CRIMINAL INNOVATION AND THE WARRANT REQUIREMENT: RECONSIDERING THE RIGHTS-POLICE EFFICIENCY TRADE-OFF

TONJA JACOBI* AND JONAH KIND**

ABSTRACT

It is routinely assumed that there is a trade-off between police efficiency and the warrant requirement. But existing analysis ignores the interaction between law-enforcement investigative practices and criminal innovation. Narrowing the definition of a search or otherwise limiting the requirement for a warrant gives criminals greater incentive to innovate to avoid detection. With limited resources to develop countermeasures, law enforcement officers will often be just as effective at capturing criminals when facing higher Fourth Amendment hurdles. We provide a game-theoretic model that shows that when law-enforcement investigation and criminal innovation are considered in a dynamic context, the police efficiency rationale for lowering Fourth Amendment rights is often inapt. We analyze how this impacts both criminal activity and innocent communications that individuals seek to keep private in the digital age. We show that both law-enforcement and noncriminal privacy concerns may be better promoted by maintaining the warrant requirement.

* William G. And Virginia K. Kames Research Professor, Northwestern University School of Law. t-jacobi@law.northwestern.edu. The authors thank Song Richardson, Matthew Sag, and Deborah Turkheimer for their helpful comments.

** Law Clerk to the Honorable Joel M. Flaum, U.S. Court of Appeals, Seventh Circuit.

TABLE OF CONTENTS

INTRODUCTION

"Little" Melvin Williams was an infamous heroin and cocaine trafficking kingpin in Baltimore in the 1970s and early 1980s.[1] When the police began investigating Williams's operation, they discovered that his gang had taken many ingenious measures to avoid police detection.[2] One such innovation was the invention of a secret code for pager communications between members of the gang.[3] Why create a special code? Because U.S. Supreme Court doctrine allows police, without a warrant, to monitor telephone numbers dialed on the public payphones the gang used to send messages to pagers. The content of the messages was the telephone number that the recipient was supposed to call.[4] The gang invented a way to mask the messages that were sent to the pagers—each number was replaced by the number opposite the "5" on the keypad, and "5" was replaced with "0."[5]

It made sense to invent a code for pager messages and to teach the code to its members because the gang knew the police could otherwise identify the pager numbers without the cost and evidentiary burden of acquiring a warrant.[6] Law enforcement officers (LEOs)[7]

---

1. Ericka Blount, *Respect*, BALT. MAGAZINE, Sept. 2004, *available at* http://perma.cc/8C8R-8LDK.

2. Much of the first season of the HBO drama "The Wire" is based on this investigation. RAFAEL ALVAREZ, THE WIRE: TRUTH BE TOLD 48 (2009).

3. *Id.*

4. Smith v. Maryland, 442 U.S. 735 (1979) (allowing use of a pen register even on a home telephone).

5. ALVAREZ, *supra* note 2, at 49.

6. The fact that the police were able to obtain a warrant for the clone beepers does not mean that they would have been able to obtain a warrant for a pen register on public payphones. Given that the Court in *Katz v. United States* found that there was a reasonable expectation of privacy in a public telephone booth being used to make phone calls, a judge would have been more reluctant to allow surveillance of a public phone, usable by anyone, than a private beeper used by a suspected criminal. 389 U.S. 347, 352-53 (1967). Even if the police had met the evidentiary burden for a warrant regarding the payphones, the extra bureaucratic, political, and time costs imposed by a warrant requirement may have derailed the investigation at this earlier stage, mitigating the incentive for a secret code.

7. Our analysis applies to policing at all levels, including federal agents, so we use the general term law enforcement officer. When discussing the common assumption that law-enforcement investigations are aided by lax or no warrant requirements, however, we use the term Police Efficiency Assumption, consistent with most judicial analyses on the topic. *See,*

are more likely to use investigative techniques like tracking telephone calls when they can avoid the costs of obtaining a warrant. When LEOs are not bound by the warrant requirement, the expected benefits of an investigation (the possibility of finding evidence) are more likely to outweigh its costs (the time and effort expended by investigation). But when faced with a higher likelihood that law enforcement will investigate their crimes, criminals have a greater incentive to try to cover up each crime: in other words, to innovate. That criminal innovation, inspired by law enforcement's ability to investigate without a warrant, may slow down an investigation as much as the warrant requirement. The Williams gang's innovation made the LEO investigation much more difficult because the police had to create "clone" pagers, which shared the same telephone numbers as the gang members' pagers.[8] The police were eventually able to crack the code, but the innovation significantly delayed the police investigation, and could easily have derailed it entirely.[9]

Today, instead of pager codes, criminal conspiracies commonly use prepaid cell phones for communication[10] because those devices are harder for LEOs to trace or to tie to specific people.[11] Prepaid phones are inexpensive, allowing criminals to dispose of them frequently to avoid being linked to the calls made.[12] They are also more difficult to trace because purchasers can provide false names and addresses to phone providers.[13] But inventing pager codes and purchasing prepaid cell phones are only two of the many actions criminals can take to avoid being identified. Even casual observers of detective stories and crime capers will be familiar with many other mechanisms of classic crime detection avoidance. Bank robbers

e.g., Riley v. California, 134 S. Ct. 2473, 2493 (2014). When appropriate, we differentiate between police and other LEOs because, as discussed later in this Section, some policing will be more reactive, and thus less amenable to a strategy of countermeasures than others.

8. A process that did itself require warrants.

9. ALVAREZ, *supra* note 2, at 48-49 (describing the process of breaking the beeper code).

10. *See, e.g.*, United States v. Skinner, 690 F.3d 772, 775 (6th Cir. 2012) (describing a criminal conspiracy to transport hundreds of pounds of marijuana from Arizona to Tennessee utilizing prepaid throwaway cell phones).

11. Eoghan Casey & Benjamin Turnbull, *Digital Evidence on Mobile Devices*, *in* DIGITAL EVIDENCE AND COMPUTER CRIME 1, 6 (3d ed. 2011); Toine Spapens, *Interaction Between Criminal Groups and Law Enforcement: The Case of Ecstasy in the Netherlands*, 12 GLOBAL CRIME 19, 28-29 (2011).

12. *See* Casey & Turnbull, *supra* note 11, at 6.

13. Spapens, *supra* note 11, at 28-29.

use masks to prevent identification by witnesses, burglars use gloves to hide their fingerprints, and gunmen use silencers so that their crimes do not attract attention.[14]

In the digital age, many forms of sophisticated detection avoidance have been developed, from simple steps such as anonymous e-mail accounts, to complex encryption of computer programs to mask the content of computer files and Internet activity, to convoluted rerouting of internet traffic to avoid location identification. For example, the reopened "Silk Road" Internet marketplace, which serves as an online black market, primarily for illegal drugs,[15] has multiple mechanisms to avoid law-enforcement investigations. Users are required to install the Tor network, a software system that facilitates anonymity by rerouting IP addresses behind firewalls and using multiple layers of encryption.[16] Only the unregulated electronic currency "Bitcoin" is accepted,[17] and sellers are required to delete all unique buyer information after confirmation of an item's arrival.[18] All of these mechanisms provide additional assurances of anonymity.

Clearly, criminal innovations can take many forms, including new business methods as well as traditional masking techniques. Innovations are costly in time and effort but are undertaken because they reduce the likelihood that criminal participants will be caught. The possibility of warrantless investigations intensifies these behaviors. For example, some of the Silk Road innovations are designed specifically to avoid warrantless law-enforcement investigations. LEOs need only a subpoena—not a warrant backed by probable cause—to install the computer equivalent of a pen register, which allows them to track "the to/from address of [a suspect's] e-mail messages, the IP addresses of the websites that [a suspect]

14. For more examples of these behaviors, see Jacob Nussim & Avraham D. Tabbach, *Controlling Avoidance: Ex Ante Regulation Versus Ex Post Punishment*, 4 REV. L. & ECON. 45, 45 (2008).

15. Emma Moore, *Online Subterfuge: Silk Road, Tor and Bitcoins*, BROWN POL. REV. (Nov. 13, 2013, 11:00 AM), http://www.brownpoliticalreview.org/2013/11/online-subterfuge-silk-road-tor-and-bitcoins/ [http://perma.cc/B2U2-SF7U].

16. *Silk Road—An Overview of the Online Marketplace*, SILK ROAD DRUGS (Apr. 18, 2013), http://silkroaddrugs.org/silkroad-drugs-complete-step-by-step-guide/ [http://perma.cc/F2PW-4RQZ].

17. *Id.*

18. *See* Moore, *supra* note 15.

visited and the total volume of information sent to or from [a suspect's Internet] account."[19] The National Security Agency (NSA) can, without a warrant, analyze identifying information, such as IP addresses, in communications between Americans and foreigners and can search its massive databases of communications data—some of it solely domestic—for the identifying information of specific individuals.[20] The Silk Road's built-in protections from such warrantless investigatory powers make the job of investigators much more difficult—perhaps as difficult as it would be if the warrant requirement were applied to tracking IP addresses.[21]

Local police and federal agents often undertake large-scale, sometimes multiyear, multiagency investigations that involve a back-and-forth between criminal innovation and law-enforcement counterresponse. This is illustrated by the international tracking and capture of Joaquín Guzmán Loera, also known as "El Chapo," chief of the world's biggest drug-trafficking cartel, Sinaloa in Mexico, who was involved in a combination of high-tech and low-tech criminal innovation.[22] Guzmán evaded the Drug Enforcement Administration (DEA), Mexican intelligence, and special forces, among other agencies, for eight years by using both sophisticated encryption programs and simple avoidance of direct phone conversations, combined with a complicated system of intermediaries and relays:

> If you needed to communicate with the boss, you could reach him via B.B.M., BlackBerry's instant-messaging application.... Your message would go not directly to Guzmán, however, but to a

19. United States v. Forrester, 512 F.3d 500, 505 (9th Cir. 2007).

20. James Ball & Spencer Ackerman, *NSA Loophole Allows Warrantless Search for U.S. Citizens' E-mails and Phone Calls*, GUARDIAN (Aug. 9, 2013, 12:08 PM), http://www.theguardian.com/world/2013/aug/09/nsa-loophole-warrantless-searches-email-calls [http://perma.cc/AQN9-KRAJ].

21. Although investigators were able to take down the original Silk Road and arrest multiple people involved in the market, including its leader, Ross Ulbricht, they did so through old-fashioned (non-cyber) police work, lucky breaks (such as a Postal Inspector's detection of illegal substances in a package), and exploiting one amateurish mistake by Ulbricht. Kim Zetter, *How the Feds Took Down the Silk Road Drug Wonderland*, WIRED (Nov. 18, 2013, 6:30 AM), http://www.wired.com/2013/11/silk-road/ [http://perma.cc/C9KC-LENJ].

22. Patrick Radden Keefe, *The Hunt for El Chapo*: *How the World's Most Notorious Drug Lord Was Captured*, NEW YORKER (May 5, 2014), http://www.newyorker.com/magazine/2014/05/05/the-hunt-for-el-chapo [http://perma.cc/3LH8-SU5Z].

> trusted lieutenant, who spent his days in Starbucks coffee shops and other locations with public wireless networks. Upon receiving the message, the lieutenant would transcribe it onto an iPad, so that he could forward the text using WiFi—avoiding the cellular networks that the cartel knew the authorities were trolling. The transcribed message would be sent not to Guzmán but to a second intermediary, who, also using a tablet and public WiFi, would transcribe the words onto *his* BlackBerry and relay them to Guzmán. Although Guzmán continued to use a BlackBerry, it was almost impossible to track, because it communicated with only one other device.[23]

This "mirror" system was almost impossible for the authorities to penetrate, but by studying the patterns of the cartel's communications, the DEA was able to locate Guzmán's intermediaries, and eventually physically locate him at the home of a coconspirator.[24]

From balaclavas to computer encryption, all of these criminal behaviors decrease, to a greater or lesser extent, the probability that LEOs will find evidence linking an individual to a crime. In this Article, we consider all such measures under the general concept of "criminal innovation." These are actions that take place prior to a criminal's arrest to avoid identification, as opposed to actions taken following an arrest to avoid conviction, such as influencing witnesses or consulting experts.[25]

Most forms of criminal innovation are uninteresting to analyze because due to their low cost and large benefit, criminals will have a clear incentive to make use of them, and law enforcement can do little to counteract their effectiveness. For a criminal robbing a bank, wearing a mask is obviously an optimal choice because this tool of innovation is easy to obtain, inexpensive, and will make it much more difficult for witnesses to identify the robber. Police can do little to lift such a veil. That does not mean that police do not innovate to counteract criminal innovation, but most street policing is reactive, and countermeasures are generally developed at the policy level, rather than in response to specific criminal behavior. Criminal innovation and law-enforcement countermeasures become

---

23. *Id.*

24. *Id.* Guzmán temporarily escaped through a system of hidden tunnels before being captured shortly thereafter. *Id.*

25. *See* Nussim & Tabbach, *supra* note 14.

more interesting when considering marginal innovations, which criminals will make only in some situations. For example, it only makes sense to use prepaid cell phones if the decreased likelihood of law-enforcement detection outweighs the added cost of their use. Likewise, developing and implementing high-tech encryption programs is costly and time consuming, and only worthwhile as long as the criminal stays one step ahead of LEO countermeasures.[26] It is obvious that criminals will want to innovate, but because innovation is often costly, the interesting question is this: When will innovation be worthwhile?

We show that a major factor in that calculation is whether the warrant requirement applies to law-enforcement countermeasures. When policing is not simply reactive to immediate instances of criminal behavior, but involves longer-term investigation, such as when federal agents take on high-level drug and gun rings, the Fourth Amendment generally requires LEOs to obtain a warrant before conducting a search, which requires probable cause,[27] or even higher evidence of criminality.[28] But the courts do not consider many types of law enforcement activity to be searches for Fourth Amendment purposes, and so LEOs do not need to obtain warrants to act.[29] For instance, the Sixth Circuit Court of Appeals recently held that tracking a suspect's movements via his cell phone data was not a "search" for Fourth Amendment purposes, and so the

26. For descriptions of the recent "encryption wars" between LEOs and criminals in the United States and the United Kingdom, see Sophie Curtis, *National Crime Agency Wages War on Tor "Darknet" Anonymity*, TELEGRAPH (Oct. 10, 2013, 3:23 PM), http://www.telegraph.co.uk/technology/internet-security/10369880/National-Crime-Agency-wages-war-on-Tor-darknet-anonymity.html [http://perma.cc/FE5V-SQHW]; and Zachary Graves, *The NSA's War Against Encryption*, HUFFINGTON POST (Sept. 10, 2013, 2:48 PM), http://www.huffingtonpost.com/zachary-graves/the-nsas-war-against-encr_b_3901328.html [http://perma.cc/XV9F-TCQS].

27. *See, e.g.*, Johnson v. United States, 333 U.S. 10, 14 (1948) ("When the right of privacy must reasonably yield to the right of search is, as a rule, to be decided by a judicial officer, not by a policeman.").

28. For instance, an application for electronic surveillance under Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act), 18 U.S.C. § 2518(1)(c) (2012), "must contain a statement affirming that normal investigative procedures have been tried and failed, are reasonably unlikely to succeed if tried, or are too dangerous to employ." *See* U.S. ATTORNEYS' CRIMINAL RESOURCE MANUAL 28 (2012), *available at* http://perma.cc/TQ8H-PYD2.

