction in Chicago*, 30 INT'L J. FORECASTING 491, 495 (2014) (describing hotspot policing and predictive policing methods, which rank geographic locations based on historical data and the estimated risk of future crimes, in order to allocate scarce police resources).

[68] *See* Lawrence McClendon & Natarajan Meghanathan, *Using Machine Learning Algorithms to Analyze Crime Data*, 2 MACHINE LEARNING & APPLICATIONS: AN INT'L J. 1, 2 (2015) (noting the goal of data mining and machine learning algorithms is to predict future outcomes).

[69] *See* Chao Zhang et al., *Keeping Pace with Criminals Designing Patrol Allocation Against Adaptive Opportunistic Criminals*, *in* PROCEEDINGS OF THE 14TH INTERNATIONAL CONFERENCE ON AUTONOMOUS AGENTS AND MULTIAGENT SYSTEMS 1351, 1357–58 (2015) (describing learning results from planning algorithms for anticipating opportunistic criminal offenders).

[70] This is not to say that digital policing systems do not face similar time and computational constraints. The difference is that people have more limited computational power than do machines; they also have more limited storage capability. *See*, *e.g.*, RUSSELL & NORVIG, *supra* note 52, at 845–46 (discussing challenge of bounded rationality for artificial intelligence).

[71] An "interface" is a set of rules that governs the manner in which an observer can extract information from her environment: on one side of the interface resides the information which will remain hidden from observers; on the other, the information that the designer makes available to any observer who interacts with that environment through that interface. Because of this information-filtering characteristic, interfaces are an important mechanism for hiding information. *See* Jakob Nielsen, *Usability Engineering*, *in* THE COMPUTER SCIENCE AND ENGINEERING HANDBOOK 1440,

through abstraction[73] and modular design.[74] This helps reduce the overall complexity of processing and using that information.[75]

Digital policing systems can evaluate information in real-time, or merely capture it to store and process at later times. Processing information on an as-needed basis is useful in reducing complexity and computational costs,[76] and avoiding wasteful processing of information that is never used. This sort of "lazy evaluation" of data creates an option value similar to a

---

1440–41 (Allen B. Tucker, Jr. ed., 1997) (describing branch of computer science that deals with the problem of reducing the complexity that humans experience when they interact with computers).

[72] Since the cognitive load of interacting with a system increases with the number of components, it follows one can reduce complexity by "hiding" components from users. *See* STEVE MCCONNELL, CODE COMPLETE 118 (1993) (stating, in the context of software engineering, that information hiding is "one of the few theoretical techniques that has indisputably proven its value in practice"); Timothy H. Goldsmith, *Optimization, Constraint, and History in the Evolution of Eyes*, 65 Q. REV. BIOLOGY 281, 282–84 (1990) (describing end result of several evolutionary processes by which eyes have adapted to, among other things, abstract away from superfluous information); Herbert A. Simon, *The Organization of Complex Systems*, *in* MODELS OF DISCOVERY 245, 254 (1977) (stating that in hierarchical systems one can reduce complexity by having the system components operate "in independence of the detail of the others; only the inputs it requires and the output it produces are relevant for the larger aspects of system behavior").

[73] *See* HAROLD ABELSON & GERALD JAY SUSSMAN, STRUCTURE AND INTERPRETATION OF COMPUTER PROGRAMS 80–82 (2d ed. 1996) (describing the use of data abstraction in computer programs in order to clearly separate the way that data objects are *implemented*—the manner in which data is represented and stored in the computer's memory—from the way that they are *used* by procedures that manipulate them); CALEB DRAKE, OBJECT ORIENTED PROGRAMMING WITH C++ AND SMALLTALK 98 (1998) (stating that abstraction is "the process of extracting the relevant information about a category, entity, or activity, and ignoring the inessential details"); ROBERT CECIL MARTIN, DESIGNING OBJECT-ORIENTED C++ APPLICATIONS: USING THE BOOCH METHOD 9 (1995) (stating that abstraction involves the "elimination of the irrelevant and the amplification of the essential").

[74] Modular design "glues" together the various components of a complex system in order to (1) reduce the cognitive load faced by both designers and users; (2) make it easier to modify the system by reducing the number of interdependencies among its components; and (3) create "standardized modules" that can be reused when creating new systems with similar functionality. *See* ABELSON & SUSSMAN, *supra* note 74, at 359 (stating that computer programmers control complexity using same type of modularity techniques used by engineers at large, in which the system is stratified along different levels of abstraction, "each one adopting appropriate large-scale views of system structure"); Simon, *supra* note 73, at 254 (stating that loose coupling of system components allows each component to operate independently of others by localizing all interactions on inputs and outputs carried out through the interface of each component).

[75] *See* Woodrow Hartzog et. al, *Inefficiently Automated Law Enforcement*, 2015 MICH. ST. L. REV. 1763, 1768–73 (summarizing developments in law enforcement technologies that have automated parts of traditional policing).

[76] It is not necessary for the whole information bundle to be completely processed before an actor can undertake other processing tasks. The only requirement is that the actor can eventually reconstitute the knowledge gained from processing each chunk. For example, operating systems are designed so that they can interrupt an ongoing process to take on a new one with higher priority, and to be able to return to the interrupted process in some future period to continue its execution. *See* Thomas E. Anderson et al., *Thread Management for Shared-Memory Multiprocessors*, *in* THE COMPUTER SCIENCE AND ENGINEERING HANDBOOK 1165, 1670–72 (Allen B. Tucker, Jr. ed., 1997) (describing processor scheduling issues in operating systems).

financial option.[77] Eager surveillance, on the other hand, involves proactive surveillance in order to stop potential offenders before they are able to commit a crime.[78] Information gathered for eager surveillance purposes can be used after the fact for lazy evaluation.

H. *The Social Welfare Effects of Digital Policing*

1. *Social Benefits*

There are a number of social benefits produced by digital policing. Digital policing can also reduce the costs of ex ante law enforcement. It creates economies of scale that allow for a greater amount of enforcement activities per dollar spent. It reduces complexity and bounded rationality constraints, thereby allowing officers to make more informed decisions.[79] One consequence is that digital policing will generally require offenders to expend more resources to plan, execute, and cover-up their crimes. This can lead to increased deterrence of some offenders.

Digital policing can also reduce the loss borne by crime victims to the extent that it increases deterrence or leads to an increase in the number of crimes interrupted by the police before the offender can complete them.[80] Potential victims can reduce their own investments in crime prevention.[81] They can either rely on the increased public preventive enforcement, or purchase off-the-rack surveillance cameras and other devices, which have become more cost effective in part due to the growing demand for these technologies by law enforcement.

Finally, digital policing can reduce the number of wrongful convictions and wrongful acquittals. For example, it can lead the authorities to rely less on eyewitness testimony, which is more prone to

---

[77] Lazy evaluation is in some pure functional programming languages, such as Haskell, that make great use of recursive functions that require a lot of computational power. The basic idea is to evaluate functions only when it is clear that the program needs the information to continue to execute properly. A program that uses lazy evaluation can process infinite lists in finite time, given that such lists would not be evaluated until they are needed (and only those portions that are relevant to the task at hand). Lazy evaluation, therefore, allows programmers to create the illusion that a list of objects is infinite when in fact it is not. *See* RICHARD BIRD, INTRODUCTION TO FUNCTIONAL PROGRAMMING USING HASKELL 217–221 (2d ed. 1998) (describing how lazy evaluations helps reduce two types of complexity problems in computer programs: those brought about by the limited storage space within computers and the limited time to execute programs).