29. In general, a police investigation is a search if it violates an individual's "reasonable expectation of privacy." Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring); *see* Smith v. Maryland, 442 U.S. 735, 746 (1979) (Stewart, J., dissenting).

warrant requirement did not apply.[30] If the police can ping a cell phone or track it using a Global Positioning System (GPS) without going through the effort of obtaining a warrant, they will be more likely to so investigate. An enterprising criminal will therefore have greater incentive to innovate in order to prevent this type of investigation from succeeding by buying prepaid phones without GPS technology,[31] altering the phones to prevent tracking through pinging, or turning to masked electronic communications. Investigation of crime is a constant back-and-forth between criminal innovation and law-enforcement countermeasures—an "arms race" between criminal innovation and police counterresponse.[32]

We challenge the assumption that requiring LEOs to obtain a warrant prior to undertaking a particular action will always make law-enforcement investigations and prosecutions more difficult. Often, perhaps even usually, not needing a warrant will be better for law enforcement for obvious reasons: officers must expend time and effort to obtain the warrant; the warrant process may create delays that allow for the destruction or concealment of evidence; and having to show probable cause to obtain the warrant means that some investigations will be blocked altogether.[33] However, because criminals can innovate, the assumption of greater law-enforcement efficiency in the absence of the warrant requirement can be wrong.[34]

When LEOs do not need a warrant, they will be more likely—all other things being equal—to investigate because the costs of investigation are lower.[35] However, this lowered cost of investigation will incentivize criminals to innovate more often because innovations lower the likelihood of detection in the event of law-enforcement

30. United States v. Skinner, 690 F.3d 772, 777 (6th Cir. 2012).

31. *See* Orin Kerr, *Sixth Circuit Rules That Pinging a Cell Phone to Determine Its Location Is Not a Fourth Amendment "Search,"* VOLOKH CONSPIRACY (Aug. 14, 2012, 2:02 PM), http://www.volokh.com/2012/08/14/sixth-circuit-rules-that-pinging-a-cell-phone-to-determine-its-location-is-not-a-fourth-amendment-search/ [http://perma.cc/CN42-FURX] (discussing whether the warrant requirement applies to nonprepaid phones).

32. Nina Totenberg, *Weighing the Risks of Warrantless Phone Searches During Arrests*, NPR (Apr. 29, 2014, 3:14 AM), http://www.npr.org/blogs/alltechconsidered/2014/04/29/306262746/weighing-the-risks-of-warrantless-phone-searches-during-arrests [http://perma.cc/6HLM-VB4Z] (describing police attempts to search cell phones before arrestees' co-conspirators remote wipe the devices).

33. *See infra* Part I.B.

34. *See infra* notes 110-12 and accompanying text.

35. *See infra* note 106 and accompanying text.

investigation.[36] In many cases, the gains to LEOs from not having to obtain a warrant will be offset by a decreased likelihood of finding evidence due to increased criminal innovation. We show that abolishing or lowering the warrant requirement will often lead criminals to innovate more regularly, making law-enforcement investigations less likely to succeed. LEOs will not increase their rate of investigation and will not capture more criminals.

One means by which the courts avoid the warrant requirement is by narrowing the range of law-enforcement activities that are considered "searches," eliminating the application of the Fourth Amendment to those investigations. A Fourth Amendment search only occurs, and thus a warrant is only required, if LEOs violate an individual's "reasonable expectation of privacy."[37] The reasonable expectation of privacy test has been derided as circular[38] because an expectation of privacy will depend on the extent to which police regularly breach that expectation;[39] moreover, expectations of privacy will depend on legal decisions, which are supposed to be based on people's expectations of privacy.[40] This circularity can lead to a spiral of ever-decreasing Fourth Amendment rights whereby increased government surveillance erodes people's privacy expectations, making the surveillance legal under the test. Though such a downward spiral decreases the rights of everyone, including noncriminals, it is usually considered at least to have the beneficial

---

36. *See supra* note 21 and accompanying text. This logic does not assume that criminals will know when LEOs have or have not obtained a warrant, but rather that criminals will know when LEOs do and do not *need* to obtain warrants to gather information relevant to their criminal conduct. Although in some cases criminals will be ignorant of the law, many criminal conspiracies will be aware of the extent that the warrant requirement gives them greater protection, and thus greater latitude, as the initial Williams example illustrated.

37. Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring).

38. *See, e.g.*, Richard H. Seamon, Kyllo v. United States *and the Partial Ascendance of Justice Scalia's Fourth Amendment*, 79 WASH. U. L.Q. 1013, 1023-24 (2001) ("Under the test, the less privacy we have ... the less we can reasonably expect. As our reasonable expectations of privacy decrease, the types of government intrusions that will be found to fall outside of the Fourth Amendment (as not constituting searches) increases.").

39. Tonja Jacobi, *The Law and Economics of the Exclusionary Rule*, 87 NOTRE DAME L. REV. 585, 664 (2011) ("[W]hether an expectation of privacy exists will itself depend on the extent to which police regularly breach that expectation.").

40. Richard A. Posner, *The Uncertain Protection of Privacy by the Supreme Court*, 1979 SUP. CT. REV. 173, 188 ("[I]t is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is.").

effect of making it easier for law enforcement to catch criminals. Our analysis, however, demonstrates that this advantage will often be illusory. LEOs will often not have an easier time catching criminals because increased surveillance may simply result in increased criminal innovation. In the cat-and-mouse game between law enforcement and criminals, the reasonable expectation of privacy test will erode the rules of the game without making it easier for the cat to catch the mice; meanwhile, innocent bystanders will receive less Fourth Amendment protection.

Therefore, the dichotomy in the Fourth Amendment literature between police efficiency concerns and criminal rights protections is often a false one. We show that by removing the warrant requirement, law enforcement can sometimes be easier, but often will not be. In circumstances when there is significant uncertainty—by criminals as to whether LEOs will investigate, and by LEOs as to whether criminals will innovate—the assumption of greater efficiency for warrantless searches is incorrect. In such cases, removing the warrant requirement will not make police investigations more effective.

We show that uncertainty is likely to arise frequently. The nonapplication of the warrant requirement will often cause little gain for law enforcement and a significant incursion on the rights of noncriminals. We consider a variety of mechanisms of privacy protection available for digital communications, such as e-mail and more fleeting electronic chatting. We show that some existing digital mechanisms are too costly for the average noncriminal user, but are perfectly calibrated to aid avoidance of detection of criminal behavior and will enable highly effective criminal innovation. Nonapplication of the warrant requirement will only encourage criminal use of such technology, making law enforcement no better off because unraveling powerful e-mail encryption, for example, will be far more difficult than obtaining a warrant. Programs most suited to noncriminal behavior will be left unprotected.

We establish these effects by using a game-theoretic model of criminal innovation and law enforcement countermeasures. An extensive economic literature exists that analyzes the most efficient and effective mechanisms of deterring crime by varying the extent

of punishment, among other factors.[41] But discouraging criminal behavior by changing incentives will change the opportunity cost to law enforcement in choosing any given investigative priority.[42] This in turn will change criminals' expectations of being caught, and thus their incentive to innovate.[43] The interactions between criminals and LEOs must be considered dynamically, in terms of their feedback effects on one another. Unlike previous analyses, we account for this dynamic interaction by employing a game-theoretic model that allows us to simultaneously map the effect of criminal avoidance on the law-enforcement decision to investigate, and vice versa.

This Article describes the "Police Efficiency Assumption"—that law-enforcement investigations are impeded when an investigation is considered a search and a warrant is required—and shows when the Assumption fails. Part I begins by reviewing the law regarding Fourth Amendment searches and showing the distorting effect of the Police Efficiency Assumption. Part II reviews the existing literature on criminal innovation and discusses ways in which innovation can defeat the Assumption. Part III presents a model that demonstrates the conditions necessary for the Assumption to fail. Part IV discusses the policy implications of these results and shows how they apply to mechanisms of ensuring privacy in the digital age, including e-mail encryption and utilization of programs specifically made for destroying communication trails, such as Privnote[44] and Snapchat.[45] It concludes with a discussion of the recent NSA mass data collection and analysis, and shows that the nonapplication of the warrant requirement undermines Fourth Amendment rights more than that recent controversial governmental spying program.

---

41. *See, e.g.*, A. Mitchell Polinsky & Daniel L. Rubinfeld, *A Model of Optimal Fines for Repeat Offenders,* 46 J. PUB. ECON. 291, 292 (1991) (showing that maximal deterrence may require variation in punishment levels by recidivism); Steven Shavell, *A Model of Optimal Incapacitation,* 77 AM. ECON. REV. 107, 107 (1987) (factoring in the value of incapacitating likely reoffenders).

42. *See infra* Part III.B.

43. *See infra* Part III.B.

44. *See About Privnote*, PRIVNOTE, https://privnote.com/about/ [http://perma.cc/GZU6-HS6T] (last visited Feb. 22, 2015).

45. *See* Jenna Wortham, *A Growing App. Lets You See It, Then You Don't*, N.Y. TIMES, Feb. 9, 2013, at A1.

I. THE ROLE OF THE FOURTH AMENDMENT IN LAW-ENFORCEMENT INVESTIGATIONS

The Fourth Amendment sets broad limits on federal and state law-enforcement conduct during the investigation of crime[46] by prohibiting "unreasonable searches and seizures"[47] and providing that "no Warrants shall issue, but upon probable cause."[48] This seemingly straightforward language leaves many questions unanswered, including the definition of a "search"[49] and the relationship between the Reasonableness Clause and the Warrant Clause.[50] Case law has sought to clarify these important issues, but in this Part we show that the ubiquitous Police Efficiency Assumption has led to a distortion of key doctrines in this area.

A. The Warrant Requirement and the Manipulation of Definitions of a Search

From the text of the Fourth Amendment, it is unclear whether LEOs are required to obtain a valid warrant in order to conduct a search.[51] Read literally, the clause specifies only a limit on when warrants can issue—with probable cause—and presents a separate prohibition on unreasonable searches.[52] Many commentators have argued that the two clauses of the amendment are unconnected, and that warrantless searches are constitutionally valid as long as they are "reasonable"; the Warrant Clause of the Fourth Amendment is relevant under this view only when LEOs wish to obtain a warrant prior to a search.[53] Nonetheless, the Supreme Court has long

46. *See* Wolf v. Colorado, 338 U.S. 25, 28 (1949).

47. For simplicity of language, we refer to searches and seizures collectively as "searches" in this Article because the distinction is irrelevant to our analysis.

48. U.S. CONST. amend. IV.

49. *See, e.g.*, Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 122 (2002).

50. *See, e.g.*, Jeffrey Bellin, *Crime-Severity Distinctions and the Fourth Amendment: Reassessing Reasonableness in a Changing World*, 97 IOWA L. REV. 1, 8 (2011); Joseph D. Grano, *Rethinking the Fourth Amendment Warrant Requirement*, 19 AM. CRIM. L. REV. 603, 603 (1982).

51. *See, e.g.*, Bellin, *supra* note 50; Grano, *supra* note 50.

52. U.S. CONST. amend. IV.

53. *See, e.g.*, Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV.

considered warrantless searches to be presumptively unreasonable,[54] and has also ordained that ordinarily, reasonableness is only satisfied through obtaining a warrant.[55] Thus, LEOs are routinely required to obtain warrants prior to undertaking any search, unless the search falls into one of the well-delineated exceptions to the warrant requirement.[56]

A requirement that LEOs obtain a warrant for all searches raises the question of what constitutes a search under the Fourth Amendment. Many actions that LEOs undertake during the course of investigating a crime, such as interviewing victims or reading the criminal records of suspects, are clearly not searches. However, as we explain below, there are many types of law-enforcement activity that courts do not consider to be searches in the constitutional sense of triggering the protections of the Fourth Amendment, but laypeople would widely consider to be a type of search.[57] For instance,

---

757, 761 (1994) ("The words of the Fourth Amendment really do mean what they say. They do not require warrants, even presumptively, for searches and seizures.").

54. *See, e.g.*, Katz v. United States, 389 U.S. 347, 357 (1967) (" 'Over and again this Court has emphasized' ... that searches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment." (quoting United States v. Jeffers, 342 U.S. 48, 51 (1951))). The Court is arguably moving away from the warrant requirement in recent decisions. *See, e.g.*, Peter Swire, *A Reasonableness Approach to Searches After the* Jones *GPS Tracking Case*, 64 STAN. L. REV. ONLINE 57, 59-60 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-57.pdf [http://perma.cc/L954-B8LK]; *see also* Tom Goldstein, *Why* Jones *Is Still Less of a Pro-Privacy Decision Than Most Thought* (*Conclusion Slightly Revised Jan. 31*), SCOTUSBLOG (Jan. 30, 2012, 10:53 AM), http://www.scotusblog.com/2012/01/why-jones-is-still-less-of-a-pro-privacy-decision-than-most-thought/ [http://perma.cc/4HZT-DDUW].

55. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) ("[R]easonableness generally requires the obtaining of a judicial warrant." (citing Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 619 (1989))).

56. *See, e.g.*, California v. Acevedo, 500 U.S. 565, 573 (1991) (search of containers within automobiles); Maryland v. Buie, 494 U.S. 325, 327 (1990) (protective sweep); Skinner v. Ry. Labor Execs.' Ass'n, 489 U.S. 602, 620 (1989) (special needs doctrine); United States v. Watson, 423 U.S. 411, 416 (1976) (felony arrest exception); Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973) (consent); Coolidge v. New Hampshire, 403 U.S. 443, 465 (1971) (discussing the plain view doctrine); Chambers v. Maroney, 399 U.S. 42, 48 (1970) (general automobile exception); Chimel v. California, 395 U.S. 752, 756 (1969) (search incident to lawful arrest); Terry v. Ohio, 392 U.S. 1, 20 (1968) (*Terry* stops); Camara v. Mun. Court of S.F., 387 U.S. 523 (1967) (administrative searches); Schmerber v. California, 384 U.S. 757, 770-71 (1966) (exigent circumstances).

57. *See* Susan F. Mandiberg, *Reasonable Officers vs. Reasonable Lay Persons in the Supreme Court's* Miranda *and Fourth Amendment Cases*, 14 LEWIS & CLARK L. REV. 1481, 1516-18 (2010).

listening to a conversation via a wire worn by a confidential informant may be solid police work, but laypeople could easily consider this to be a search[58]—contrary to Supreme Court doctrine.[59] Similarly, having a professionally trained police narcotics detection dog sniff an airline passenger's luggage[60] or a person's car trunk[61] in order to detect contraband hidden within may be reasonable, but is nonetheless arguably a search,[62] just as it would be if that dog was sniffing near the entrance of a house.[63] Yet the Court has deemed that LEO-guided canine examinations are not searches in the first two situations,[64] whereas dog sniffs near the home are considered to be searches.[65]

These distinctions are illustrations of a general doctrinal problem: many activities that would ordinarily be considered searches are not deemed searches by courts for Fourth Amendment purposes.[66] Courts fail to classify investigations as searches in order to avoid the consequent assumption of unreasonableness of the activity in the absence of probable cause and a warrant, as well as the potential application of the exclusionary rule.[67] Courts typically assume the warrant requirement impedes police efficiency,[68] and often fudge whether an investigation constitutes a search in order to avoid requiring a warrant.[69]

---

58. *See* United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

59. United States v. White, 401 U.S. 745, 752-53 (1971).

60. United States v. Place, 462 U.S. 696, 707 (1983).

61. Illinois v. Caballes, 543 U.S. 405, 408 (2005).

62. *See* Jacobi, *supra* note 39, at 662 (criticizing the Court's analysis in *United States v. Place*, 462 U.S. 696).

63. Florida v. Jardines, 133 S. Ct. 1409, 1414, 1417-18 (2013) (involving an intrusion upon the homeowner's property).

64. *See Caballes*, 543 U.S. at 409; *Place*, 462 U.S. at 707.

65. *Jardines*, 133 S. Ct. at 1417.

66. *See, e.g.*, *Caballes*, 543 U.S. at 409; *Place*, 462 U.S. at 707.

67. *See* Jacobi, *supra* note 39, at 586.

68. Police efficiency in this context refers to the general notion of economic efficiency: the ability of law enforcement to use its scarce resources (time, money, and skill) to produce a service (the capture and eventual conviction of criminals).

69. As Judge Guido Calabresi put it:

> Judges—politicians' claims to the contrary notwithstanding—are not in the business of letting people out on technicalities. If anything, judges are in the business of keeping people who are guilty in on technicalities.... [T]he judge facing a clearly guilty murderer or rapist [claiming a Fourth Amendment

In order to delineate between legal searches and common-sense searches, we use the term "investigations" to refer to any type of action LEOs take in order to obtain evidence. Investigations includes those deemed "searches" under the Fourth Amendment, as well as "nonsearches"—any law-enforcement activity that courts do not consider to be a search under the Fourth Amendment, even if laypeople may be consider it to be a type of search. Searches require a warrant in the absence of an exception to the warrant requirement, whereas LEOs are not required to obtain a warrant for a nonsearch.

The Supreme Court's primary test for distinguishing between searches and nonsearches appears in *Katz v. United States*.[70] The most influential expression of the test comes from Justice Harlan's concurrence:[71] a law-enforcement investigation is a search if it violates an individual's "reasonable expectation of privacy,"[72] meaning first that the individual has "exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[73] In *Katz*, the Court found that the defendant had a reasonable expectation of privacy in his telephone conversation that took place within a closed public phone booth, even though such a location would not ordinarily be considered a private place.[74] Recently in *United States v. Jones*, the Supreme Court added to the *Katz* framework by specifying that any physical trespass of a constitutionally protected area may constitute a search.[75]

---

violation] will do her best to protect the fundamental right and still keep the defendant in jail.

Guido Calabresi, *The Exclusionary Rule,* 26 HARV. J.L. & PUB. POL'Y 111, 112 (2003).

70. 389 U.S. 347, 360-61 (1967).

71. For a discussion about Justice Harlan's concurrence, see, for example, Minnesota v. Carter, 525 U.S. 83, 97 (1998) (Scalia, J., concurring); Cecil J. Hunt, II, *Calling in the Dogs: Suspicionless Sniff Searches and Reasonable Expectations of Privacy*, 56 CASE W. RES. L. REV. 285, 313 (2005); and David A. Sullivan, *A Bright Line in the Sky? Toward a New Fourth Amendment Search Standard for Advanced Surveillance Technology*, 44 ARIZ. L. REV. 967, 975 (2002).

72. *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

73. *Id.* at 361.

74. *Id.* at 351-52 (majority opinion) ("[T]he Fourth Amendment protects people, not places.").

75. 132 S. Ct. 945, 949, 950 & n.3 (2012). Justie Scalia, writing for the Court, claimed to be applying well-settled law that a trespass is sufficient to constitute a search. *Id.* at 950. But numerous previous decisions explicitly rejected the trespass doctrine. *See, e.g.*, Kyllo v. United

Both *Katz* and *Jones* expanded the definition of search. *Katz* expanded a search beyond the physical penetration of constitutionally protected areas,[76] and *Jones* redefined a physical penetration as sufficient,[77] albeit not necessary after *Katz*, to constitute a search. Nevertheless, most doctrine pertaining to searches has used the definition of a search to *exclude* a wide variety of law-enforcement investigations from the category of constitutionally recognized searches. Though there are many types of nonsearches, three doctrines are especially useful to illustrate the efforts courts go to in order to avoid categorization of investigative practices as searches, and thus to avoid the application of the warrant requirement and its assumed interference with police efficiency.

First, the Fourth Amendment does not protect information knowingly relinquished to someone else.[78] This rule also encompasses parties not participating directly in a conversation, such as a telephone company that keeps records of numbers dialed.[79] The rationale for this doctrine is that it is unreasonable for someone to have an expectation of privacy in information given to another because the other person is free to divulge the information to anyone.[80] Courts have applied the doctrine to many circumstances. For example, it is not a search when an undercover agent or confidential informant speaks with a subject,[81] even if the informant is wearing a wire that allows LEOs to simultaneously hear the conversation.[82] Following this logic, the third-party doctrine precludes any expectation of privacy in the telephone numbers an individual dials, even from a home phone, despite the protections of the home.[83] By simply

States, 533 U.S. 27, 32 (2001); Rakas v. Illinois, 439 U.S. 128, 143 (1978). Moreover, the Court has not yet clarified how this can be reconciled with the rule that trespasses onto property that constitute "open fields" under Fourth Amendment law are not considered searches at all. *See infra* notes 97-99 and accompanying text. Nevertheless, *Jones* does not change the analysis in this Article in any meaningful way and does not disturb existing case law regarding the search/nonsearch distinction.

76. *Katz*, 389 U.S. at 351-52.

77. *Jones*, 132 S. Ct. at 949, 950 & n.3.

78. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743-44 (1979); Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 584 (2011).

79. *Smith*, 442 U.S. at 744.

80. *See* United States v. White, 401 U.S. 745, 749 (1971).

81. Hoffa v. United States, 385 U.S. 293, 295, 302 (1966).

82. *White*, 401 U.S. at 751.

83. *See Smith*, 442 U.S. at 743-44.

dialing a phone number, an individual has "voluntarily conveyed numerical information to the telephone company and exposed that information to its equipment in the ordinary course of business. In so doing, [the individual] assumed the risk that the company would reveal to the police the numbers he dialed."[84]

The implications of this doctrine are vast: any provision of information, however detailed and personal, when given to third parties, no matter how hidden the presence of those third parties, is exposed to state investigation without the protection of the Fourth Amendment. This includes a person's banking information: because his bank has access to the records, the state is free to access those records without such access being considered a search.[85] The third-party doctrine is controversial,[86] and Justice Sotomayor recently proposed its reconsideration due to the breadth of its impact on daily personal activities;[87] however, the Justices recognized such considerations at the time of the doctrine's development,[88] and considered the goal of efficient policing strong enough to overcome that concern.[89]

A second category of nonsearch covers situations in which LEOs, while observing actions occurring in plain sight in a public forum, "augment[ ] the sensory faculties bestowed upon them by birth with such enhancement as science and technology afford[ ] them."[90] This allows the police to fly airplanes[91] or helicopters[92] over the property of those suspected of growing marijuana without such conduct being categorized as a search, even if they are using high-powered cam-

84. *Id.* at 744 (internal quotation marks omitted).

85. *See* United States v. Miller, 425 U.S. 435, 443 (1976).

86. *See, e.g.*, Gerald G. Ashdown, *The Fourth Amendment and the "Legitimate Expectation of Privacy,"* 34 VAND. L. REV. 1289, 1315 (1981); Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1254-56 (1983); Tokson, *supra* note 78, at 585.

87. *See* United States v. Jones, 132 S. Ct. 945, 955-57 (2012) (Sotomayor, J., concurring) (arguing that GPS data reveals intensely private information, such as trips to the psychiatrist, the abortion clinic, or the AIDS treatment center, and that being watched chills associational and expressive freedoms).

88. *See* United States v. White, 401 U.S. 745, 761-64 (1971) (Douglas, J., dissenting).

89. We return to consideration of the third-party doctrine in Part IV.B when discussing electronic mechanisms that attempt to ensure digital privacy.

90. United States v. Knotts, 460 U.S. 276, 282 (1983).

91. California v. Ciraolo, 476 U.S. 207, 215 (1986).

92. Florida v. Riley, 488 U.S. 445, 451-52 (1989).

eras.[93] The only significant limit on the capacity of law enforcement to use enhanced technology applies when the technology enables LEOs to gain information about events occurring *inside* the home. This limitation still permits LEOs to place radio transmitters in goods given to a suspect as long as the transmitter allows law enforcement only to track the suspect's public movements[94] and not the suspect's movements within her home.[95] Conversely, the use of thermal-imaging devices to detect patterns of heat emanating from a home is a search that requires a warrant because it provides law enforcement with information about activity *inside* that they would not be able to sense without the device.[96] Though there may be good reason to distinguish between the level of protection that a home versus a public space should receive, it seems counterintuitive to consider the use of the same technology to look for the same information in the same way a search in one case and a nonsearch in the other, simply due to the change in location. The reason for such a doctrinal contrivance may be that courts assume the police efficiency of avoiding the warrant requirement—achieved by labeling such investigations outside the home nonsearches—is high enough to overcome the privacy lost through allowing law enforcement investigative freedom in public places, but not high enough to overcome the privacy costs of similarly liberalizing investigations of the home.

Additional judicial artifices have nonetheless mitigated the protection of the home as the Court has adopted a restrictive definition of what parts of private property constitute the home. This brings us to the third category of nonsearches: an investigation that takes place in an "open field" surrounding the home is not a search.[97] To be classified as an open field, and thus for law-enforcement investigations to be categorized as nonsearches, the property in question need not be open or a field. An open field can include any unoccupied or undeveloped area outside of the "curtilage" of a

93. Dow Chemical Co. v. United States, 476 U.S. 227, 239 (1986).

94. *Knotts*, 460 U.S. at 282.

95. United States v. Karo, 468 U.S. 705, 719 (1984).

96. Kyllo v. United States, 533 U.S. 27, 40 (2001). The Court required a warrant for the additional reason that the device was not in such public use as to make a reasonable person expect that a private citizen would point one at a home. *Id.*

97. *See* Oliver v. United States, 466 U.S. 170, 178 (1984).

home,[98] which is the land that immediately surrounds the house and is associated with it.[99] The Court's definition of unoccupied land is at times quite broad. For instance, in *Oliver v. United States*, police entered a private property on which there was a parked camper, a barn, and a locked gate.[100] The Court held that there was no reasonable expectation of privacy even though the homeowner had posted "no trespassing" signs.[101] In *United States v. Dunn*, even two sets of fencing, which isolated two barns from the outside world, did not preclude federal officers' warrantless entry into the barns from constituting a nonsearch.[102] So, LEOs may search private property containing a home and other associated structures—and those structures themselves—under the rubric of nonsearches, thus avoiding the jurisdiction of the Fourth Amendment altogether.

These three categories of nonsearches are by no means exhaustive, but they are enough to illustrate the restrictive approach of the Supreme Court's Fourth Amendment search jurisprudence. Law-enforcement investigations that would be considered searches under any straightforward interpretation of the text of the Fourth Amendment are routinely categorized as nonsearches. The problems with this outcome are twofold: It promotes a jurisprudence that lacks plausibility and coherence, and it leaves many innocent citizens without recourse against unreasonable law-enforcement intrusions on their property and persons—for if an investigation is deemed to be a nonsearch, the court never needs to determine whether the law-enforcement action was unreasonable. The next Section shows that the reason for such harmful doctrinal manipulation is the courts' assumption that warrants impede law-enforcement investigations.

B. The Distorting Effect of the Assumption that Warrants Impede Investigations

In the Fourth Amendment context, courts often recognize the facilitation of law-enforcement investigations as a central value in the debate over what the law should be and, to the extent that

98. *Id.* at 180 n.11.
99. *See* United States v. Dunn, 480 U.S. 294, 300-01 (1987).
100. *Oliver*, 466 U.S. at 173.
101. *Id.* at 179.
102. *Dunn*, 480 U.S. at 297, 301-03.

courts decide Fourth Amendment questions through a balancing analysis, what the law is. Investigating crime in an effective manner is essential to disincentivizing crime and maintaining law and order, and so protecting the right to be free from violence. For this reason, although the Fourth Amendment makes explicit the value of protecting privacy rights against police intrusions, courts regularly enunciate the additional, and arguably countervailing, value of respecting and enabling the ability of law enforcement to investigate and prosecute crime. For most Fourth Amendment questions, the analysis ultimately boils down to a balancing of whether prohibiting a particular investigative technique without a warrant does more to protect the privacy interests of citizens or to harm the ability of LEOs to effectively investigate crime. This type of balancing inquiry appears in the Supreme Court's analysis of the warrant requirement,[103] the search/nonsearch distinction,[104] and various exceptions to the warrant requirement.[105]

When deciding these types of Fourth Amendment questions, courts and commentators often assume that requiring LEOs to obtain warrants will impede the investigation and ultimate prosecution of crimes. Requiring LEOs to obtain a warrant for a particular investigation will make it more difficult to find evidence because warrants cost LEOs both time and effort[106] and because LEOs must

---

103. *See, e.g.*, Robbins v. California, 453 U.S. 420, 438-39 (1981) (Rehnquist, J., dissenting) (arguing that the warrant requirement should be reconsidered given its negative impact on law enforcement); Bernard E. Harcourt & Tracey L. Meares, *Randomization and the Fourth Amendment*, 78 U. CHI. L. REV. 809, 815 (2011); Swire, *supra* note 54, at 59-62. The Court has, however, at times denied using such a balancing inquiry regarding the warrant requirement. *E.g.*, Coolidge v. New Hampshire, 403 U.S. 433, 481 (1971) ("The warrant requirement ... is not an inconvenience to be somehow 'weighed' against the claims of police efficiency.").

104. For instance, in cases in which LEOs augment their senses with technology without a warrant, the Court has considered the enhancement of law-enforcement detection such technology offers, weighed against the added intrusion into privacy. *See, e.g.*, California v. Ciraolo, 476 U.S. 207, 215 (1986); United States v. Knotts, 460 U.S. 276, 282 (1983).

105. *See, e.g.*, Steagald v. United States, 451 U.S. 204, 220-22 (1981); Mincey v. Arizona, 437 U.S. 385, 393 (1978).

106. Technology is making it easier for LEOs to attain a warrant quickly. *See* Cecilia Chan, *Search-Warrant Process for DUIs Faster for Phoenix Police*, AZCENTRAL (Apr. 11, 2013, 8:37 PM), http://www.archive.azcentral.com/community/phoenix/articles/20130410phoenix-police-search-warrant-process-duis-faster-brk.html [http://perma.cc/K2B-7CBY] (reporting that police in Phoenix can use the eSearch Warrant Application to send a warrant from the patrol car directly to a judge, who can approve or reject it from a laptop). There is, however, always some nonzero cost for procuring a warrant, as the Court has recently noted: "Even with modern technological advances, the warrant procedure imposes burdens on the officers who

establish probable cause ex ante.[107] Laying out the basis of officers' suspicion before a neutral magistrate can delay an investigation, and the magistrate's potential failure to find probable cause can prevent the search from taking place altogether. Allowing LEOs to proceed without a warrant, in contrast, could lead both to the discovery of evidence that would have been destroyed during the wait for a warrant and the seizure of evidence that would never have been found if there was no probable cause for a legal search.[108]

The assumption that the warrant requirement impedes police efficiency is mentioned frequently both by commentators critiquing the general warrant requirement and those advocating possible exceptions to the requirement: they argue that warrants impede police investigations and that this cost outweighs privacy concerns.[109] In juxtaposition, advocates of expansive Fourth Amendment rights argue that the concern about impeding law enforcement investigations is overstated, either because probable cause is a low bar for the procurement of a warrant,[110] or because the time and effort costs of obtaining a warrant have not been shown to be prohibitively high.[111] Even those commentators skeptical of the police efficiency justification, however, assume that the warrant requirement impedes a law-enforcement investigation to some extent; they simply dispute by how much.[112] Both sides of the debate assume a trade-off between police efficiency and rights. They merely disagree about the

---

wish to search [and] the magistrate who must review the warrant application." Fernandez v. California, 134 S. Ct. 1126, 1137 (2014); *see also infra* Part III.D.

107. *See, e.g.*, James J. Tomkovicz, California v. Acevedo*: The Walls Close in on the Warrant Requirement*, 29 AM. CRIM. L. REV. 1103, 1153-54 (1992).

108. *See, e.g.*, *id.* at 1154.

109. *See, e.g.*, John Kaplan, *The Limits of the Exclusionary Rule*, 26 STAN. L. REV. 1027, 1027 (1974) (discussing this argument); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1228 n.142 (2004) (arguing that search warrants should not be required to obtain "noncontent" information provided to an internet service provider).

110. *See* Tokson, *supra* note 78, at 641 ("[T]here is evidence to suggest that this concern is overstated.... [P]olice may often be able to gather sufficient evidence for probable cause before obtaining [the evidence sought in a warrant].").

111. *See* Tomkovicz, *supra* note 107, at 1157.

112. *See* Tokson, *supra* note 78, at 640-41 ("[R]equiring a warrant to obtain [evidence] would unduly burden the police ... [because] [i]t could prevent them from gathering the initial evidence required to show probable cause, and thus preclude effective investigations altogether."); Tomkovicz, *supra* note 107, at 1157 ("[T]he deliberate warranted search process undoubtedly results in some lost prosecutions.").

normative value of each opposing possible outcome: warrantless searches and nonsearches versus imposing the warrant requirement and delaying or even preventing some searches.