[78] *See* Ric Simmons, *Ending the Zero-Sum Game How to Increase the Productivity of the Fourth Amendment*, 36 HARV. J.L. & PUB. POL'Y 549, 562 (2013) (stating that "wiretaps on telephones and Terry stops are [describing] proactive surveillance techniques whose aim is to "identify potential criminals before they have committed a more severe crime," including wiretaps and *Terry* stops).

[79] *But see* Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541, 542–44 (2016) (describing systematic errors in databases used by police).

[80] Anthony A. Braga, *Better Policing Can Improve Legitimacy and Reduce Mass Incarceration*, 29 HARV. L. REV. F. 233, 238–39 (2016).

[81] *Id.*

erroneous identifications.[82]

2. *Social Costs*

There are social costs associated with digital policing. Digital policing creates a number of well-known Fourth Amendment concerns.[83] Digital policing can also increase the potential privacy intrusions borne by innocent, law-abiding citizens. These privacy intrusions can have the perverse effect of leading some otherwise law-abiding individuals to violate the law. To see this, assume that in an investigative policing scheme innocent third parties bear no externality costs. Assume further that if someone obeys the law and suffers a privacy intrusion, they would value the disutility of that intrusion at a cost of $100. Offenders, on the other hand, are more likely to have taken counter-surveillance measures, as part of their effort to avoid being detected. Assume, therefore, that an offender's privacy disutility from this added surveillance is $0. Adding $100 to the costs of *obeying* the law will reduce the net benefits from obedience. As a result, all other things being equal, it will increase the incentive of otherwise law-abiding individuals to violate the law.

Additionally, as shown in Section III, digital policing can lead to systematic, inefficient overdeterrence. It can also lead to "technology wars" between law enforcement and offenders. Expenditures in surveillance can, in short, lead to expenditures in counter-surveillance, which can in turn lead to a ratcheting-up of surveillance expenditures, and so on.

One would also expect that as police departments become more dependent on digital policing, they will have an incentive to focus their attention on monitoring populations whose activities can be digitally observed and measured. One would also expect that they will increasingly use digital policing to surveil individuals residing in localities in which direct law enforcement is costlier to carry out, is more dangerous, or is subject to a greater potential for police mistakes. Digital policing using predictive policing machine learning software can create an additional social cost: it can lead the police to inappropriately focus on detecting crimes committed by certain populations and in certain localities.

Finally, one would expect that as the cost of digital policing goes down, the likelihood of grossly negligent uses of deadly force due to poor training will increase. With the increased use of digital surveillance, police officers spend less time engaged in traditional forms of monitoring and

---

[82] *But see infra* Section III.E. (discussing specific contexts in which digital policing can increase potential errors).

[83] *See* Logan & Ferguson, *supra* note 80, at 548, 577–83 (discussing Fourth Amendment concerns in the realm of examining "significant legal and practical barriers that stand in the way of detecting, curing, and remedying data error").

surveillance that can help them "learn-by-doing." The tacit knowledge gained through direct experience can put officers in a better position to make split-second judgments about whether it is appropriate to use deadly force, about whether a crime has been committed, about the seriousness of the crime, and about the identity of the offender. These last three types of mistakes played a role in a number of the recent controversial uses of deadly force.

III. DIGITAL POLICING AND DETERRENCE POLICY

Digital policing, as we have seen, helps reduce the overall complexity of law enforcement. By doing so, it allows authorities to shift their focus from investigative policing to preventive policing, which is a much more complex undertaking. This Section examines the extent to which the increased use of digital policing, and the related expansion of preventive policing regimes, can affect deterrence policy.

This Section first shows that digital policing can lead to inefficient overdeterrence. It then describes an offender's transaction costs—investments in planning, executing, and covering up crimes—and analyzes their effect on deterrence policy. The Section then examines the relationship between digital policing and wrongful acquittals and convictions. The Section concludes by examining digital policing's effects on marginal deterrence.

A. *Overdeterrence in Specific and General Enforcement Regimes*

Recall that under optimal deterrence, a lawmaker will first determine the expected harm from a particular crime, and it will then set the expected sanctions equal to the expected harm. Under such a regime, offenders will decide to commit a crime only when they receive an expected benefit greater than the expected harm they impose on victims. The expected sanctions in turn depend on two factors: the gross sanctions and the probability of detection. In order to increase the probability of detection, a lawmaker will have to invest in law enforcement.

1. *Specific Enforcement Regimes*

Under the standard economic approach, a lawmaker should use a specific enforcement regime. Under specific enforcement, the lawmaker treats each crime individually: for each, it decides how much to spend on enforcement, and thus where to set the probability of detection.[84] This allows the lawmaker to create a better tailored enforcement regime, one less likely to lead to inefficient overdeterrence or underdeterrence.

---

[84] *See* Polinsky & Shavell, *supra* note 16, at 62 (stating that to achieve specific enforcement, a lawmaker would choose the optimal probability of detection for each different type of crime).

Due to economies of scale, digital policing allows society to increase the probability of detection without having to incur additional enforcement expenditures. If society leaves the gross sanctions at the same level that they were before the advent of digital policing, then offenders subject to a specific enforcement regime would be overdeterred.[85] The overdeterrence problem is exacerbated once we take into account how digital policing affects general enforcement.

2. *General Enforcement Regimes*

In general enforcement, the lawmaker does not draw as fine a distinction between crimes. Instead, they rely on enforcement mechanisms that apply to multiple types of crime, mechanisms in which a single enforcement act can detect different types of crimes.[86] For example, a police officer patrolling a beat may come across different crimes during their patrol or a review of CCTV camera footage may reveal different types of crimes.

The growing use of digital policing in law enforcement has had the concomitant effect of shifting enforcement policy toward the general-enforcement end of the spectrum. A number of surveillance, big data, and machine learning enforcement technologies developed to prevent terrorism and other major crimes have produced an "enforcement externality": they can be used to detect and prevent other types of offenses, without having to make significant additional enforcement investments.[87] The latest iteration of this move toward general enforcement is the growing use of predictive

---

[85] For example, suppose that under a pre-digital policing regime, society spends $100 to produce a probability of detection of $q = 0.25$. By using digital policing, society, with that same $100 enforcement investment, can increase the probability of detection to $p = 0\,5$. Under the economics approach, the optimal sanctions equal: ([the harm, *h*, created by the crime]/[probability of detection]) + [enforcement expenditures]. Suppose that a crime creates a social harm of $10,000. Under a pre-digital policing regime, the optimal sanctions are: [$10,000/0.25] + $100 = $40,100. Under digital policing, the optimal sanctions are: [$10,000/0.5] + $100 = $20,100.

[86] *See* Polinsky & Shavell, *supra* note 16, at 62 (describing general enforcement as involving an action by an enforcement authority that has the possibility of detecting more than one type of violation). Suppose that an offense produces a harm, *h*, the probability of detection is *p*, and the optimal sanction is *h*/*p*. A lawmaker who relies on specific enforcement will choose a crime-specific probability of detection, *p*, which it will implement through its enforcement expenditures. For example, it may set *p* at 0.1 for criminal trespass and at 0.3 for robbery. If the lawmaker chooses to implement a pure general enforcement regime, it would, in theory, adopt a general detection mechanism in which all crimes would have the same probability of being detected. In other words, *p* would be the same across all crimes.