The Court has been inconsistent in its willingness to explicitly acknowledge that it has balanced an interest in facilitating law-enforcement investigation against the privacy concerns underlying the warrant requirement. The Court has most often held that the general interest in police efficiency alone cannot justify holding that LEOs are *not* required to obtain a warrant,[113] and has at times used the interest as part of a balancing test.[114] At other times the Court has explicitly stated that "the mere fact that law enforcement may be made more efficient can never itself justify disregard of the Fourth Amendment."[115] The latter statement, however, has largely become a catchphrase of dissenting justices in opposing majorities' implicit acceptance of the trade-off between rights and police efficiency.[116] Even this opposing position implies only that the value of police efficiency is not enough *by itself* to overcome a constitutionally recognized right to privacy, not that police efficiency is irrelevant. Regardless of whether police efficiency is important enough to overcome privacy concerns, the Justices have commonly assumed that law-enforcement investigations are in fact impeded to some extent when warrants are required: "The investigation of crime would always be simplified if warrants were unnecessary."[117]

One area in which the Court has displayed its acceptance of the value of the Police Efficiency Assumption and its impairment by the warrant requirement is in crafting exceptions to the warrant require-

---

113. *See* Georgia v. Randolph, 547 U.S. 103, 115 n.5 (2006); Steagald v. United States, 451 U.S. 204, 222 (1981); Mincey v. Arizona, 437 U.S. 385, 393 (1978).

114. *See Steagald*, 451 U.S. at 222 (balancing the impediment to law-enforcement investigations against the intrusion into privacy of unwarranted searches).

115. *Mincey*, 437 U.S. at 393.

116. *See, e.g.*, New York v. Belton, 453 U.S. 454, 469 (1981) (Brennan, J., dissenting) (criticizing the majority for justifying comprehensive searches of the person of an arrestee without a warrant in order to guide the officer in the field).

117. *E.g.*, *Mincey*, 437 U.S. at 393; *see also Steagald*, 451 U.S. at 222 ("Any warrant requirement impedes to some extent the vigor with which the Government can seek to enforce its laws."). Some Justices have argued that this impediment is small. *See* Arkansas v. Sanders, 442 U.S. 753, 767 (1979) (Burger, C.J., concurring) ("[The] warrant requirement is not so onerous."); Harris v. United States, 331 U.S. 145, 171 (1947) (Frankfurter, J., dissenting) (arguing that the degree to which Fourth Amendment impedes effective law enforcement is grossly exaggerated).

ment. For instance, the Court in *New York v. Belton* determined that the passenger compartment of a car is included in the "the one lunge area"[118]—the area within the immediate control of the arrestee in a search incident to arrest.[119] The Court concluded that searching the passenger compartment was an automatic entitlement, regardless of where the arrestee was when the search took place, or whether he was truly able to reach the passenger compartment.[120] The Court was willing to make a broad generalization that articles inside the passenger compartment "are in fact generally, even if not inevitably, within 'the area into which an arrestee might reach in order to grab a weapon or evidentiary item.'"[121] The Court justified this factual presumption largely on the basis that "a policeman [cannot otherwise] know the scope of his authority."[122] The Court was concerned about the practical difficulties that would arise for LEOs without such a bright line, and looked for a rule that would provide them certainty, and thus efficiency, in investigating crime and making arrests.[123] The Court created this warrant exception expansion out of the concern for effective law-enforcement practice but subsequently rejected that position in *Arizona v. Gant*.[124] However, in *Gant*, the Court reversed itself on the basis that the factual claim in *Belton* was no longer true, not because the Court rejected the Police Efficiency Assumption. The Court concluded that the *Belton* decision itself had undermined its own factual claim in that the incentives created by the rule had changed law-enforcement practices.[125]

The assumption that the warrant requirement impedes law-enforcement investigations also plays a role in cases defining the distinction between a search and a nonsearch, as described above. The Court has often presented this trade-off in terms of the value to LEOs of using bright-line rules.[126] For instance, in defining what

118. *Belton*, 453 U.S. at 460.

119. *Id.*; Leslie A. Lunney, *The (Inevitably Arbitrary) Placement of Bright Lines*: Belton *and Its Progeny*, 79 TUL. L. REV. 365, 396 (2004).

120. *Belton*, 453 U.S. at 460.

121. *Id.* (citing Chimel v. California, 395 U.S. 752, 763 (1969)).

122. *Id.*

123. *Id.* at 459-60.

124. 556 U.S. 332, 341-44 (2009).

125. *Id.* at 342-43. This interactive dynamic is returned to in Part III.C.

126. For an example of bright-line rules in search/nonsearch cases, see Kyllo v. United

constituted an open field, a majority of the Court explicitly rejected a case-by-case test proposed by the dissent,[127] in part because the lack of an ex ante rule would be unworkable for LEOs.[128] Consequently, even the existence of "no trespassing" signs and the inability to see the field from the air did not prevent land from being an open field—a rule that prevented even unreasonable law-enforcement investigations from triggering Fourth Amendment protection.[129]

For the same reason, the Court has considered police efficiency when deciding whether the automobile warrant exception extends to the investigation of containers within a car. Initially, the Court distinguished between containers in a car (for which a warrant was required) versus other objects in a car (which could be searched without a warrant);[130] in *California v. Acevedo*, however, the Court recognized that this rule "provided only minimal protection for privacy and ... impeded effective law enforcement."[131] The Court attempted to manage what it had assumed to be an implicit trade-off between police efficiency and privacy protection, although it was realizing that in practice it did not work that way.[132] The Court was concerned that the rule "confused courts and police officers and impeded effective law enforcement."[133] It also "noted the virtue of providing clear and unequivocal guidelines to the law enforcement profession."[134] Ultimately, the Court "conclude[d] that it was better to adopt one clear-cut rule to govern automobile searches" and to

States, 533 U.S. 27, 40 (2001).

127. Oliver v. United States, 466 U.S. 170, 189 (1984) (Marshall, J., dissenting) ("[W]e have traditionally looked to a variety of factors in determining whether an expectation of privacy asserted in a physical space is 'reasonable.'").

128. *Id.* at 181 (majority opinion) ("Nor would a case-by-case approach provide a workable accommodation between the needs of law enforcement and the interests protected by the Fourth Amendment.").

129. The Court has similarly applied this analysis to other state actors, including prison officials. For example, the Court has deemed the search of prison cells and seizure of noncontraband not to require a warrant due to the constant surveillance needed for the "institutional security and internal order" of prisons. Hudson v. Palmer, 468 U.S. 517, 527-28 (1984).

130. United States v. Chadwick, 433 U.S. 1, 13 (1977)

131. California v. Acevedo, 500 U.S. 565, 574 (1991).

132. This interactive dynamic is returned to in Part IV.A.

133. *Acevedo*, 500 U.S. at 576.

134. *Id.* at 579 (quoting Minnick v. Mississippi, 498 U.S. 146, 151 (1990)) (internal quotation marks omitted).

expand the automobile warrant exception to include containers in a car.[135]

Finally, the Court has acknowledged the influence of police efficiency in its analyses of the probable cause test—the threshold that LEOs must satisfy in order to gain a warrant. *Illinois v. Gates* laid out the modern totality-of-the-circumstances test for establishing probable cause.[136] In *Gates*, the Court justified its willingness to relax the two prongs that had been rigidly applied to probable cause[137] out of recognition of the practical difficulties that LEOs face in the field: "[A]ffidavits [for search warrants] are normally drafted by nonlawyers in the midst and haste of a criminal investigation. Technical requirements of elaborate specificity once exacted under common law pleadings have no proper place in this area."[138] In this way, the Court made probable cause easier for LEOs to establish out of recognition of the need for police efficiency under trying circumstances.

These and other examples show that the judicial desire to promote police efficiency has driven much of the doctrinal development in Fourth Amendment law. The Police Efficiency Assumption makes a great deal of intuitive sense—undoubtedly, a warrant requirement will in many cases make it more difficult for LEOs to find admissible evidence, both because of the direct costs of obtaining a warrant, and because of the screening function of the probable cause requirement. However, this Article shows that, in many circumstances, requiring LEOs to obtain a warrant before they can undertake an investigation will not make it harder to obtain evidence. The key to this insight is that criminals can innovate in order to prevent LEOs from finding evidence in an investigation.[139] As we show below, allowing LEOs to investigate without warrants will often provide criminals with a greater incentive to innovate.[140] This innovation will decrease the likelihood that law enforcement will find evidence during an investigation,

135. *Id.*

136. 462 U.S. 213, 238 (1983).

137. The Court created this rigid two-prong test in Spinelli v. United States, 393 U.S. 410, 415-16 (1969).

138. *Gates*, 462 U.S. at 235 (quoting United States v. Ventresca, 380 U.S. 102, 108 (1965)) (internal quotation marks omitted).

139. *See infra* Part II.

140. *See infra* Part III.

and, under certain conditions, will offset the benefit that law enforcement gains from not having to obtain a warrant. In these cases, the Police Efficiency Assumption will be incorrect.

II. CRIMINAL INNOVATION

It has long been accepted that criminals respond to incentives.[141] Modern empirical research has shown that increased expected punishments deter crime.[142] Yet punishment can cause criminals to change their behavior in ways other than deciding whether to commit a crime, including by innovating. Criminal innovation occurs when a criminal changes his behavior in a strategy designed to decrease the likelihood that law enforcement obtains admissible evidence of a completed or planned crime. Although this phenomenon has been addressed in the economic literature,[143] it has been largely overlooked in legal scholarship, including its implications for the warrant requirement. Additionally, the economic analysis of criminal innovation has been static, and has not considered the dynamic nature of police-criminal interactions. In this Part, we survey the existing work regarding criminal innovation and discuss the impact that criminal innovation may have on the Police Efficiency Assumption.

A. Existing Scholarship on Criminal Innovation

Under the conventional economic model of crime—the Becker model—criminals are deterred from committing crime when the benefit of crime is outweighed by the expected punishment, defined as the probability of being convicted multiplied by the punishment that comes with conviction.[144] Both public policy and the law place a high value on protecting and enhancing the ability of LEOs to

141. JEREMY BENTHAM, PRINCIPLES OF PENAL LAW, *reprinted in* 1 THE WORKS OF JEREMY BENTHAM 365, 399 (Edinburgh, Simpkin, Marshall & Co., 1843) (1789) ("The profit of the crime is the force which urges a man to delinquency: the pain of the punishment is the force employed to restrain him from it.").

142. For a survey of this research, see Daniel S. Nagin, *Criminal Deterrence Research at the Outset of the Twenty-First Century*, 23 CRIME & JUST. 1, 8-12 (1998).

143. *See, e.g.*, Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169 (1968).

144. *Id.* at 185.

investigate crime and obtain prosecutions, and various reforms to sentencing practices were considered to maximize crime prevention and crime resolution.

In contrast, the implications of criminal innovation on models of criminal behavior were long overlooked, despite the fact that criminals can take many measures to avoid punishment.[145] Avoidance behaviors can occur before a crime has been committed, after the crime but before arrest, or after indictment.[146] Collectively, these behaviors are known in the literature as "detection avoidance."[147] Simple examples of anticipatory detection avoidance that occur during commission of a crime include wearing gloves or installing a radar detector in one's car; more complex mechanisms, such as e-mail encryption, are explored later.[148] Detection avoidance may also occur after indictment through providing false testimony in court or escaping from custody.[149] Because this Article concerns law-enforcement investigations and the warrant process, we focus on only those detection avoidance innovations that occur prior to arrest.[150]

By innovating, criminals can decrease the likelihood that evidence of a crime will be detected, yet the Becker model of crime does not take this into account.[151] More recently, scholars have begun to

---

145. *See* Chris William Sanchirico, *Detection Avoidance and Enforcement Theory: Survey and Assessment* 1 (U. of Pa. Inst. for Law & Econ. Research Paper Series, No. 10-29, 2010), *available at* http://perma.cc/B9EZ-JU6H ("The subject of evidentiary foul play—inclusive of fabricated testimony, document destruction, and myriad other modes of detection avoidance—is underrepresented in both legal and law and economic scholarship on procedure and evidence.").

146. *See* Nussim & Tabbach, *supra* note 14.

147. *See* Sanchirico, *supra* note 145.

148. See *infra* Part IV.B.

149. Most of the detection avoidance strategies that occur after indictment are themselves punishable as crimes. *See id.* For a discussion of the possibility of criminalizing criminal innovation behaviors, as well as problems with this idea, see *infra* notes 156-60 and accompanying text.

150. Police investigations, such as searches of a suspect's home, can of course occur after the suspect's arrest. But the behavior necessary to hide evidence generally takes place prior to the arrest.

151. Sanchirico, *supra* note 145, at 3. ("The probability that wrongs and offenses are detected is a central feature of the conventional model of enforcement. But the conventional model is starkly asymmetric regarding the determinants of this probability. It takes into account the government's efforts at detecting violations, but it ignores violators' efforts at avoiding detection."); *see also* Chris William Sanchirico, *Detection Avoidance*, 81 N.Y.U. L. REV. 1331, 1333 (2006) ("Our theories of evidence and procedure focus too much on wrongdoing as the subject of evidence, and not enough on evidence as the subject of wrongdoing.").

study the impact that criminal detection avoidance can have on the conventional model of crime.

The first model to incorporate criminal detection avoidance was published by Arun Malik in 1990.[152] Aside from introducing avoidance into models of criminal behavior, the model demonstrated that a crucial result of Becker's model of crime—that crime should be punished by fines that are set as high as possible[153]—does not hold if criminals are able to engage in avoidance because the prospect of a large fine provides an incentive to engage in avoidance.[154]

Nussim and Tabbach extended this model by showing that increasing the direct costs of crime, or the likelihood of punishment, may actually increase the amount of criminal activity if avoidance is possible.[155] A subsequent article by the same authors looked at the possibility of punishing avoidance behaviors as a way to deter them.[156] Their model showed that, whereas ex ante regulation of avoidance activities—such as taxes on radar detectors—decreases both crime and avoidance, ex post punishment of avoidance—such as increased fines for being caught speeding while using a radar detector—may be counterproductive, inducing more avoidance and more crime.[157] The difficulty with this conclusion, as a number of authors have argued, is that it may be impossible to effectively sanction avoidance because it is difficult to detect.[158] This is even more difficult for ex ante regulation, because many items used for avoidance, such as ski masks or prepaid cell phones, have legitimate as well as criminal uses.[159] Furthermore, sanctioning avoidance simply creates an incentive for criminals to avoid detection of this avoidance.[160]

This Article differs from earlier work on criminal avoidance in two respects. First, it analyzes the interaction of criminal avoidance

---

152. Arun S. Malik, *Avoidance, Screening and Optimum Enforcement*, 21 RAND J. ECON. 341, 342 (1990).

153. Becker, *supra* note 143, at 193.

154. Malik, *supra* note 152.

155. Jacob Nussim & Avraham D. Tabbach, *Deterrence and Avoidance*, 29 INT'L REV. L. & ECON. 314, 321 (2009).

156. Nussim & Tabbach, *supra* note 14, at 45.

157. *Id.* at 62.

158. For a brief survey of authors taking this position, see Sanchirico, *supra* note 145, at 18.

159. Nussim & Tabbach, *supra* note 14, at 48-49.

160. *See* Sanchirico, *supra* note 151, at 1331, 1338-40.

with the warrant requirement, a topic that has not been previously addressed. Second, it considers the effects that criminal avoidance may have on LEOs' decision whether to investigate. Because this inquiry is two-sided, our analysis employs game theory rather than a direct economic model of crime. Like the Becker model,[161] this game-theoretic approach uses law and economics to model human behavior, building on the assumption that people act rationally—that they make consistent decisions that maximize their utility.[162] But instead of examining only the utility of the criminal facing possible punishment, we consider the interwoven incentives of LEOs to investigate more or less vigorously. We analyze not only the "best response"[163] of the criminal to crime enforcement policies, but also the best response of law enforcement to criminal innovation in response to those policies, the best response of criminals to the responses of law enforcement, and so on. This allows us to predict outcomes in a dynamic interaction, representing the ongoing cat-and-mouse game between criminals and law enforcement.

B. Criminal Innovation and the Police Efficiency Assumption

Criminals' ability to innovate can defeat the Police Efficiency Assumption in certain situations. Criminals have more incentive to innovate when a warrant is not required than when a warrant is required, which in turn occurs because it is easier for LEOs to investigate without a warrant. Ultimately, LEOs may be no better off in terms of their ability to catch criminals when warrants are

161. *See generally* Becker, *supra* note 143.

162. *See, e.g.*, RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 3-6 (5th ed. 1998). This is sometimes contrasted with behavioral economics, which is based on experimental findings that people often make decisions that are economically irrational due to so-called "cognitive biases." *See, e.g.*, Joshua D. Wright & Douglas H. Ginsburg, *Behavioral Law and Economics: Its Origins, Fatal Flaws, and Implications for Liberty*, 106 NW. U. L. REV. 1033, 1034 (2012). Although behavioral economics analysis is very valuable, it is necessarily secondary: it is essential to first determine what a rational response to a problem is before analyzing likely deviations from that rational response. Because criminal innovation has never before been conceived as part of a game between the police and criminals, it is important to create a basic model of this interaction before introducing cognitive biases into our model to determine how these may change the results.

163. In game theory, a "best response" is the strategy or strategies that produces the most favorable outcome for a player, taking the other players' strategies as given. PETER C. ORDESHOOK, GAME THEORY AND POLITICAL THEORY 115 (1986).

required versus when they are not because the extent of criminal innovation can overwhelm the reduced costs of not needing a warrant.

The interaction between criminal incentives and LEO incentives is dynamic. Criminals will have an increased incentive to innovate when LEOs can incur lower effort costs in order to conduct an investigation because, absent the cost of this innovation, LEOs could otherwise investigate more often. This increased innovation will lead to the failure of the Assumption when the gains to LEOs from not having to obtain a warrant are offset by a reduction in the likelihood of finding evidence during an investigation due to criminal innovation. This is not like saying that better cars lead to worse driving; rather, the dynamic is interactive, and key to that interaction is the interdependence of the conduct of both criminals and LEOs in a context of uncertainty. If the criminal knows that LEOs will investigate regardless, the criminal's innovation will not differ based on the warrant requirement; the same is true if LEOs are certain not to investigate.[164] If LEOs decide to always investigate when they do not need a warrant, but never investigate when they do need a warrant, this may also lead the criminal to innovate. Although this situation does not violate the Assumption, innovation nevertheless reduces law-enforcement gains from not having to obtain a warrant.[165]

In developing various exceptions to the warrant rule, the Supreme Court Justices have painfully learned the importance of understanding the dynamic nature of police-criminal interactions. For instance, as discussed above,[166] the Court previously held that different levels of protection applied to evidence located in containers in cars versus evidence located in the car itself, even when the evidence was in a part of the car that itself forms a kind of container, such as the glove box or the trunk.[167] But this rule created perverse incentives: the only innovation required of criminals to skirt the automobile exception was to keep contraband in containers within the car, which was practically costless, and so the rule

164. *See infra* Part III.

165. *See infra* Part III.

166. *See supra* Part I.B.

167. Robbins v. California, 453 U.S. 420, 426 (1981); *see also* Arkansas v. Sanders, 442 U.S. 753, 763-65 (1979).

became unworkable.[168] Similarly, the automobile arrest exception initially automatically included the whole of the passenger compartment of the car within the assumed "one lunge" area of potential danger posed by the arrestee.[169] But it later became standard practice to handcuff the arrestee and place him in the back of the squad car, where he clearly posed no danger to the officer, thus undermining the justification for the exception.[170] The difficulty with reversing the "one lunge" assumption was that doing so could incentivize LEOs to put themselves in danger by leaving the arrestee unhandcuffed and near the car in order to gain the power to search the car.[171] Thus both criminal and police incentives can change dramatically based on doctrinal developments. Finally, because the Court has held that law-enforcement surveillance flights do not breach any reasonable expectation of privacy—because they provide information only about open fields and not the home[172]—criminals have been incentivized to innovate by hydroponically growing marijuana inside, so that overhead airplanes and helicopters cannot view the plants.[173] The changing jurisprudence in many of the exceptions previously described illustrates the dynamic nature of police-criminal interactions.

Often, that dynamic involves criminal innovations, which are not limited to the secreting of contraband. The ability of LEOs to obtain bank records without a warrant encourages criminals to keep their funds in less official financial institutions, and money laundering is

168. *See* United States v. Ross, 456 U.S. 798, 820 (1982) ("[T]he practical consequences of the *Carroll* decision would largely be nullified if the permissible scope of a warrantless search of an automobile did not include containers and packages found inside the vehicle.").

169. *See supra* notes 118-24 and accompanying text.

170. *See, e.g.*, Arizona v. Gant, 556 U.S. 332, 344 (2009).

171. *See id.* at 362 (Alito, J., dissenting) ("If the applicability of the ... rule turned on whether an arresting officer chooses to secure an arrestee prior to conducting a search, rather than searching first and securing the arrestee later, the rule would 'create a perverse incentive for an arresting officer to prolong the period during which the arrestee is kept in an area where he could pose a danger to the officer.'" (quoting United States v. Abdul-Saboor, 85 F.3d 664, 669 (D.C. Cir. 1996))).

172. *See supra* notes 91-94 and accompanying text.

173. *See* Glenn Smith, *Marijuana Bust Shines Light on Utilities*, POST & COURIER (Jan. 29, 2012, 12:01 AM), http://www.postandcourier.com/article/20120129/PC1602/301299979 [http://perma.cc/SFY4-6CNW]. Arguably, the result has been stronger strains of marijuana, but this is subject to ongoing debate. *See Potency of Marijuana*, UNIV. OF WASH. ALCOHOL & DRUG ABUSE INST., http://www.adai.uw.edu/marijuana/factsheets/potency.htm [http://perma.cc/S66F-Y86A] (last updated June 2013).

a reaction to authorities' ability to monitor a suspect's finances. In the digital realm, criminals fearing police surveillance can invest in stronger encryption techniques, such as the Tor program.[174] Each of these innovations potentially creates significant hurdles to the ability of law enforcement to catch these criminals. The question is, do those investigatory impediments offset the advantage to law enforcement from the eliminated costs of obtaining a warrant? And if so, when?

III. AN ECONOMIC MODEL OF CRIMINAL INNOVATION AND THE WARRANT REQUIREMENT

This Part provides an economic model that demonstrates when the Police Efficiency Assumption will fail, or when LEOs will not be better be off in terms of their ability to catch criminals, if they are not required to obtain a warrant for an investigation than they would be if a warrant were required. To make this assessment, we analyze law-enforcement decisions in two different scenarios: one, under the "Warrant" condition, when a court has determined that a particular investigation is a search; the other, under the "Nonwarrant" condition, when a court has determined that the investigation is a nonsearch. For example, if a court finds that an investigative practice that LEOs widely consider to be a search is in fact a nonsearch, or vice versa, we can compare the effect of the rule change on police efficacy: if LEOs do not gain from the change away from the warrant requirement, the Assumption fails. In economic language, the Assumption fails if officers' expected utility[175] under the Warrant condition is greater than or equal to that in the Nonwarrant condition.

Economic models enable us to formalize the incentives of both criminals and LEOs, and to examine the effect of different rules on their predicted behavior. Specifically, we use a game-theoretic model because we need to examine the decisions of both LEOs and the criminal as they influence each other.[176] The likelihood that

174. *See infra* Part IV.B.

175. Expected utility is calculated by multiplying an actor's utility from each possible outcome by the probability that it will occur, and then summing across all possible outcomes. JAMES D. MORROW, GAME THEORY FOR POLITICAL SCIENTISTS 16 (1994).

176. *See* MARTIN J. OSBORNE, AN INTRODUCTION TO GAME THEORY 7 (2004) (explaining that

LEOs will conduct an investigation depends upon the amount of innovation by criminals, because the latter impacts the chances that an investigation will find evidence. Likewise, the incentives for criminals to innovate will increase when LEOs are more likely to conduct an investigation. The utility of each actor depends on both its own decisions and those of the other actor.

Most analyses of criminal innovation have not taken this approach and have simply looked at the criminal's decision whether to innovate.[177] These papers have treated a criminal's likelihood of being caught as a function of the amount of criminal innovation and the amount of resources society devotes to detecting crime. However, this view overlooks the fact that the decision by LEOs to investigate a particular crime is not fixed, but rather depends on the likelihood that an investigation will be successful—in other words, that it will reveal admissible evidence. Increased criminal innovation leads not only to a smaller chance of LEOs finding evidence if they conduct an investigation, but also to a smaller likelihood that LEOs will investigate at all, given the fact that they know criminals may innovate.[178] Thus, it is crucial to look at both of these effects when analyzing a criminal's decision whether to innovate.[179]

---

game theory is applicable when the variables that impact one decision maker include other decision makers).

177. *See supra* Part II.A.

178. This is true if the police are aware of possible innovation and have full information regarding the incentives that may lead criminals to innovate. As discussed below, we assume that the police do have knowledge of these incentives, just as criminals have knowledge of the incentives faced by the police. *See infra* Part III.B.

179. The police will be able to innovate as well by developing better investigatory techniques, such as having informants wear wires. Just like criminals, the police will innovate when the benefits of innovation—the increased likelihood of finding admissible evidence—outweigh the cost. We exclude police innovation from the analysis for two reasons. First, the police will likely be able to spread the costs of an innovation over many different investigations, making the cost of police innovation more of a long-term assessment than a decision dictated by the context of a single investigation. For the most part, the amount of police innovation can be considered as an exogenous variable when police decide whether to innovate. Second, the warrant requirement does not affect the police decision to innovate because the need for, and effectiveness of, police innovation depends on criminal innovation rather than the warrant requirement. An exception would arise if the police had an innovation that was especially effective in response to a specific criminal's particular innovation; in that case, police innovation may be more likely when criminals innovate. Likewise, the criminal's innovation decision is not usually affected by police innovation; only the incentive to commit the crime itself is changed.

This Part begins by discussing the variables that influence the decision by law enforcement whether to search and the decision by the criminal whether to innovate. It then lays out the games and solves them to determine the likelihood that LEOs will search and that the criminal will innovate. We are then able to specify the conditions under which the Police Efficiency Assumption fails.

A. Criminal Utility

Criminals act to maximize the utility gained from their crime. The model used here to analyze criminal decision making is adapted from the Becker model of crime.[180] That model analyzes a person's decision regarding the amount of crime to commit, comparing the benefits from crime to the expected cost of committing crime—the probability of detection multiplied by the punishment that comes with detection.[181] Our model is similar to Becker's model, but includes some important changes.

First, we assume that the criminal has committed or is going to commit a single isolated crime. This means that the criminal's only decision is whether to innovate to cover up the crime. This assumption is in accord with what could be termed a "career criminal" or a "sophisticated criminal," who will definitely engage in a certain crime. The analysis thus applies only to crimes that will not be deterred by a transition from the Warrant condition to the Nonwarrant condition. Otherwise, the innovation and response effect we are trying to assess could be obscured by the possible benefits to society that may result in a move to the Nonwarrant condition through a reduction in the overall level of crime.[182] By examining a single crime that the criminal is determined to commit, we can set aside the possibility of crime reduction, which has been studied elsewhere.[183]

---

180. *See generally* Becker, *supra* note 143 (providing intuitive proofs of the Becker model of crime).

181. *See id.* at 181.

182. There is evidence that strictly enforcing the warrant requirement may lead to an increase in crime. *See* Raymond A. Atkins & Paul H. Rubin, *Effects of Criminal Procedure on Crime Rates: Mapping Out the Consequences of the Exclusionary Rule* 16 (Indep. Inst., Working Paper No. 9, 1999), *available at* http://perma.cc/3PVU-LNFT.

183. *See* William J. Stuntz, *Local Policing After The Terror*, 111 YALE L.J. 2137, 2144-45 (2002) ("The police help to restrain crime. Rules that restrain the police thus tend to remove

Second, we assume that the criminal can engage in innovation that reduces the likelihood that LEOs will find evidence of crime in the event of an investigation.[184] This is the insight of the literature regarding criminal innovation. However, unlike that literature, which considers the amount of innovation to be a continuous variable that can be chosen by a criminal,[185] this model will treat innovation as discrete rather than continuous—the criminal either decides to innovate or not to innovate. The benefit of this assumption is that it more closely reflects the reality of the situation in which a criminal must decide whether to make an innovation in order to avoid detection for a particular crime. A bank robber cannot buy half of a mask and would not buy two masks for himself; a murderer does not need two silencers for his single gun, but also cannot purchase a silencer unless he pays the full price for it. A criminal in this situation is undoubtedly already using some nonzero amount of innovation; this preexisting innovation is encapsulated in the probability that LEOs will find evidence in an investigation. In Part IV, we consider what happens when innovation occurs on a sliding scale—when the choice is still whether to innovate, but there is a range of innovation options.

Third, unlike in the Becker model, the likelihood that LEOs will investigate a crime is not fixed for any given crime,[186] but instead changes depending on whether the criminal innovates. The exact manner in which innovation changes the law-enforcement decision whether to investigate depends upon the incentives that LEOs face, but it is clear that LEOs will be less likely to investigate if criminals innovate because the likelihood of finding evidence is reduced. This interaction between the law-enforcement decision to search and the criminal's decision to innovate is central to the analysis and necessitates the use of game theory to analyze the situation.

---

restraints on crime.... Restrictions on police authority act as a tax; they make criminal investigations more expensive than they otherwise might be." (footnote omitted)).

184. *See, e.g.*, Malik, *supra* note 152.

185. *See id.*

186. *See* Becker, *supra* note 143, at 181 (explaining the variables in the Becker model).

The criminal will aim to maximize his expected utility,[187] which will change depending on whether he innovates and whether LEOs investigate:

Figure 1: Criminal's Payoffs

		Law-Enforcement Action	
		Investigate	Not Investigate
Criminal's Choice	Innovate	$-c - a^L$	$-c$
	Not Innovate	$-a^H$	0

The first utility matrix shows the relative costs of innovating and not innovating, for each possible law enforcement action. Because the criminal does not know whether LEOs will in fact investigate, he weighs the relative costs and benefits of innovating or not innovating within each shaded column, which models when LEOs have either investigated or not investigated, respectively. This calculation is analyzed in Part III.C.

Criminal utility is a function of c, the cost of innovation, and a, the probability that LEOs will find a particular piece of evidence if they investigate, with the probability being high (a^H) if the criminal does not innovate, and low (a^L) if he does. The criminal's punishment if he is convicted has been normalized to equal 1; as such, c can be interpreted as the cost of innovation as a percentage of the amount of punishment the criminal faces.

Other variables that may influence a criminal's level of innovation, such as the probability that the criminal will be convicted if the evidence is found and the amount of punishment a convicted criminal will receive, are omitted because they do not affect the general result. Unlike for LEOs, the criminal's payoffs are the same in the Warrant and Nonwarrant conditions,[188] so only one matrix is shown.

187. We make the standard assumption that the criminal and law enforcement are risk-neutral. *See, e.g.*, Malik, *supra* note 152, at 341; Sanchirico, *supra* note 145, at 3 n.8.

188. The warrant requirement shapes the criminal's utility in that it determines the relative costs to the police of investigating and not investigating, which is accounted for in the

B. Law-Enforcement Activity

Unlike in most models of criminal innovation, which consider the likelihood of a law-enforcement investigation to be fixed,[189] LEOs in this model investigate only if it is in their best interests to do so. In order to assess the best interests of the police, we need to conceptualize law-enforcement utility. Unlike criminal utility, which is obviously the profits of crime, in these models it is standard to treat law-enforcement utility as constituted purely by an interest in effectively catching criminals. Thus, we disregard any other elements of job satisfaction or external interests, such as possibility of corruption. There is an opportunity cost for any law-enforcement investigation in terms of other investigations not undertaken or delayed; rationally, LEOs will prioritize investigations that are likely to lead to positive results. Viewed in these terms, it follows that LEOs will have an incentive to search less often if criminals innovate, because the likelihood of finding evidence in a search will be smaller.

Similar to the criminal, LEOs will try to maximize their expected utility. Just as the criminal's utility depends on the actions of law enforcement, in turn law-enforcement utility will change depending on whether the criminal innovates. But because LEOs do not know whether the criminal has innovated, they weigh the relative costs of investigating and not investigating in each possible scenario. Thus in the second utility matrix, LEOs decide whether to investigate by comparing the expected payoffs for a given criminal action in each shaded row.