[87] *See* Rosa Brooks, *The Trickle-Down War*, 32 YALE L. & POL'Y REV. 583, 590–91 (2014) (discussing increased use of technology, such as drones, developed for military, and programs through which the Defense Department donates unneeded equipment to police departments); Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1659–60 (2016) (discussing legislation passed to limit police surveillance and better regulate transfer of military equipment to police departments, particularly in light of Ferguson).

policing, carried out using off-the-shelf machine learning software.[88] Predictive policing algorithms use historical crime data to give police officers a greater sense of when and where potential crimes may occur.[89]

The turn toward digital policing has had the effect of bringing together, within a general enforcement regime, crimes that had been previously under a specific enforcement regime. But each crime class that is brought under the general enforcement digital policing scheme will automatically inherit a higher probability of detection.[90] In order to keep the level of deterrence at the same level, and thus avoid overdeterring offenders, the gross sanctions for those crime classes must be reduced.[91] As mentioned above, however, we have not seen a concomitant reduction in gross sanctions.

B. *Overdeterrence of Serial Offenders*

This section shows that digital policing will lead to even greater levels of overdeterrence if the offender has committed previous crimes.

1. *Serial Offenders*

It is useful to draw a distinction between serial offenders and repeat offenders. The former includes an offender who commits more than one crime at different points in time,[92] whether or not they are apprehended and convicted. A repeat offender (or recidivist) is a serial offender who has been previously convicted of a crime. Serial misconduct is a common phenomenon. Many types of crimes afford offenders with repeated

---

[88] *See* Ric Simmons, *Quantifying Criminal Procedure How to Unlock the Potential of Big Data in Our Criminal Justice System*, 2016 MICH. ST. L. REV. 947, 954-57 (describing different predictive policing software used by police departments); Mara Hvistendahl, *Can Predictive Policing' Prevent Crime Before It Happens?*, SCI. MAG. (Sept. 28, 2016, 9:00 AM), http://www.sciencemag.org/news/2016/09/can-predictive-policing-prevent-crime-it-happens.

[89] *Id.*

[90] All other things being equal, an increase in general enforcement should lead a lawmaker to lower the gross sanctions for a crime.

[91] For example, suppose that crimes C_1, C_2,…,C_n have the same probability of detection, p, and that C_1 creates harm h_1, C_2, creates harm h_2, and so on. Finally, suppose that $h_1 > h_2 > \ldots > h_n$. Then it follows that the gross sanction for crime C_1 should be higher than that for crime C_2, and so on. Suppose that crime C_1 creates a loss for the victim of \$10,000 and crime C_2 a loss of \$5,000, and that the general enforcement common probability of detection is $p = 0.5$. Then an offender who commits crime C_1 should be fined \$20,000, and one who commits crime C_2 should be fined \$10,000. Suppose now that a crime D creates a harm $h =$ \$10,000 and, up to this point, it has been subject to a specific enforcement scheme, with a probability of detection of $q = 0.25$. The optimal gross sanctions for this crime are \$40,000. Assume that the general enforcement strategy is expanded slightly so that crime D now falls within it. Under general enforcement, the probability of detection doubles from $q = 0.25$ to $p = 0.5$. It follows that in order to maintain the same level of deterrence, the gross sanctions must be reduced from \$40,000 to \$20,000.

[92] These crimes may be spaced out over a short spree or over years in the case of a career criminal.

opportunities to violate the law. Employees who embezzle funds often do so repeatedly and over extended periods.[93] Co-conspirators in criminal enterprises and members of gangs engage in a variety of repeated criminal activity over long periods of time. Managers who falsify financial results usually do so in more than one reporting period and may over time resort to other fraudulent transactions to cover up the false disclosure. More generally, serial misconduct is common in securities, antitrust, and environmental law, as well as in a number of other regulatory contexts.

2. *Escalating Sanctions and Overdeterrence*

Under the economics approach to criminal law, the optimal expected sanctions are solely determined by the harm produced when an offender violates the law, which (all other things being equal) will be the same across offenders and regardless of the number of times the crime is committed.[94] That is, a rational offender will commit a crime ten times (or equivalently, ten offenders will each commit it once) only if, in each instance, the benefits are greater than the expected sanctions (and thus greater than the harm produced).

Since, for the purpose of setting optimal sanctions, all instances of the same crime are identical, the standard approach does not draw a distinction between the one-time and serial offender. The law, however, routinely punishes previously convicted offenders and those who commit more than one crime before being caught (whether or not previously convicted) with "super-punitive" expected sanctions.[95] Serial offenders face sanctions that

---

[93] Greg Jones, *Good Workers Gone Bad How to Spot Employee Theft*, CNBC (Feb. 28, 2012, 11:54 AM), http://www.cnbc.com/id/46556452.

[94] *See* Ehud Guttel & Alon Harel, *Matching Probabilities The Behavioral Law and Economics of Repeated Behavior*, 72 U. CHI. L. REV. 1197, 1198 (2005) (stating that the standard law and economics approach to repeated misconduct has "long assumed that whether such choices are made repeatedly or on a one-time basis is expected to have little or no effect on individuals' decisions . . . .").

[95] The Federal Sentencing Guidelines Manual provides for heightened sanctions for repeat and career offenders. *See* U.S. SENTENCING COMM'N, U.S. SENTENCING GUIDELINES MANUAL § 4A1.1 (U.S. SENTENCING COMM'N 2006) (allowing for the addition of points to criminal history dependent upon the type and length of prior sentence); *id.* at § 4B1.1 (2006) (adjusting the offense level for career offenders). Under the Immigration Reform and Control Act, the range of penalties for a first-time offender are $250 to $2,000; for a second-time offender they are $2,000 to $5,000; and for a third-time offender they increase to $3,000 to $10,000. Immigration Reform and Control Act of 1986 § 101, 8 U.S.C. § 1324a(e)(4)(A) (2000). In addition, a person who engages in a pattern of violation of the Act can also be subject to a six-month jail sentence. *See* 18 U.S.C. § 1324a(f)(1). Environmental statutes, such as the Clean Water Act and the Clean Air Act, also have provisions for escalating criminal penalties for repeat offenders. Under the Clean Water Act, the available penalties are doubled after a first conviction. *See* Water Quality Act of 1987 § 312, 33 U.S.C. § 1319(c)(1)–(2) (2000) (stating that negligent violators face a maximum of $25,000 per day and a one-year jail sentence, knowing violators face maximum of $50,000 per day and three-year jail sentence for first conviction and providing that the sanctions for second offenses in each can be doubled); *see also* Clean Air Act § 701, 42 U.S.C. § 7413(c)(1) (2000) (allowing maximum sanctions for second offense to be double those for first offenses).

are greater than the aggregate expected harm created by repeatedly engaging in prohibited activity[96] or delaying compliance with legally-imposed duties.[97] Proponents of the economics approach to criminal law acknowledge that increasing sanctions for serial offenders can lead to overdeterrence[98] for which they have offered various explanations.[99] Nonetheless, the use of escalating sanctions for serial offenders remains a puzzle. The move towards digital policing will only make this overdeterrence puzzle more difficult to explain.

Digital policing has made it easier for the authorities to record for future use the digital evidentiary trace created by a serial offender each time that she commits a crime. If an offender is caught, her past decisions to obey or disobey the law can affect how others frame and judge her current act of misconduct—her state of mind, intent, and knowledge[100]—and parcel reactive sentiments of resentment or indignation.[101] The increased use of digital policing has magnified an offender's expected future costs if she were caught and convicted. The digital trace from a previous conviction will increase the likelihood of detection in future

---

[96] *See*, *e.g.*, United States v. Technic Servs., Inc., 314 F.3d 1031, 1047–48 (9th Cir. 2002) (affirming sentence enhancement for defendant's violation of Clean Water Act for repeatedly washing asbestos down drain that discharged into bay); United States v. Liebman, 40 F.3d 544, 549–51 (2d Cir. 1994), *overruled by* United States v. Contreras, 593 F.3d 1135, 1136 (9th Cir. 2010) (agreeing that a sentence can be enhanced for "ongoing and repetitive discharge" of a hazardous substance).

[97] *See*, *e.g.*, Water Quality Act of 1987 § 312, 33 U.S.C. § 1319(c)(2) (2012) (stating that each one-day delay in complying with the agency's order is an act of misconduct, triggering daily fines between $5,000 and $50,000, regardless of the connection between the ongoing delay and the harm caused by the violation being remedied).

[98] *See* A. Mitchell Polinsky & Steven Shavell, *On Offense History and the Theory of Deterrence*, 18 INT'L REV. L. & ECON. 305, 307 (1998) (admitting that escalating sanctions may overdeter some criminal behavior). A similar argument holds for the use of punitive damages in tort. *See Punitive Damages*, *in* 3 THE NEW PALGRAVE DICTIONARY OF ECONOMICS AND THE LAW 192, 193 (Peter Newman ed., Macmillan Ref. Ltd. 1998) ("[I]f damages are less than harm, levels of activity will tend to be socially excessive, and if damages exceed harm, levels of activity will tend to be low.").

[99] *See* C.Y. Cyrus Chu et al., *Punishing Repeat Offenders More Severely*, 20 INT'L REV. L. & ECON. 127, 130–31 (2000) (arguing that because the risk of an erroneous conviction is greater for a first conviction, the penalty for a first conviction is set lower than the expected harm); POSNER, *supra* note 15 at 228–29 (noting several reasons why higher sanctions make sense, including to offset the reduced stigma effect from a second conviction and to counteract the learning-by-doing of repeat offenders); Polinsky & Shavell, *supra* note 99, at 308–09 (arguing that punishing repeat offenders more severely increases the level of deterrence because a first-time offender will take into account the expected sanctions for both the first and second offense).

[100] *See* Roger C. Cramton, *Enron and the Corporate Lawyer A Primer on Legal and Ethical Issues*, 58 BUS. LAW. 143, 147 (2003) (arguing that lawyers should anticipate hindsight bias when advising clients acting at the margin of legality); Jeffrey J. Rachlinski, *A Positive Psychological Theory of Judging in Hindsight*, 65 U. CHI. L. REV. 571, 590–94 (1998) (discussing the role of the hindsight bias in ex post reconstructions of past behavior).

[101] *See* R. Jay Wallace, *Reason and Responsibility*, *in* NORMATIVITY AND THE WILL: SELECTED PAPERS ON MORAL PSYCHOLOGY AND PRACTICAL REASON 123, 123–24 (2006) (describing expectations of behavior in moral communities as reactive sentiments and judgments).

crimes.[102] That is, in a world of increased surveillance, a previous arrest will provide information to the police about the offender's identity, which will in turn reduce future enforcement costs vis-à-vis that offender. It follows, that as the level of post-parole surveillance increases, the sanctions imposed for future offenses should *decrease*.

C. *Some Possible Reasons Why Gross Sanctions Have Not Been Reduced*

1. *Overcoming Systematic Underdeterrence*

One possible explanation is that lawmakers believe that existing sanctions are systematically underdeterring offenders,[103] and thus should be ratcheted up.[104] This may explain why society seems to spend more on enforcement than the economics approach predicts.[105] Offenders who are wealth-constrained and thus "judgment-proof" would be underdeterred by fines but not by prison sentences.[106] The perception by lawmakers that some offenders are not just judgment-proof but also "prison-proof" is what has led states to adopt three-strikes laws.[107]

The emergence of three-strikes laws is not the only indication that

---

[102] *See* David A. Dana, *Rethinking the Puzzle of Escalating Penalties for Repeat Offenders*, 110 YALE L.J. 733, 742 (2001) (arguing that the probability of detection increases with prior convictions because convicted offenders leave a record in the system; therefore, optimal sanctions should be lower for previously convicted offenders).

[103] A number of criminal law scholars have persuasively argued that in practice, this approach has led to repeated increases of criminal sanctions without achieving the deterrence lawmakers desired. *See*, *e.g.*, John M. Darley, *On the Unlikely Prospect of Reducing Crime Rates by Increasing the Severity of Prison Sentences*, 13 J.L. & POL'Y 189, 193–95 (2005) (describing the problem of underdeterrence notwithstanding ever-increasing prison sentences).

[104] There are two reasons why policymakers may intentionally adopt sanctions that underdeter offenders. The first reason is that risk averse offenders will be overdeterred by the optimal sanctions for risk neutral offenders. Risk averse offenders would prefer lower actual sanctions and a higher probability of being caught, given that if they are caught, the extra disutility to them from the higher sanctions is a deadweight loss. For example, if the actual fine is $100,000, a risk averse person who is caught will perceive a loss greater than $100,000, but society will only get the $100,000 fine. As a result, policymakers who believe that the population is comprised of more risk averse than risk neutral individuals will adopt lower sanctions. Second, policymakers may want to adopt expected sanctions that are slightly lower than the expected harm, up to the point that the savings in enforcement costs are greater than the marginal harm that is not deterred. *See* SHAVELL, *supra* note 23, at 484–85 (illustrating the relationship between a low probability and high magnitude sanction policy).

[105] *See* Garoupa, *supra* note 20, at 271 (stating that policymakers resort to prison sentences before exhausting fines); Polinsky & Shavell, *supra* note 16, at 51 (arguing that fines should be exhausted before resorting to prison sentences because fines are socially costless).

[106] SHAVELL, *supra* note 23, at 495 (noting that an actor whose benefit exceeds the maximum imprisonment time will not be deterred).

[107] The Supreme Court recognized as much when it refused to strike down California's three-strikes law in *Ewing v. California*, explaining that California's legislature made a "deliberate policy choice that individuals who have repeatedly engaged in serious or violent criminal behavior, and whose conduct has not been deterred by more conventional approaches to punishment, must be isolated from society in order to protect the public safety." 538 U.S. 11, 24 (2003).

many lawmakers believe that there is a deterrence gap. Since the early 1970s, the average prison sentence in the United States nearly has tripled in length,[108] and the number of inmates in prison has increased from 216,000 to 2,173,800.[109] There also seems to be a perception that white-collar criminals are being systematically underdeterred. This has led lawmakers repeatedly to ratchet-up both fines and prison sentences for white-collar crimes.[110]

2. *Undeterrable Offenders*

Undeterrable offenders are those who cannot be deterred, regardless of the sanction.[111] What does one mean when one says that an offender cannot be deterred?[112] An offender cannot be deterred if her expected benefit is greater than any potential penalty. With some offenses, such as terrorist attacks and shooting sprees in public places, there is a very high probability that the offender may die during the commission of the crime. In other words, the probability of the maximum possible sentence—death—is almost 100%, and thus the expected costs to an offender from committing such a crime are higher than those for any other possible crime.[113] The inability to deter this sort of offender may be based on other factors, such as mental illness, sociopathy, or drug addiction. Heat of passion offenses are equally difficult to deter.