Further complicating the situation here are considerations of the different payoffs to law enforcement first under the condition in which a warrant is required for the investigation, and then when no warrant is required:

---

criminal utility matrix.

189. *See, e.g.*, Malik, *supra* note 152.

Figure 2: Law-Enforcement Payoffs

A. Warrant Condition

		Law-Enforcement Choice	
		Investigate	Not Investigate
Criminal's Action	Innovate	$-z-w+ga^{L}$	0
	Not Innovate	$-z-w+ga^{H}$	0

B. Nonwarrant Condition

		Law-Enforcement Choice	
		Investigate	Not Investigate
Criminal's Action	Innovate	$-z+ga^{L}$	0
	Not Innovate	$-z+ga^{H}$	0

The variables z and w are constants that signify the cost of an investigation and warrant, respectively. An investigation is costly because of opportunity costs and the use of law enforcement resources. Warrants are directly costly to obtain because of the time and resources necessary to obtain a warrant and are also indirectly costly—that is, they are costs that exist because of the warrant requirement, rather than the cost of acquiring a warrant. These indirect costs are twofold: First, some prospective investigations will be foreclosed due to the probable cause requirement necessary to procure a warrant. Second, there is the possibility that evidence will be destroyed during the warrant application process.[190] We can nonetheless group these costs together as costs of the warrant, w, which are fixed costs of gaining a warrant—costs that do not arise in the Nonwarrant condition.

The variable g signifies the gain to law enforcement that comes from a conviction. This gain includes all of the societal benefits of catching and convicting a criminal, such as the deterrence of future

190. A cost that was previously more considerable than it is now, in an era of electronic warrants.

crime, the punishment of past crime, and the successful return of money or goods that were taken in a crime. Finally, a is again the probability that evidence will be found in an investigation and is again conditional on the amount of innovation that the criminal has chosen. As with the variables that make up the criminal's expected utility function, each of these variables is assumed to be positive. Once again, other variables that do not change the model, such as the probability of conviction if evidence is found in an investigation, are omitted for simplicity.

We have made the difference between the Warrant and Nonwarrant conditions as simplified as possible—warrants increase the cost for LEOs, but have no other effect. This establishes the easiest possible test for the Police Efficiency Assumption. If we can show that the Assumption sometimes fails under these conditions, then it should fail more often under more complex conditions in which the warrant requirement also changes criminal incentives directly.

C. Game-Theoretic Solutions

We need to adopt a solution form that captures the simultaneous dynamic of criminal innovation and law-enforcement response, given that a criminal's utility depends not only upon his own decision whether to innovate, but also upon the decision of LEOs to investigate, and vice versa. Game theory is the study of situations in which the results of a person's actions depend not only on her own decisions, but also upon the decisions of others.[191] It defines the best strategy of each party for every possible choice, given the expected action of the other party.[192]

Broadly speaking, games can be either sequential or simultaneous. In a sequential game, one player chooses her action before the second player, and the second player knows what the first player chose. In a simultaneous game, both players choose their actions at the same time, with no knowledge of what the other has chosen. In the real world of criminal innovation, of course, a criminal will make the decision whether to innovate before LEOs decide whether to investigate. However, often the LEO will also not initially know

191. *See* OSBORNE, *supra* note 176.
192. *See supra* Part II.A.

whether the criminal has masked his crime through innovation; the LEO thus cannot base her investigation decision on the criminal's innovation decision, and the criminal will not know whether law enforcement is likely to investigate. Therefore, the game ought to be modeled as a simultaneous game because even though the criminal actually makes his decision first, the players might as well have made their decisions simultaneously.

Here, there are two separate games: one for the Warrant condition, and one for the Nonwarrant condition. In the latter, LEOs do not need to pay the cost w of obtaining a warrant if they decide to investigate. The two players in the game are the criminal and the law-enforcement agency. Each has two possible actions: the criminal can innovate or not innovate; law enforcement can investigate or not investigate. The solution maps the response of each player for each possible set of actions of the other. For instance, the criminal can adopt a strategy to innovate regardless of what law enforcement does—hence the (Innovate, Investigate) and (Innovate, Not Investigate) options in Figure 2.[193] We look at the utilities associated with such a choice and predict the outcome for each player, given the likely response. Both actors attempt to maximize their own expected utility, but must keep in mind the decisions of the other actor when doing so.

From interpreting the games in the Warrant and Nonwarrant conditions, we can determine if (or how often) the criminal will innovate and LEOs will search, depending on the other variables in the model. To do so, it is necessary to determine the Nash equilibria for each game. A Nash equilibrium occurs when both players are playing the best possible response they can, given the actions of the other player.[194] For example, (Innovate, Not Investigate) is a Nash equilibrium if (a) the criminal is better off innovating than not innovating, assuming that LEOs do not investigate, and (b) law enforcement is better off not investigating than investigating, assuming that the criminal innovates. We find the solutions to the game by finding the Nash equilibria: only outcomes that are Nash equilibria should arise, because outside that equilibrium, by definition at least

193. The first part of the parenthetical is the criminal's action, and the second part is the action of police.

194. MORROW, *supra* note 175, at 80.

one player will be better off by unilaterally changing his or her strategy.[195] A game can have one Nash equilibrium, many, or none.[196] Thus, the solution to the game does not tell us the only possible course of action; rather, it tells us the possible outcomes.

There are two types of Nash equilibria. The example of (Innovate, Not Investigate) is a "pure strategy Nash equilibrium" because each player will definitely play a particular action in this equilibrium.[197] A game may also have "mixed strategy Nash equilibria," in which one or both players, rather than choosing one definite action, choose between different actions based on a probability distribution over the player's possible actions.[198] For example, there could be a mixed strategy Nash equilibrium in which the criminal innovates with a probability of one-third (and does not innovate with a probability of two-thirds), and in which LEOs investigate with a probability of three-fourths (and do not investigate with a probability of one-fourth). Conceptually, this means that LEOs do not know whether the criminal will innovate; however, for a given probability that the criminal will innovate, they have a best response, which may itself be probabilistic. By finding the Nash equilibria in these two games, it is possible to determine when the Police Efficiency Assumption does not hold. The assumption will fail if, for a given set of parameters, law-enforcement utility in the Nash equilibrium under the Warrant condition is greater than or equal to law-enforcement utility in the Nash equilibrium under the Nonwarrant condition.

We now present the Nash equilibria, with brief intuitive explanations of what they each contain. The next Section describes in more detail the substantive meaning and significance of each possible outcome, and our overall results. There are three possible pure Nash equilibria in the warrant world. Only one of the equilibria can

---

195. *See id.* at 81 ("A Nash equilibrium is stable because neither player has an incentive to deviate unilaterally from its equilibrium strategy."). Some scholars have argued that Nash equilibria are not in fact accurate predictions of human behavior. *See, e.g.*, George J. Mailath, *Do People Play Nash Equilibrium? Lessons from Evolutionary Game Theory*, 36 J. ECON. LITERATURE 1347, 1347-48 (1998); Rosemarie Nagel, *Unraveling in Guessing Games: An Experimental Study*, 85 AM. ECON. REV. 1313, 1325 (1995). However, they are more likely to be accurate when games are repeated multiple times, as will be the case with the police and criminals. Mailath, *supra*, at 1353; Nagel, *supra*, at 1325.

196. *See* OSBORNE, *supra* note 176, at 23-24.

197. *See* ORDESHOOK, *supra* note 163, at 118.

198. *See id.* at 133.

actually occur at a time; which one will occur will depend on the values of different variables within the model.

> (Innovate, Investigate) is a Nash equilibrium if $c<a^H-a^L$ and $w+z<ga^L$. Intuitively, this is when the cost of innovation is less than the resultant expected gain in reduced detection and punishment, and when the expected gains to law enforcement from investigating are larger than the fixed costs of the investigation and warrant.
>
> (Not Innovate, Investigate) is a Nash equilibrium if $c>a^H-a^L$ and $w+z<ga^L$. Intuitively, this is different from the first equilibrium in that the gains from innovation are now smaller than the cost.
>
> (Not Innovate, Not Investigate) is a Nash equilibrium if $ga^H>w+z$, meaning that the gain to law enforcement from investigating is smaller than the costs, even if the criminal does not innovate.[199]
>
> Note that the outcome (Innovate, Not Investigate) is never a Nash equilibrium because if LEOs are not going to investigate, the criminal would be better off not innovating.

There is also one mixed strategy Nash equilibrium in the warrant condition: The criminal innovates with probability $\lambda=\left[\frac{1}{a^H-a^L}\right]\left[a^H-\frac{w+z}{g}\right]$, and LEOs investigate with probability $\phi=\frac{c}{a^H-a^L}$. This Nash equilibrium occurs when $c<a^H-a^L$ and $ga^L<w+z<ga^H$. Intuitively, this means that LEOs will mix strategies when the cost of investigating is in between the expected utility that they receive if the criminal does innovate and does not innovate,[200] and once again that the criminal will innovate when the cost of innovation is less than the resultant expected gain in reduced detection and punishment.

---

199. The criminal prefers to innovate if LEOs investigate only if $c<a^H-a^L$. Likewise, LEOs prefer to investigate if the criminal innovates if $ga^H>w+z$. (Innovate, Not Investigate) is not an equilibrium: If LEOs do not investigate, the criminal will choose not to innovate, because $b>b-c$.

200. Thus, the criminal will mix if $EU_c(\textit{Innovate, Investigate})\cdot p_p(\textit{investigate})+EU_c(\textit{Innovate, Not Investigate})\cdot[1-p_p(\textit{Investigate})]=EU_c(\textit{Not Innovate, Investigate})\cdot[1-p_p(\textit{Investigate})]$.

There are also four Nash equilibria in the Nonwarrant condition. These are the same as the Warrant condition Nash equilibria, except without the "w" warrant cost terms:

- (Innovate, Investigate) if $c < a^H - a^L$ and $z < ga^L$.
- (Not Innovate, Investigate) if $c > a^H - a^L$ and $z < ga^L$.
- (Not Innovate, Not Investigate) if $ga^H > z$.
- The criminal innovates with probability $\lambda = \left[\frac{1}{\alpha^H - \alpha^L}\right]\left[\alpha^H - \frac{z}{g}\right]$, and LEOs investigate with probability $\phi = \frac{c}{\alpha^H - \alpha^L}$ when $c < a^H - a^L$ and $ga^L < z < ga^H$.

D. When Is the Assumption Violated?

The Police Efficiency Assumption is violated if, for a given set of constants (z, w, c, g, a^L, and a^H), the expected utility of law enforcement under the Nonwarrant condition is not greater than it is under the Warrant condition, as is commonly assumed and used to justify nonapplication of the warrant requirement. This Section shows that the Assumption sometimes fails—sometimes law enforcement does not benefit from its ability to conduct warrantless searches, or from an investigation not being considered a Fourth Amendment search at all. Here we show when the Assumption will fail, when it will not, and argue that the circumstances when the Assumption fails are likely to be quite significant.

We begin with two simple outcomes—one in which the Assumption holds, and one in which it fails—in order to illustrate the logic, before considering more complex scenarios. Consider the circumstance in which (Innovate, Investigate) is the Nash equilibrium under both the Warrant and the Nonwarrant condition. If we were to move from the Warrant condition to the Nonwarrant condition—for instance, if the law became less stringent for law enforcement—LEOs would face lower costs because they would not have to bear the costs of seeking a warrant. Furthermore, because the criminal is already innovating under this set of strategies, LEOs would also encounter no greater difficulty in finding evidence. Thus, the Assumption is not violated: elimination of the warrant requirement would simply lower law-enforcement costs.

In contrast, if (Not Innovate, Not Investigate) is the equilibrium in both conditions, the Assumption is violated. Under both scenarios, LEOs receive utility of zero because they do not investigate. Doing away with the warrant requirement does the officers no good if they are not going to investigate even without the costs of a warrant. This example is not very informative about the effect of warrants on innovation and law-enforcement investigation because in this scenario neither investigation nor innovation ever takes place; but other equilibria that violate the Assumption have more significance.

More significantly, the Police Efficiency Assumption is violated if the Nash equilibrium is a mixed strategy in both of the conditions. The mixed strategy will be a Nash equilibrium under both conditions if $c<a^H-a^L$ and $ga^L<z<w+z<ga^H$. The latter term requires that $w<ga^H-z$ and $\frac{z}{g}<a^H-a^L$. If the Nash equilibrium in both conditions is mixed, we can test the Assumption by determining when the expected utility of law enforcement in the Warrant condition is greater than or equal to the expected utility in the Nonwarrant condition, with both actors mixing with the probabilities given by the equilibrium. It turns out that in this mixed Nash equilibrium, LEOs gain no benefit from not having to obtain warrants.

The Assumption failing whenever a mixed strategy is the equilibrium in both conditions is a very significant result, as we can expect this to be a very common outcome. Most pure strategy Nash equilibria are somewhat artificial: it is quite obvious that the criminal may be better off innovating if LEOs are going to investigate, but they will not bother incurring the cost of innovating if LEOs are not going to investigate. But because the criminal will have to make that decision without knowing what LEOs will do, he will usually be better off varying his strategy, that is, playing a mixed strategy. Similarly, if criminals generally know that LEOs will always investigate when they innovate, the criminals will have an advantage; therefore, LEOs will be better off varying their approach, and playing a mixed strategy. In combination, the outcome will be a mixed strategy equilibrium. Thus, in reality, we would expect mixed equilibria to be the most common result in the criminal innovation-police response game. This first result shows that in this common situation, LEOs will not benefit from their

ability to investigate without a warrant—that is, a warrant requirement will not impede police efficiency.

The second significant result of our model is that the Assumption is also violated in a switch from the pure strategy equilibrium (Not Innovate, Not Investigate) to the mixed equilibrium. When mixing, the police will have an expected utility of zero—the same as when they do not investigate.[201] This situation will occur when $c<a^H-a^L$ and $ga^L<z<w+z<ga^H$. Conceptually, this result shows that criminals will increase their innovation when LEOs do not have to obtain a warrant.

We argue that the failure of the Assumption in these circumstances is not a fluke that occurs only rarely when the variables just happen to align in a certain way. Rather, the circumstances in which the Assumption fails likely characterize a large percentage of potential law-enforcement investigations. This becomes clear once one considers what having a mixed Nash equilibrium means in this police-criminal interaction. For the criminal, it means that innovating is worth its cost when he is certain that LEOs will investigate, but innovating is not worthwhile if LEOs are definitely not going to investigate. Obviously, the criminal has no reason to innovate if LEOs are not going to investigate because innovation is costly; thus this requirement is satisfied if the innovation's cost is less than the gain to criminals in detection reduction. This is likely to be the case in many circumstances, and only would rule out innovations that are costly yet bring few gains. We discuss specific applications of this conclusion in the next Part. For LEOs, the mixed Nash equilibrium simply means that LEOs would find it worthwhile to search if they were sure the criminal did not innovate, but would choose not to search if they knew the criminal had innovated. For the mixed Nash equilibrium to hold in both scenarios, this cost-benefit relationship would have to hold both with and without the cost of the warrant included. Again, this seems likely to be true in

201. If LEOs get zero utility from mixing—the same that they would get from never investigating—why do they ever investigate? They mix because ceasing investigations altogether would create an unstable situation that would lead back to the mixed equilibrium. If LEOs stop investigating, the criminals will stop innovating. But because the probability of finding evidence then rises, LEOs will sometimes start investigating—putting us back where we started.

many real-life cases, in which criminal innovation can turn a worthwhile law-enforcement investigation into a losing proposition.

We can generalize our results rather than viewing them in terms of moving from one equilibrium to another. The Police Efficiency Assumption is violated under the following conditions:

(1) $c<a^H-a^L$ and $ga^L<z<w+z<ga^H$.

This first result means that the Assumption is violated when, for the criminal, the cost of innovation is less than the difference between the high and low probability that LEOs will find a particular piece of evidence if they investigate; and for LEOs, the cost of obtaining a warrant and investigating are greater than the gains of a search that is unlikely to be successful and less than the gains of a search that is likely to be successful.

(2) $c<a^H-a^L$ and $ga^L<z<ga^H<w+z$.