When an offender cannot be deterred, society has to determine whether the harm from their offense is greater than the costs of preventing the crime altogether. The increased use of digital surveillance, intelligence policing, and preventive policing generally is aimed, in part, at dealing with offenders who are immune to deterrence.

---

[108] Darley, *supra* note 104, at 190.

[109] DANIELLE KAEBLE & LAUREN GLAZE, CORRECTIONAL POPULATIONS IN THE UNITED STATES, 2015 2 (U.S. DEP'T OF JUSTICE 2015).

[110] The Sarbanes-Oxley Act provides for enhanced criminal penalties for white-collar offenders. *See* Sarbanes-Oxley Act of 2002, Pub. L. No. 107–204, § 807, 116 Stat. 745, 804 (2002) (codified at 18 U.S.C. § 1348) (detailing corporate and criminal fraud accountability); *id.* §§ 902–05 (codified at 18 U.S.C. § 1349) (providing penalty enhancements for white collar crime); *id.* § 1106 (codified at 15 U.S.C. § 78ff(a)) (providing penalties for any person who willfully and knowingly provides false and misleading statement to the Securities Exchange Commission). This Act exposes an additional puzzle of the neoclassical approach: the fact that lawmakers routinely adopt imprisonment sanctions for offenders, such as white-collar criminals, who have sufficient disposable wealth to pay optimal fines. *See* Garoupa, *supra* note 20, at 271 (explaining that in the United States, and much less in Europe, policymakers resort to prison sentences before exhausting fines).

[111] *See* Christopher Slobogin, *A Jurisprudence of Dangerousness*, 98 NW. U.L. REV. 1, 40–46 (2003) (describing various properties of undeterrable offenders).

[112] *See* United States v. Griffin, 543 Fed. Appx. 789, 793 (10th Cir. 2013) (offender undeterred from criminal activity notwithstanding "numerous contacts with the criminal justice system").

[113] Now, of course, some offenders may see a life sentence as providing them with a much higher aggregate disutility. This would not affect the general claim that these offenders—regardless of the penalty—are undeterrable.

3. *Salient Crimes*

So far we have assumed that an offender's crime creates an objective ex ante harm, in the sense that the level of harm does not vary after the fact based on how the crime is perceived by third parties. Some crimes—gruesome murders, shooting sprees, and terrorist acts—are more salient than others.[114] In fact, the aim of terrorism is to perpetrate salient acts that have a greater impact than the actual harm caused.

When offenders succeed in committing salient crimes, social outrage leads to stepped-up enforcement activities to prevent future occurrences.[115] Salient crimes, over time, will lead to the ratcheting-up of enforcement activities aimed at total prevention. The enforcement activities for salient crimes will increase the overall deterrence for other crimes. This means that the expected sanction for other crimes will increase. This will lead to overdeterrence, unless society lowers the sanctions for non-salient crimes that do not call for total deterrence.

D. *The Transaction Costs of Crime and Overdeterrence*

When offenders commit crimes they take into account two types of costs: the punishment they will incur, if caught; and the up-front investments[116] they must make in order to plan, execute, and cover-up their crimes. These transaction costs of crime have not received much attention in the economic literature on criminal deterrence. This is understandable, given that under the standard economic approach, the goal is to set enforcement expenditures as low as possible, while setting gross sanctions at their maximal level.

But as we have seen, offenders face a much higher likelihood of being detected and arrested under digital policing regimes. Knowing this, rational offenders will invest more resources in planning, executing, and covering-up their crimes. Offenders incur these transaction costs in order to increase the likelihood that they will succeed in their criminal endeavor. Success, from the offenders' point of view, includes receiving the benefits they had

---

[114] *See* Robert J. Smith & Zoë Robinson, *Constitutional Liberty and the Progression of Punishment*, 102 CORNELL L. REV. 413, 422–32 (2017) (summarizing various reactions by courts and legislatures to salient crimes, including ratcheting up gross sanctions).

[115] Darryl K. Brown, *Prosecutors and Overcriminalization Thoughts on Political Dynamics and a Doctrinal Response,* 6 OHIO ST. J. CRIM. L. 453, 453–56 (2009).

[116] These transaction costs of criminal misconduct are best labeled as investments since they require an offender to incur immediate costs at time t in order to produce delayed rewards at time $t + 1$. As a general matter, an individual will make an investment at time t, if the immediate costs are less than the delayed future payoffs, properly discounted to take into account the uncertainty regarding the delayed payoffs and to account for the offender's impatience. This long-term impatience, modeled in the usual fashion, using an exponential function, includes not just psychological based impatience, but also the general time value of money—which captures the return from investing instead in a risk-free asset, at the market risk-free return.

counted on, and escaping justice. The transaction costs of crime will thus play a larger role in their cost-benefit calculus, when deciding whether or not to commit a crime. It follows that if society fails to take into account these transaction costs of crime, offenders will be overdeterred.

1. *Planning Crimes Under Uncertainty*

During the planning phase, offenders must take into account the uncertainty surrounding the crime, and determine how much to expend to acquire information to reduce this uncertainty.[117] These immediate planning expenditures may produce negative returns if the offender decides not to commit the crime, is caught before he has completed it, or right afterwards, before he has received the full fruit from his labors.

Offenders may be uncertain about the magnitude of the punishment that they will face if caught, which will depend on the intricacies of sentencing guidelines or norms and whether the crime results in injuries, death, or collateral damage to property. Offenders are often uncertain about the likelihood that they will be caught, convicted, and punished. A victim may be an undercover police officer; there may or may not be witnesses, surveillance cameras, or other means of capturing and preserving other characteristics of an offender that can later be used to identify and convict him.

Third parties (who may or may not become an actual victim in a future crime) may also expend resources to protect themselves from crime,[118] and in doing so, increase the transaction costs faced by offenders. In some instances, potential victims are in the best position to take precaution against crime at the lowest cost. For example, a casino owner concerned that employees will embezzle cash proceeds can install CCTV cameras and adopt internal control mechanisms[119] to detect and punish errant employees.[120] Society can provide an incentive to victims to take greater precaution by reducing their own enforcement efforts, which will have the

---

[117] *See, e.g.*, Kenneth J. Arrow, *Information and Economic Behavior*, *in* COLLECTED PAPERS OF KENNETH J. ARROW: THE ECONOMICS OF INFORMATION 136, 138–40 (4th ed. 1984) (discussing the role of information in reducing uncertainty and its value to economic actors who are thus willing to pay to acquire it).

[118] *See* Keith N. Hylton, *Optimal Law Enforcement and Victim Precaution*, 27 RAND J. ECON. 197, 198 (1996) (describing under-enforcement scheme aimed at providing victims with incentive to take precautions).

[119] *See* Merrill Lynch & Co. v. Allegheny Energy, Inc., 229 F.R.D. 441, 448 (S.D.N.Y. 2004) (defining "internal control" mechanism as "a process—effected by an entity's board of directors, management, and other personnel—designed to provide reasonable assurance regarding . . . : (a) reliability of financial reporting, (b) effectiveness and efficiency of operations, and (c) compliance with applicable laws and regulations").

[120] *See* Matthew Bunn & Kathryn M. Glynn, *Preventing Insider Theft Lessons from the Casino and Pharmaceutical Industries*, 41 J. NUCLEAR MATERIALS MGMT. 4, 6 (2013) (describing process of pre-employment screening and post-employment monitoring, training, and access restriction).

effect of exposing victims to a greater risk of loss.[121] Alternatively, society can subsidize private actors to undertake due care against crime.[122]

Similarly, offenders may be uncertain about the expected benefits from committing a crime. A bank robber may be uncertain about how much money is in the bank vault; a mugger, about the contents of a victim's wallet; a murderer, about the utility that he will receive from seeing the victim dead.[123] Faced with uncertainty about the benefits from crime, an offender may invest in "searching" for the best possible crime to commit, in the same way a consumer may search for the best seller of the good she wants to buy.[124]

2. *Executing Crimes*

Offenders also incur transaction costs when they carry out the crime. Even if there are no immediate monetary outlays, the offender will still experience immediate disutility from the exertion of effort, the anxiety of getting caught, and moral conflict.[125] One would expect that the amount of effort and level of anxiety will increase the greater the likelihood that the offender will be caught in the act. What is important is the offender's subjective probability[126] that he will encounter resistance from a victim or that the police will arrest him *in medias res* or right after completing the crime. The likelihood that any of these will occur will tend to increase, the greater the level of digital policing, and the more that society shifts

---

[121] *See* KEITH HYLTON, AN ECONOMIC APPROACH TO CRIMINAL PROCEDURE (describing goal of providing victims incentive to take due care by exposing them to part of the loss from any enforcement shortcomings).

[122] In other words, if it would cost society $1,000 in enforcement expenditures to deter crime, but a private party can do so for $250, one can maximize social welfare by making a $250 transfer to the private party to invest in prevention. For example, they can be given a $250 tax credit if they purchase and install a CCTV camera.

[123] James Q. Wilson & Allan Abrahamse, *Does Crime Pay?*, 9 JUST. Q. 359, 367, 375 (1992) (finding that criminals consistently miscalculate the net expected benefits of committing crimes).

[124] *See* George J. Stigler, *The Economics of Information*, 69 J. POL. ECON. 213, 213 (1961) (discussing consumer search decisions).

[125] Even when moral strictures are not sufficient to deter criminal activity, they can still create internal moral discord. While some criminals are morally bankrupt or at least morally agnostic, one cannot adopt a blanket assumption. One can plausibly assume that some potential wrongdoers give weight to moral norms or at least deliberate in their shadow. The cognitive dissonance literature is concerned with explaining how individuals may, over time, change their internalized moral rules in order to make them comport more closely with their acts of misconduct. Whether or not a person engages in this type of moral arbitrage in response to their acts of misconduct, it is likely that such a person had moral reasons, at least in the back of his mind, when deciding whether or not to engage in misconduct. In other words, it is unlikely that a person can completely turn off his moral compass, at least in the deliberate types of misconduct that concern us and which are the ones likely to lead to dissonance adjustments. *See* JONATHAN BARON, THINKING AND DECIDING 217–19 (4th ed. 2000) (providing an overview of the cognitive dissonance literature).

[126] *See* SHAVELL, *supra* note 23, at 503–04 (noting that, for deterrence purposes, an offender's belief of the probability of detection is more important than the actual probability).

towards preventive policing regimes.

3. *Covering-Up Crimes*

Criminals must also expend resources and exert effort to avoid detection after the crime, such as disposing of incriminating evidence and doing other things to cover-up their tracks.[127] These immediate costs can be higher for repeat offenders and co-conspirators at least to the extent that their activities involve greater levels of deception, anxiety, and effort at keeping stories straight and remembering who has been told what, as well as who may have overheard, detected inconsistencies, or otherwise become suspicious. Moreover, co-conspirators will need to monitor each other to assure that no one will defect in order to get a more lenient sentence.[128]

In conclusion, all other things being equal, the greater the level of digital policing, the more that offenders will have to invest in planning, executing, and covering up their crimes. A lawmaker who fails to take these transaction costs into account will adopt penalty schemes that will overdeter offenders.

E. *Enforcement Errors and Digital Policing*

There are two types of errors in criminal enforcement: an individual who actually committed a crime is "wrongfully acquitted"; or an individual who did not commit a crime is "wrongfully convicted."[129] Both types of errors lead to a dilution in the level of deterrence.

If a portion of guilty offenders are wrongfully acquitted, potential offenders, as a group, will be underdeterred. If innocent individuals are wrongfully convicted, law abiding citizens, as a group, will have a greater incentive to violate the law. A potential offender will commit a crime only if the net benefits from crime are greater than the net benefits from obeying the law. Suppose that the expected benefits from committing a crime are $450 and the expected sanctions are $350, leaving a net benefit of $100. Further suppose that if the offender instead chooses to obey the law, he will receive a net benefit of $150. An individual, for example, may choose between exerting effort to commit a crime and exerting effort to engage in lawful employment, where the efforts from a lawful job yield, in this case, a net benefit of $150. If the probability of a wrongful conviction is zero,

---

[127] *See* Chris William Sanchirico, *Detection Avoidance*, 81 N.Y.U. L. REV. 1331, 1352–60 (2006) (discussing empirical evidence on avoidance costs incurred by offenders).

[128] *See* Neal Kumar Katyal, *Conspiracy Theory*, 112 YALE L.J. 1307, 1350–53 (2003) (describing monitoring costs within conspiracies to prevent defections).

[129] *See* United States v. Havens, 446 U.S. 620, 626 (1980) (stating that "finding the truth is a fundamental goal of our [criminal justice] system"); United States v. Nobles, 422 U.S. 225, 230 (1975) (identifying that two important properties of the system are assuring that "guilt shall not escape or innocence suffer" (quoting Berger v. United States, 295 U.S. 78, 88 (1935))).

then the potential offender will obey the law, given that the net benefits from lawful employment exceed the net benefits of crime.

Now suppose that the probability of a wrongful conviction is 0.20. This means that obeying the law yields a benefit of $150 minus the wrongfully imposed expected sanctions $350 x 0.20 = $70. The net benefit from obeying the law, taking into account the likelihood of a wrongful conviction, is now $80, which is less than the net benefit of $100 that the offender would receive from committing the crime.

Suppose that digital policing reduces the likelihood of wrongful acquittals and wrongful convictions. Since both types of errors dilute the overall level of deterrence, reducing these errors would increase the overall level of deterrence. If lawmakers want to keep the level of deterrence at the same level as before, then they would have to either reduce the gross sanctions or the probability of detection. Digital policing, as we have seen, leads to an increase in the probability of detections. It follows that lawmakers would have to reduce the gross sanctions in order to keep the level of deterrence the same.

Suppose instead that digital policing leads to an increase in both types of error. Increasing digital surveillance, for example, can in some instances increase the likelihood of a wrongful conviction. Certain types of digital surveillance will be given undue weight by juries. This is true of DNA, which can both decrease and increase the likelihood of wrongful convictions.[130] Moreover, individuals who appear in police databases, due to prior convictions, prior arrests, *Terry* stops, or for other reasons, are more likely to show up on police dashboards and police suspect lists. Recorded individuals make more salient suspects, which can lead to wrongful convictions.

As we have seen, when the probability of error increases, deterrence is diluted. Lawmakers, therefore, would have to increase the expected sanctions to keep the level of deterrence the same. This means that they would either have to increase the probability of detection or the gross sanctions.

F. *Marginal Deterrence and Digital Policing*

Some crimes cause more harm than others. If sanctions for each possible crime are set to the optimal level, then an offender will properly internalize the harm that he creates, regardless of the crime that he chooses

---

[130] *See* Manuel A. Utset, *Telling Differences Observational Equivalence and Wrongful Convictions*, 2008 UTAH L. REV. 49, 79 (2008) (discussing the tendency of DNA evidence to increase rather than decrease potential mistaken convictions "whenever a jury gives undue weight to the invariance condition . . . and not enough weight to potential variance conditions—for example, the fact that an innocent defendant's DNA could have been left behind at the crime scene for some other reason").

to commit. But sanctions, as we have seen, are not always set optimally.