This second result means that the Assumption is violated when the cost of innovation is as described in (1); and that the cost of an investigation without a warrant also lies in the region described in (1). But rather than the cost of the warrant adding to the cost of the investigation, instead this requirement holds that the probabilistic gain of a successful search is less than the cost of an investigation and the cost of gaining a warrant.

Together, these two results show that the Assumption can fail when the costs to law enforcement outweigh the benefits of a probabilistically successful search, and also when they do not, as long as the other requirements hold.

(3) $ga^H<z$.

Third, the Assumption is also violated if LEOs do not search in either condition. This means that the gains of a successful investigation are less than the cost of investigation, which makes it not worthwhile for LEOs to search, regardless of whether they need a warrant.

Finally, external factors can change specific elements of the police-criminal interaction. For instance, as technology improves, innovation could become less costly. Our results yield comparative statics[202] that allow us to show how the likelihood that the Assumption

202. "Comparative statics is the method of analyzing the impact of a change in the para-

is violated varies with such changes. Changes could take place that affect the incentives of criminals, which in turn affects the incentives of law enforcement. First, the Assumption is weakened as the cost of innovation (c) decreases, because criminals are more likely to innovate when they face lower costs. If criminals innovate more, the chance of a successful investigation decreases, and LEOs are less likely to investigate even without the warrant requirement. Second, a greater innovation-created reduction in the likelihood of LEOs finding evidence in an investigation ($a^H - a^L$) weakens the Assumption. This could come about, for instance, as innovation methods become more effective. Once again, that would drive criminals to innovate more. We discuss some of the costs associated with various electronic innovations in the next Part.

Additionally, changes could take place that affect the incentives of LEOs more directly. First, although the cost of seeking a warrant (w) does not determine when the Assumption is violated, it does matter in assessing the gains of law enforcement when the Assumption *is not* violated. If LEOs are certain to investigate in both conditions, the extent that they are better off is determined solely by that cost. Second, the Assumption fails when the non-warrant cost of an investigation (z) is neither too high nor too low, relative to the difference in a high and low likelihood of finding evidence. If investigations become expensive enough, they will be worthwhile to do only some of the time, warrant or not, and the Assumption fails. Additionally, the Assumption is also violated if z is so high that LEOs never investigate.

Overall, our findings show that the Police Efficiency Assumption can fail under many different circumstances. That failure is not contingent on a very specific cost of innovation or a particularly high cost of investigation, for example, but rather hinges on the relationship between the two. Most importantly, we have shown that the only possible mixed equilibria involves the Assumption failing—which means that the Assumption is likely to fail if there is a serious degree of uncertainty between likely responses and counterresponses among criminals and law enforcement. In the next Part,

---

meters of a model by comparing the equilibrium that results from the change with the original equilibrium." 1 THE NEW PALGRAVE: A DICTIONARY OF ECONOMICS 517 (John Eatwell et al. eds., 1998).

we show how these theoretical results bear out in practice, and illustrate how the uncertainty is likely to be common, and thus so is the regular failure of the Police Efficiency Assumption.

IV. DISCUSSION AND POLICY IMPLICATIONS

Our results have significant implications for current Fourth Amendment thought. We first consider the general implications of our findings, and we then consider the specific application of electronic privacy.

A. General Implications

First, the assumption that the job of law enforcement in catching criminals is greatly simplified when a warrant is not required to investigate is severely weakened when criminals can innovate. Our results show that in many situations, law enforcement is not in fact better off when a warrant is not required. This includes the most likely scenario, in which LEOs will investigate sometimes, but not all the time, in both the Warrant and the Nonwarrant conditions. Additionally, although there are circumstances in which law enforcement will be better off without having to obtain a warrant, the degree to which they gain is smaller in some of these situations if criminals are able to innovate.[203] The Police Efficiency Assumption is a key part of the balancing inquiry that courts undertake to determine whether a warrant is required for a particular investigation.[204] Our analysis shows that the weight of this Assumption in that balance should be significantly lowered.

Second, ridding law enforcement of the necessity of obtaining a warrant does not affect just criminals: it does great harm to people who have not committed a crime. The Fourth Amendment is meant to protect those who LEOs wrongly suspect. In such a case, law enforcement and the suspect will have different information to one another—whereas the civilian knows that she has committed no

203. Specifically, the gain to law enforcement is not diminished by innovation when they would search with certainty in the Warrant condition; this is when (Innovate, Investigate) is a Nash equilibrium in this condition. Law enforcement's gain will be diminished by innovation in a switch to or from the mixed strategy Nash equilibrium.

204. *See supra* Part I.

crime, law enforcement will wrongfully suspect her. In that case, the suspect—who is actually innocent—is unlikely to innovate. LEOs, however, will be more likely to investigate in the Nonwarrant condition because the investigation is less costly.[205] Thus, without a warranty requirement, there will be a greater number of investigations of innocent suspects.[206] The privacy interests of innocent people are harmed when LEOs are not required to obtain a warrant for an investigation.[207] We have shown that the Police Efficiency Assumption is fragile even ignoring these effects;[208] considering these important privacy ramifications weighs further against the Assumption when determining whether an investigation should be termed a search. We explore this in greater detail with reference to specific applications in the next Section.

Furthermore, the weakness of the Police Efficiency Assumption casts a further shadow on the already much-maligned reasonable expectation of privacy test for determining whether an investigation is a Fourth Amendment search. As noted above, the reasonable expectation of privacy test has often been derided as circular because the actions of law enforcement—as well as court decisions and legislation—shape societal expectations.[209] This allows the state to gradually shift the boundaries of what law enforcement is constitutionally allowed to do by engaging in small increases in surveillance over time that are mild enough to avoid judicial reproach but significant enough to change expectations.[210] Reasonable expectations of privacy also diminish over time as technology increasingly intrudes upon private life, at least when courts allow the use of new surveillance tools.[211] As more and more surveillance

205. *See supra* Part I.B (noting that proponents and opponents of the warrant requirement recognize the cost of obtaining a warrant impedes the investigation process).

206. This is a common argument made in favor of requiring warrants. *See, e.g.*, Oren Bar-Gill & Barry Friedman, *Taking Warrants Seriously*, 106 NW. U. L. REV. 1609, 1652-57 (2012); Christopher Slobogin, *Why Crime Severity Analysis Is Not Reasonable*, 97 IOWA L. REV. BULL. 1, 5 (2012).

207. *See, e.g.*, L. Rush Atkinson, *The Bilateral Fourth Amendment and the Duties of Law-Abiding Persons*, 99 GEO. L.J. 1517, 1527-29 (2011) (arguing that innocent people may change their behavior to avoid being targeted as suspects).

208. *See supra* Parts II.B, III.D.

209. *See supra* notes 37-40 and accompanying text.

210. *See* Jacobi, *supra* note 39 (noting that a reasonable expectation of privacy depends on how frequently the police breach that expectation).

211. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 47 (2001) (Stevens, J., dissenting) ("[T]he

techniques become expected, the privacy of all—criminal and noncriminal alike—recedes. The standard response to this critique is that such diminished privacy will make it easier for LEOs to catch criminals, yet our analysis shows the weakness of this assumption.[212] In particular, although increased law-enforcement authority to undertake warrantless investigations may decrease the amount of crime—innovation is costly, and a need to innovate may make committing some crimes ex ante irrational—it will in many cases not increase the likelihood that criminals will be brought to justice.[213]

Importantly, combining these last two implications means that there will be an increased need for noncriminals to innovate. Without the warrant requirement, with a decreasing realm of privacy and less costly law-enforcement investigations, innocent people may face a stark choice: either acquiesce to increased law-enforcement intrusion upon their privacy rights, or spend their resources on their own "innovation." For the innocent, such innovation consists not of finding ways to hide incriminating evidence from law enforcement, but rather of measures legitimately taken to protect one's privacy from intrusion.[214] Innocent civilians may need to buy encryption programs to protect themselves from cyber surveillance, or a roof to protect their backyard from police helicopter videography. Of course, criminals will do the same, and LEOs will not gain. In the next Section, we discuss how criminal and noncriminal innovation may intensify in the new context of mass NSA searches.

We have shown that the reliability of the Police Efficiency Assumption is much weaker than previously thought,[215] and that continuing to rely on it has severe adverse effects for privacy of noncriminals.[216] Accordingly, we must now consider what potential

---

threat to privacy will grow, rather than recede, as the use of intrusive equipment becomes more readily available."); Steven Penney, *Reasonable Expectations of Privacy and Novel Search Technologies: An Economic Approach*, 97 J. CRIM. L. & CRIMINOLOGY 477, 483-86 (2007).

212. *See supra* Part II.B.

213. *See supra* Part III.D.

214. *E.g.*, Doug Gross, *How to Hide Your Data from Internet Snoops*, CNN, http://www.cnn.com/2013/06/18/tech/web/how-to-encrypt-email/ [http://perma.cc/JR8R-Z9Q9] (last updated June 19, 2013, 6:47 AM).

215. *See supra* Part II.B.

216. *See* Atkinson, *supra* note 207.

policy responses can be made, given our results. There are three primary policy options stemming from the above analysis, but each have their drawbacks.

First, courts could decide to give the Police Efficiency Assumption less weight when deciding whether to term an investigation a search or a nonsearch. This option is compelling because of the weakened strength of the Assumption when criminals are able to innovate, as well as the negative effects that terming an investigation as a nonsearch has on innocent suspects.[217] Our analysis also shows, however, that allowing LEOs to investigate without a warrant does make the job of law enforcement easier in a significant amount of situations.[218] Consequently, we do not recommend that the Assumption should be entirely eliminated, but our results do show that the weight accorded to it should be diminished.

Second, courts could tailor their analyses by giving the Assumption less weight in situations when it is least likely to hold. Courts could consider whether the possibility of criminal innovation, and any potential counterresponse by law enforcement, is likely to make the Assumption particularly unreliable. At a general level, courts could be particularly careful about making the Assumption when considering whether to define an investigation as a search or a nonsearch—in contrast to recognizing an investigation as a search, but invoking a warrant exception—because criminal innovation can exacerbate the self-reinforcing nature of an absence of a reasonable expectation of privacy, as described above.[219] When we get into more specific recommendations, however, this policy option becomes more treacherous.

A variant of this more particularized scrutiny of the Police Efficiency Assumption would be to apply it differentially for different crimes. For example, consider a specific investigation: a canine sniff of an air passenger's luggage. It is possible that the cost of preventing the detection of marijuana (through selective plant breeding or cloaking scents) could be very different than the cost of preventing the detection of cocaine. Thus, the Assumption could be

217. *See id.* (discussing ways in which innocent citizens suffer and alter behavior if searches increase); *see also supra* note 207 (showing that unconstitutional searches already take place, and that many innocent individuals are searched).

218. *See supra* Part III.D.

219. *See supra* Part II.B.

violated when a certain type of investigation targets one crime, but not violated when it targets a different crime. The problem with this approach is that courts would need to undertake, albeit intuitively, essentially the same analysis contained in Part III. Courts would need to consider the cost of warrants, investigations, and criminal innovations, as well as the decreased probability that police will find evidence as a result of an innovation. But such a task would be quite difficult for courts—formal models are an attempt to capture the effect of various incentives, not advocate a blueprint of proposed judicial analysis.

Nevertheless, we can ascertain general principles from the model as to when the Assumption is more likely to hold, and use that as a tool for particularized application. One general result is that the Assumption is more likely to hold when the gains to law enforcement of a conviction are particularly high[220]—or, put differently, when the severity of the crime is high. Legal scholars commonly argue that courts should "incorporate the severity of the crime being investigated into determinations of constitutional reasonableness" when deciding whether a warrantless search is reasonable, or whether an investigation is a search at all.[221] The Justices explicitly considered whether to include seriousness of the offense in a case last term.[222] However, this type of "crime severity analysis" is controversial.[223] The analysis raises serious legitimacy concerns because it means that a defendant's rights decrease as the length of the potential sentence he faces increases. Another problem with this approach is that some general results of the model may point in somewhat different directions. For instance, in addition to demonstrating that the Assumption is more likely to hold when the crime is more serious, the model shows that the Assumption is

220. This result occurs because the police will investigate with or without needing to obtain a warrant, whereas the criminal will not change her innovation behavior.

221. Bellin, *supra* note 50, at 6; *cf.* Richard A. Posner, *Excessive Sanctions for Governmental Misconduct in Criminal Cases*, 57 WASH. L. REV. 635, 645 (1982) ("The graver the crime, the more the parties are likely to invest in the litigation process itself, and that greater investment should increase the accuracy of the guilt-determining process.").

222. Navarette v. California, 134 S. Ct. 1683 (2014). At oral argument, in analyzing whether independent corroboration is required to stop a driver who is reportedly under the influence, the Justices considered whether a sliding scale should apply depending on the seriousness of the offense. Transcript of Oral Argument, Navarette v. California, 134 S. Ct. 1683 (2014) (No. 12-9490).

223. *See* Slobogin, *supra* note 206, at 2.

particularly likely to hold when warrant costs are high.[224] In contrast to the implication of the seriousness result, the implication of this second effect suggests that making warrants easy for the police to obtain is not necessarily the right decision.

The third and final possible policy change that could be made is reducing the frequency of situations in which the Assumption does not hold. One route could be to increase the cost of innovation so that criminals will be less likely to innovate. One way to do this is to increase punishments or increase the likelihood of conviction—common proposals in economic models of crime.[225] Either of these responses, however, would make it *more* likely that the Assumption will fail because the criminal will be *more* likely to innovate.[226] An alternative to ex post punishment of innovation is ex ante regulation of criminal innovation through taxes.[227] Taxation is likely to be more effective than increased punishment because it reduces both innovation and crime.[228] However, ex ante taxation of criminal innovation is very difficult because it is often impossible to discern whether a product will be used for legitimate purposes or for criminal innovation.[229] This concern applies not only to seemingly innocent products that can be used to cover up crimes, such as a balaclava, but in light of our previous findings that innocents may need to innovate in order to protect their privacy, could also apply to products specifically designed for eluding law-enforcement detection, such as encryption software.[230] A separate problem is that punishing innovation creates an incentive for the criminal to innovate further, to cover up the initial innovation.[231] Finally, raising the costs of innovation also raises barriers to use these mechanisms

224. *See supra* Part III.D.

225. *See, e.g.*, James Andreoni, *Reasonable Doubt and the Optimal Magnitude of Fines: Should the Penalty Fit the Crime?*, 22 RAND J. ECON. 385-86 (1991) (critiquing maximum punishments for decreasing the probability of conviction); Polinsky & Rubinfeld, *supra* note 41, at 292-93 (arguing that maximal deterrence may require increasing punishment levels for recidivists).

226. Nussim & Tabbach, *supra* note 14, at 46, 56-57.

227. *Id.* at 48.

228. *Id.* at 46, 55-56.

229. *Id.* at 46.

230. *See infra* note 247 and accompanying text (noting that encryption use is so rare among citizens that encrypted e-mails are subject to greater scrutiny by the NSA).

231. Sanchirico, *supra* note 151, at 1339.

for privacy protection by innocents, as explored in detail in the next Section.

B. Application to Private Communication in the Digital Age

This Section considers in what situations the central result of our model—the challenge to the orthodoxy that law enforcement will always be better off without a warrant requirement—is likely to have a significant impact. We demonstrate that the most normatively unattractive outcome, situations in which innocent individuals suffer from the lack of a warrant requirement yet LEOs gain little benefit in terms of catching criminals, is increasingly likely to arise in the digital arena. We show this by considering in detail how some privacy-enhancing innovations actually work, and why many are ill-suited to meeting the needs of innocents but are nonetheless attractive to wrongdoers when warrants are not required for LEOs to search. We first consider e-mail encryption, and its practical limitations for the average noncriminal user. Then we describe new alternative means of electronic identification and content masking, such as Privnote and Snapchat. These programs offer less protection than e-mail encryption, but are considerably more practical. This allows us to consider what occurs when there exists a range of options for criminal innovation. Finally, we assess how the negative repercussions we describe compare to the privacy incursions posed by the NSA spying program.