Suppose that this is the case, and an offender, who is undeterred, is choosing between a more harmful and less harmful crime. A lawmaker would want to incentivize the offender to choose the less harmful crime. It can do so by setting the expected sanctions for the more harmful crime higher than those for the less harmful crime. More generally, marginal deterrence requires that a lawmaker adopts a penalty scheme in which more serious crimes are penalized more heavily.

As we saw above, under digital policing, enforcement is more general in nature. General enforcement equalizes the probability of detections across different crimes. This leaves lawmakers with one option for achieving marginal deterrence: a system of escalating gross sanctions in which more serious crimes get penalized more heavily. However, there is a limit to how high one can set sanctions.

It follows that digital policing's general enforcement approach should lead to a reduction of the gross penalty for less harmful crimes. But gross sanctions can only be reduced so much—at some point the only solution would be to decriminalize the less serious crimes.

IV. OTHER CRIMINAL LAW IMPLICATIONS OF DIGITAL POLICING

This Section develops some additional implications from the expansion of digital and preventive policing. It begins by examining the interaction between preventive policing and an offender's bounded rationality. It then argues that preventive policing can be characterized as an analogue of "incapacitation." This Section then examines the relationship between preventive policing and inchoate crimes, such as criminal attempt, conspiracy, and solicitation, as well as their relationship with the entrapment defense. Section IV concludes by examining the implications of digital and preventive policing on police searches, on plea bargains, and police corruption.

A. *The Bounded Rationality of Offenders*

When crimes do not call for total deterrence, the goal of criminal sanctions is to cause offenders to internalize the social harm produced by their crimes. To do so efficiently, society needs to signal as clearly as possible the probability of detection and the gross sanctions. But committing crimes is a complex undertaking. In deciding whether to commit a crime, an offender will need to make probability assessments about the expected benefits and expected costs of committing a crime, both of which require further probabilistic assessments regarding such matters as the level of law enforcement and vigilance, prophylactic actions of potential victims, and gross sanctions. When offenders have bounded rationality, society should make information about expected sanctions not

only clear but salient as well. Salience, in other words, is one way of overcoming an offender's potential bounded rationality and inattention.

If offenders are risk averse, then there is an even greater incentive for society to reduce the uncertainty faced by inattentive offenders. The police can make their enforcement presence salient by using uniformed officers or by installing CCTV cameras that are easy to identify. Society may also want to reduce the discretion given to the police, prosecutors, and judges, regarding enforcement activities and gross sanctions, since discretion increases the uncertainty faced by offenders.

B. *Incapacitation*

In the real world, there is a greater amount of imprisonment than what the economics approach would predict. One possible explanation is that if offenders are behind bars they are unable to commit other crimes. In prison, offenders have no real privacy—at an extreme, they are subject to continual surveillance.[131] But from a social welfare perspective, one must also take into account the costs of administering the prison system and the tangible and intangible costs borne by the offender.

Since the goal is to minimize aggregate social costs, it really does not matter how this "incapacitation" occurs. In fact, one economic rationale for the parole system and halfway houses is to allow for partial incapacitation: parole officers are able to more directly monitor released offenders and determine whether they are reverting to lives of crime. Once an offender is in the system, it is easier to surveil her. New surveillance technologies give the police instant dashboard access to the background of potential suspects. This will allow the police to better prevent potential repeat offenders from reoffending. This sort of real-time deterrence brought about by digital and preventive policing regimes can be seen as a substitute for incapacitation.

C. *Preventive Policing and Inchoate Offenses*

The criminal law punishes offenders who, with the requisite culpable state of mind,[132] harm others.[133] Some crimes, however, punish offenders,

---

[131] *See* 4 JEREMY BENTHAM, *Panopticon Or, The Inspection-House*, *in* THE WORKS OF JEREMY BENTHAM 40–41 (John Bowring ed., 1843) (proposing the Panopticon, a prison designed so that inmates could be constantly observed by a single watchman); MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 200–01 (Alan Sheridan trans., 1995) (discussing Bentham's Panopticon).

[132] 2 WAYNE R. LAFAVE, SUBSTANTIVE CRIMINAL LAW § 5.1 (2d ed. 2003).

[133] An individual convicted of a crime may lose his freedom and be stigmatized. Not surprisingly, criminal law requires clear statements of the types of actions that will trigger liability—moreover, courts will interpret the law narrowly whenever there is ambiguity or vagueness. *See* Rose v.

notwithstanding the fact that they did not harm anyone. These inchoate crimes include criminal attempt, conspiracy, and solicitation. Inchoate crimes are difficult to explain under both the economics and retributivist approaches to criminal law.[134] With the increased prominence of digital and preventive policing, one would expect that law enforcement will make increased use of inchoate offenses.

1. *Criminal Attempt*

Criminal attempt allows the police to arrest an offender before they have completed a crime. An individual will trigger inchoate liability for criminal attempt whenever he has taken substantial steps toward the commission of the underlying crime.[135] If A shoots at B with the intent of killing her, but misses, he is chargeable for attempted murder.[136] If it turns out that A thought was B was really a "dummy" that looked like B, A nonetheless triggers attempt liability.[137] Finally, if A raises his rifle and takes aim at B, but the police intervene in the nick of time, before he has fired, A is once again chargeable for attempt, given that aiming the rifle at B is sufficient to constitute a substantial step.[138] Attempt liability, in short, is an important tool for preventive policing regimes, since it allows the police to stop a crime before it has reached a point of no return, when the harm has been unleashed.

2. *Conspiracy and Solicitation*

Conspiracy and solicitation are also useful tools for preventive policing. Conspiracy liability is triggered whenever two or more

---

Locke, 423 U.S. 48, 49 (1975) (per curiam) (holding that criminal law must give adequate warning of what is prohibited); Papachristou v. City of Jacksonville, 405 U.S. 156, 170–71 (1972) (striking down an ordinance for giving too much discretion to police in its application).

[134] From a retributivist perspective, an offender is punished because his actions have harmed others, and thus he deserves to be punished, but a person who shoots at another and misses does not directly harm the intended victim and does not deserve to be punished. *See* Leo Katz, *Why the Successful Assassin Is More Wicked Than the Unsuccessful One*, 88 CAL. L. REV. 791, 795 (2000) (describing difficulty for retributivist in dealing with inchoate offenses); Leo Zaibert, *The Moralist Strikes Back*, 14 NEW CRIM. L. REV. 139, 145 (2011) (describing how the punishment of the deserving legitimizes the system).

[135] *See* MODEL PENAL CODE § 5.01(1)(c) (AM. LAW INST. 1985) ("[Criminal attempt is] an act or omission constituting a substantial step in a course of conduct planned to culminate in [the offender's] commission of the crime.").

[136] *See id.* § 5.01(1)(b) (including cases in which the action or omission is done with belief that "without further conduct on his part" it would result in crime).

[137] *See id.* § 5.01(1)(a) (including cases in which the offender "purposely engages in conduct that would constitute the crime if the attendant circumstances were as he believes them to be").

[138] *See id.* § 5.01(1)(c) (including cases in which the offender is interrupted in the criminal act and cannot complete it).

individuals agree to engage in criminal conduct or aid in the commission of a crime.[139] Unlike attempts, there is no need for conspirators to take substantial steps toward the commission of the underlying crime; all that is needed is for them to reach an agreement.[140] Moreover, while a wrongdoer may only be charged for an attempt or the actual offense,[141] co-conspirators can be charged and convicted for being part of the conspiracy, as well as for any offense committed by any of the conspirators.[142]

An offender triggers liability for solicitation to commit a crime "if with the purpose of promoting or facilitating its commission he commands, encourages or requests another person to engage in specific conduct that would constitute such [a] crime."[143] An offender may commit the crime himself or delegate its execution to a second party—a rational offender will delegate the commission of a crime whenever he determines that the expected benefits are greater than the aggregate expected cost from delegation.[144] Like criminal attempt and conspiracy, the crime of solicitation allows law enforcement to intervene earlier in the criminal process and prevent potential crimes.

D. *Preventive Policing and Entrapment*

Preventive policing often uses undercover officers. While undercover techniques are useful for a variety of crimes that are not susceptible to traditional enforcement procedures, they increase the potential for police

---

[139] *See* MODEL PENAL CODE § 5.03 (AM. LAW INST. 1985) (explaining that conspiracy liability is triggered when a person agrees with another "to engage in conduct that constitutes [a] crime or an attempt or solicitation to commit such crime" or "agrees to aid [another] in the planning or commission of such crime or an attempt or solicitation to commit such a crime"). *See also* Pettibone v. United States, 148 U.S. 197, 203 (1893) ("A conspiracy is . . . a combination of two or more persons, by concerted action, to accomplish a criminal or unlawful purpose, or some purpose not in itself criminal or unlawful, by criminal or unlawful means . . . .").

[140] *See* MODEL PENAL CODE § 5.03 (AM. LAW INST. 1985). This is the case in common law conspiracies; however, some conspiracy statutes require some overt action toward commission of the underlying crime. *See, e.g.*, N.Y. PENAL LAW § 105.20 (Consol. 1998).

[141] *See* LAFAVE, *supra* note 133, § 11.5(c) (describing the merger rule for criminal attempt).

[142] *See* Pinkerton v. United States, 328 U.S. 640, 643–44, 646–47 (1946) (holding that a defendant can be convicted for both conspiracy and the underlying offense); LAFAVE, *supra* note 133, § 12.2(b).

[143] *See* MODEL PENAL CODE § 5.02(1) (AM. LAW INST. 1985) (defining criminal solicitation and also defining solicitation to mean an act that would constitute an attempt or would trigger complicity liability).

[144] Suppose that A wants to break into B's house and steal a valuable painting. If A carries out the crime alone he will keep all of the proceeds and bear the expected cost from the burglary—the planning, execution, and cover-up costs, as well as the expected sanctions for stealing the painting. A, however, may decide that he prefers to delegate the criminal task to C. He may do so because he believes that C is a more efficient thief in the sense that he can accomplish the crime at a lower expected cost—including the likelihood of being detected. A may also decide to delegate because he does not want to bear the direct and salient disutility from committing the crime. Direct involvement is more likely to trigger disutility from violating moral strictures, for example.

misconduct.[145] Under the Model Penal Code, a defense is available when the police employ "methods of persuasion or inducement that create a substantial risk that such an offense will be committed by persons other than those who are ready to commit it."[146] This entrapment defense makes economic sense: the goal of deterrence is to deter offenders who planned to commit crimes that would harm third parties, not to use enforcement resources to stimulate unplanned criminal activity.[147]

E. *Surveillance and Warrants*

Each time that an offender commits a crime, she leaves behind an evidence trace that can, if detected, affect her future wellbeing. In order to arrest an offender, the police must have probable cause. To show cause the police must present particularized evidence, coming from public or private sources. Public evidence includes any piece of evidence available to the police without getting a search warrant. Private evidence requires the police to first get a search warrant.

In order to avoid detection, an offender will have an incentive to minimize the amount of public evidence. In some instances, there will not be sufficient public evidence to allow the police to make an arrest or even to get a search warrant to get access to private evidence.

As the costs of digital surveillance have gone down, the ability of the police to observe and gather public evidence of crimes has increased. This, in turn, has made it easier to get search warrants and gather sufficient evidence to have probable cause to make an arrest. The focus on the public/privacy divide in search warrant jurisprudence has given an incentive to the police to invest in surveillance technology that allows them to observe and gather a greater amount of crime-related public evidence. At the same time, it has led some offenders to invest in technology, such as cryptography, that reduces the amount of evidence that is in the public sphere.

F. *Plea Bargains and Surveillance*

To the extent that digital surveillance and other preventive policing techniques allow the authorities to collect a greater amount of evidence, it will increase the probability that an offender, once caught and brought to trial, will be convicted. This will increase the likelihood that an offender

---

[145] *See* Sorrells v. United States, 287 U.S. 435, 441–42 (1932) (stating that "[a]rtifice and stratagem may be employed" by police because they are often necessary "to reveal the criminal design," but not "when the criminal design originates with the officials of the Government, and they implant in the mind of an innocent person the disposition to commit the alleged offense").

[146] MODEL PENAL CODE § 2.13(1)(b) (AM. LAW INST. 1985).

[147] *See* SHAVELL, *supra* note 23, at 564–65 (arguing that individuals who had not intended to commit crimes do not need to be deterred).

will agree to a plea bargain. In a plea bargain, like in other bargaining scenarios, two parties are trying to decide whether to settle or take the case to trial.

A bargaining breakdown, and thus a trial, is more likely the greater the uncertainty about the outcome of the trial. If the authorities are able to reduce this uncertainty by gathering more evidence, they are in essence reducing the variance around a defendant's expected costs from going to trial. By reducing the variance, the defendant will be able to make a more accurate assessment about the expected costs from proceeding to a trial. As long as the settlement offer is less than these expected costs, offenders will be more likely agree to the plea bargain.

G. *Corruption and Law Enforcement.*

Increased surveillance should lead to a decrease in the level of police corruption. This is particularly the case when offenders are surveilled through multiple means by multiple parties. For example, assume that the authorities have three sources of surveillance and that each is carried out by a different agency. This means that if one monitor decides to collude with the offender, there is still a possibility that one or both of the other monitors will still gather enough evidence to arrest and convict the offender. Once arrested, the offender will have an incentive to turn on his collusion partner in return for a lighter sentence. Additionally, the very act of collusion between the offender and monitor may be recorded by the other monitors. In either case, increased surveillance, particularly when carried out by overlapping monitors, will lead to a reduction in police corruption.

CONCLUSION

Technology advances have helped change the face of law enforcement. They have led to the increased use of digital policing and preventive policing. Both of these create important privacy and criminal procedure concerns. While commentators and policymakers have given great attention to these concerns, they have largely overlooked a set of collateral effects brought about by digital and preventive policing. This Article identified and examined the implications for deterrence theory and the substantive criminal law of the proliferation of digital policing.

It shows that digital policing techniques help reduce the complexity of law enforcement and create economies of scale. It also shows that by reducing the complexity of law enforcement, digital policing has allowed society to shift its enforcement focus from investigative policing to preventive policing, which is a much more complex undertaking. The Article's main contribution is showing that digital and preventive policing will lead to inefficient overdeterrence, unless lawmakers reduce the gross

sanctions for criminal misconduct. This is true for first-time offenders and for repeat offenders. But in the latter case, the problem is magnified by the fact that the digital footprint left behind by an offender who is caught and convicted will make it much easier for the authorities to identify, arrest, and convict repeat offenders.