1. E-mail and Encryption

Although e-mail constitutes one of the central mechanisms of modern communication for private individuals, the constitutional privacy status of the trillions of e-mails[232] sent annually in the United States is ambiguous.[233] The primary reason for the potential

232. Worldwide, over 144 billion e-mails are sent per day; North America accounts for 14 percent of worldwide e-mail users. THE RADICATI GRP., EMAIL STATISTICS REPORT, 2012-2016—EXECUTIVE SUMMARY 2-3 (Sara Radicati ed., 2012), *available at* http://perma.cc/RM7A-PWTN.

233. *See* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2110 (2009).

lack of privacy from state incursions[234] is the operation of the third-party doctrine. Most individuals' e-mails are sent through massive Internet Service Providers (ISPs), such as Gmail, Hotmail, or Yahoo.[235] As such, the third-party doctrine applies, under which any communication shared with a third party—even in a rote fashion, such as making a bank deposit—is deemed to have been voluntarily shared, and consequently, any expectation of privacy in the information is lost.[236] Whether the Court will follow the third-party doctrine to this logical extreme is still untested—as discussed below, lower courts have been split on whether the NSA trawling through millions of e-mails is lawful, and at least one Justice has questioned whether the breadth of the doctrine is appropriate in the digital age.[237] As precedent stands,[238] however, ISP-based e-mail is unprotected from state surveillance.[239]

Both innocents and wrongdoers who wish to keep their e-mails private may consider potential innovations to counter the transparency of e-mail systems. The most commonly contemplated response is encryption,[240] but understanding how both e-mail systems and encryption work reveals the impracticality of this for the average

234. The possibility exists that private individuals may be able to access this information; this possibility likewise encourages the type of innovation we explore below.

235. *Email Security and Anonymity*, ANONYMOUS INTERNET COMMUNICATIONS, http://www.anonic.org/email-security.html [http://perma.cc/ML34-SF29] (last visited Feb. 22, 2015).

236. *See supra* notes 78-89 and accompanying text.

237. *See supra* note 87. However, Justice Sotomayor's critique was already understood, yet overridden, when *Smith v. Maryland* was decided. In that case, the dissenters argued that allowing the government to access information divulged to third parties would "prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts." Smith v. Maryland, 442 U.S. 735, 751 (1979) (Marshall, J., dissenting).

238. *See infra* notes 314-15 and accompanying text (noting that the district court that held the NSA's actions to be presumptively unconstitutional did so by concluding that *Smith v. Maryland* no longer applied).

239. It is unclear whether avoiding using ISP-run e-mail would circumvent the application of the third-party doctrine. For an individual to use a personalized e-mail system through her own server typically still requires "sharing" her information with the server provider of the website. If the Supreme Court does determine that the third-party doctrine applies to e-mails sent through ISP systems such as Gmail, it will then have to decide whether the doctrine applies to websites generally.

240. *See, e.g.*, Gross, *supra* note 214; *NSA-Proofing: How to Hide Data from Online Surveillance*, WEEK, http://www.theweek.co.uk/technology/55423/nsa-proofing-how-hide-data-online-surveillance [http://perma.cc/8N4W-GMGU] (last updated Oct. 3, 2013, 2:26 PM).

e-mail user. Even after learning about the NSA's spying program, most ordinary e-mail users do not use encryption. In fact, use of encryption is so rare that the NSA treats an encrypted message as a priority for its scrutiny.[241] The reason for this lack of use of encryption is that it is costly in numerous ways. Each recipient of each e-mail sent by the user must have the tools to decrypt any message sent to them.[242] Although this is becoming simpler for any given relationship, with various programs being developed that use public access keys, it is not practical for encrypting all e-mail because the recipient must have the same program as the sender.[243] Thus, although encryption may be worthwhile for specific messages that require particular privacy—such as criminal action—it is impractical for everyday use by ordinary users e-mailing a plethora of recipients.

Until recently, users could not encrypt messages with standard web-based e-mail providers, because the business model underpinning those services is based on advertising, which involves content analysis of e-mail messages.[244] Typically, ISPs only encrypted outgoing traffic, not internal traffic.[245] In the wake of increased public

---

241. Friedrich Lindenberg & Christian Stöcker, *How to Encrypt Emails: Protect Yourself from Online Snoops*, SPIEGEL (Oct. 29, 2013, 4:33 PM), http://www.spiegel.de/international/how-to-encrypt-emails-protect-yourself-from-online-spying-a-930665.html [http://perma.cc/G5JE-F383].

242. *Id.*

243. Sue Marquette Poremba, *Why You Need to Use Encrypted Email*, TOM'S GUIDE (Sept. 16, 2013, 12:26 PM), http://www.tomsguide.com/us/encrypted-email,news-17510.html [http://perma.cc/VYE3-8TND].

244. The e-mails typically traveled from the user to her ISP, to the recipient's ISP, and then to the eventual recipient, with only encryption at the middle stage. Consequently, even if messages were initially encrypted, they did not stay encrypted in the ISP system. *See* Danny Sears, *Is Your Company's Email Protected? How Does Email Security Really Work?*, EVERON (Nov. 19, 2010), http://www.everonit.com/techtips/small-business-computer-tips/email-protection/ [http://perma.cc/Y8YG-9CGN]; *Your Security and Privacy*, GOOGLE, https://support.google.com/a/answer/60762?hl=en [http://perma.cc/UD2H-YMWV] ("Our systems scan and index emails ...; this scanning is 100% automated and cannot be turned off .... [This] enable[s] us to display contextually relevant advertising.").

245. Ed Felten, *End-to-End Encrypted GMail? Not So Easy*, FREEDOM TO TINKER (Dec. 18, 2012), https://freedom-to-tinker.com/blog/felten/end-to-end-encrypted-gmail-not-so-easy/ [http://perma.cc/WSD6-NW8V]. Yahoo, Google, and Microsoft now encrypt the outgoing traffic from their servers to the user to prevent eavesdropping. John Leyden, *Well Done for Flicking Always-on Crypto Switch, Yahoo! Now Here's What You SHOULD Have Done*, REGISTER (Jan. 9, 2014), http://www.theregister.co.uk/2014/01/09/yahoo_always_on_crypto_unstrong/ [http://perma.cc/PTX5-KWQF].

demand following the NSA spying revelations, Google introduced a mechanism of encrypting Gmail-to-Gmail messages[246] and is putting pressure on other providers to improve their encryption options by reporting rates of encryption.[247] But commentators have observed that Google likely expects only the highly security-conscious minority to actually utilize the encryption software, thus enabling the continuation of its income stream.[248] And this should not be surprising, given the financial incentives of ISPs such as Google. The reality is that Gmail is not free; users pay for it partly by subjecting themselves to advertising and by providing Google with useful data at the aggregate, and possibly the individual, level.[249] Fully encrypting e-mails requires a very different quid pro quo. Therefore, for Google or a competitor to fulfill the demand of the majority of its users for encrypted e-mail in its system, it would have to develop an alternative, viable revenue stream. Any competitor would have to do so while also creating a competitive e-mail interface—with all the complex computer algorithms and marketing that involves—and a way of entering a market strongly dominated by a few powerful companies.[250] Even then, spam filtering would become impossible with encryption between the user and the ISP; users would have to be sharply protective of their privacy to give up spam filtering.

Add to these factors various other inconveniences associated with encryption, such as probably rendering inbox searches impossible,[251]

---

246. Seth Rosenblatt, *New Chrome Extension Hopes to Demystify Encryption*, CNET (June 3, 2014, 1:50 PM), http://www.cnet.com/news/new-chrome-extension-hopes-to-de-mystify-encryption/ [http://perma.cc/CGG9-8KHQ] ("Google has released a rough alpha extension for Chrome called End-to-End.").

247. *Email Encryption in Transit*, GOOGLE, https://www.google.com/transparencyreport/saferemail/?hl=en#search=google.com. [http://perma.cc/2E94-4EFU] (last visited Feb. 22, 2015).

248. Thomas Claburn, *Google Previews Gmail Encryption,* INFORMATIONWEEK (June 4, 2014, 3:26 PM), http://www.informationweek.com/mobile/mobile-business/google-previews-gmail-encryption/d/d-id/1269433 [http://perma.cc/6Y54-JUX4].

249. Yasha Levine, *Google and Encryption: Why True User's Privacy is Google's Biggest Enemy*, PANDO DAILY (Jan. 27, 2014), http://pando.com/2014/01/27/google-and-encryption-why-true-user-priacy-is-googles-biggest-enemy/ [http://perma.cc/DU8H-9US4].

250. As of late 2012, over 95 percent of Americans used either Yahoo, Gmail, or Hotmail for e-mail service. *See* Rani Molla, *Gmail Finally Beats Hotmail, According to Third-Party Data*, GIGAOM (Oct. 31, 2012, 10:38 AM), http://gigaom.com/2012/10/31/gmail-finally-beats-hotmail-according-to-third-party-data-chart/ [http://perma.cc/KL7A-EC8Z].

251. Conner Forrest, *Google's End-to-End Gmail Encryption: An Excellent Development*

and ordinary consumers are likely to come out on the non-use end of e-mail encryption. There is an inherent trade-off between security of encryption and ease of use,[252] so it is not surprising that private individuals rarely use encryption for e-mails.[253] This illustrates why our result that the loss of privacy for innocent individuals in cutting back on the warrant requirement—in order to promote the often illusory end of police efficiency—will be difficult to combat with innovation. Yet this is not likely to be the case for innovation by criminals, either for cybercrime or for electronically conveying information about nonelectronic crimes.

With the warrant requirement, the gains of masking e-mails pertaining to high-risk, high-reward criminal activity may consistently overcome the costs of innovation. The warrant requirement would simply add additional costs to law-enforcement investigation, because such criminals would innovate either way. For lower-grade crimes—particularly for ongoing criminal enterprises involving multiple contacts with multiple recipients, such as drug dealing at the end distribution stage—the same costs that arise for the innocent individual will apply to the small-time crook who needs to contact multiple clients or co-conspirators. The existence of the warrant requirement, with its associated perception that police will be restricted in their ability to conduct fishing expeditions by the need to establish probable cause prior to searching, may lead the marginal, cost-sensitive criminal to avoid incurring the costs of encryption. So in some cases, with the warrant requirement, criminals will innovate using encryption, and at other times it will not be worthwhile. Either way, as shown in our model, this could result in LEOs not searching, LEOs investigating and the criminal innovating, or LEOs investigating and the criminal not innovating. All three outcomes are Nash equilibria. So with the warrant

---

for the Enterprise, TECHREPUBLIC (June 5, 2014, 12:23 PM), http://www.techrepublic.com/article/googles-end-to-end-gmail-encryption-an-excellent-development-for-the-enterprise/ [http://perma.cc/57MN-DVS9].

252. *Id.* ("PGP [Pretty Good Privacy encryption] email is notoriously not usable .... It's very, very secure but, like a lot of things that are very, very secure, it's real easy to make mistakes.").

253. *See* Patrick Lambert, *Email Encryption: Using PGP and S/MIME*, TECHREPUBLIC (July 11, 2013, 11:00 PM), http://www.techrepublic.com/blog/it-security/email-encryption-using-pgp-and-s-mime/ [http://perma.cc/F4MK-9Y3M].

requirement, both positive and negative outcomes will occur in terms of effective law enforcement.

Those negative outcomes in which the criminal gets away with his crime, however, may occur more often when there is no warrant requirement. Without the warrant requirement, criminals will not have any expectation of warrant protection, and using e-mail encryption will be sensible in many more cases. This will negatively impact the capacity of law enforcement to catch criminals. Contrary to popular belief, although the NSA can break most encryption programs,[254] it is practically impossible for regular police to break encryption programs.[255] To understand why, it is necessary to briefly explain how encryption works.

Encryption is generally achieved by multiplying two extremely large prime numbers (the factors), to create an even larger number (the product).[256] The factors are the keys to the product, which is the lock; because both factors are prime numbers, there is only one solution to open the lock.[257] The larger the factors used, the harder it is to decrypt them; if the resulting product is large enough, it does not matter if it is publicly available as long as the factors remain hidden.[258] This is because it takes considerably less time and computing power to generate the product—to encrypt—than to reverse-engineer the factors—to decrypt.[259] Even confirming that an extremely large number is prime takes the world's most powerful computers a long time. For instance, the largest prime number yet found has over seventeen million digits and took thirty-nine days of continuous computing calculation to initially verify.[260]

---

254. *See* Adam Clark Estes, *The NSA Can Beat Almost Any Type of Encryption*, GIZMODO (Sept. 5, 2013, 3:39 PM), http://gizmodo.com/the-nsa-can-crack-almost-any-type-of-encryption-1258954266 [http://perma.cc/V22X-XRT4].

255. *See, e.g.*, Zeljka Zorz, *Police Unable to Decrypt iPhones, Asks Apple to Do It*, HELP NET SECURITY (May 13, 2013), http://www.net-security.org/secworld.php?id=14899 [http://perma.cc/L3WK-XTVQ].

256. *See* Casey Johnston, *Ask Ars: Why Spend Time and Money Finding New Prime Numbers?*, ARS TECHNICA (Feb. 14, 2013, 8:30 AM), http://arstechnica.com/science/2013/02/ask-ars-why-spend-time-and-money-finding-new-prime-numbers/ [http://perma.cc/JT7T-4NAV].

257. *See id.*

258. *See id.*

259. *See id.*

260. *See* Casey Johnston, *Volunteer Discovers a New 17 Million-Digit Prime Number*, ARS TECHNICA (Feb. 5, 2013, 5:10 PM), http://arstechnica.com/science/2013/02/volunteer-discovers-

Nevertheless, encryption codes can be cracked—it just takes considerable computing power. "Brute force decryption" can reverse-engineer the factors by simply dividing the product by every lower number until the solution is found; but the strength of the key is a product of the number of digital bits it uses.[261] Whereas previously, a 40-bit key was the gold standard, that could now be "cracked in moments by a standard desktop computer. These days, 256 bits or more (which theoretically should take thousands of years to crack) is common."[262]

The quote above illustrates two important elements at work here. First, decryption is not a practical option for the average police investigation. With enough computing power, encryptions can be cracked in less than 1000 years, but that would cost millions of dollars in computing technology.[263] Brute force decryption will realistically only be available to high-end agencies like the NSA for responding to highly salient threats, such as a potential terrorist attack. Consequently, encryption will protect lower-grade criminals far more effectively than the warrant requirement.[264] As such, if courts are concerned with police efficiency, in such instances they would be better off retaining the warrant requirement, in order to avoid making such effective criminal innovations worthwhile.

That does not mean that innovation in the form of encryption is always a dominant strategy. The speed with which old encryption programs can now be cracked illustrates the second important element: the development of encryption and decryption technology, like most criminal innovation and law-enforcement counter-response, is a back-and-forth of innovation and counter-innovation.[265] For instance, acoustic cryptanalysts have recently discovered that encryption keys can be ascertained by simply listening to a computer

---

a-new-17-million-digit-prime-number/ [http://perma.cc/4YKS-UJKG].

261. *See* Charles Arthur, *How Internet Encryption Works*, GUARDIAN (Sept. 5, 2013, 3:19 PM), http://www.theguardian.com/technology/2013/sep/05/how-internet-encryption-works [http://perma.cc/RBA6-SCL5].

262. *Id.*

263. *See* Estes, *supra* note 254.

264. *See* Timothy B. Lee, *NSA-Proof Encryption Exists. Why Doesn't Anyone Use It?*, WASH. POST WONKBLOG (June 14, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/14/nsa-proof-encryption-exists-why-doesnt-anyone-use-it/ [http://perma.cc/K8SS-JT6U].

265. Encryption also may not be the dominant strategy for a less complicated reason: if the police gain access to the key, then "the user's email becomes about as secure as a house with the keys left on the doorstep." Lindenberg & Stöcker, *supra* note 241.

decrypt an encryption program.[266] Cryptanalysts were able to extract even 4096-bit keys from a laptop in less than an hour.[267] But cryptanalysts soon discovered that this innovation, in turn, could be undermined by various noise-creation mechanisms.[268] Clearly then, as with so many criminal innovations and law-enforcement counter-responses, the success of the cryptanalysts in breaking down, and then building up, the effectiveness of encryption programs in such a short space of time "merely starts an arms race between the blinders and the spies."[269]

Consequently, the cost-benefit equation of investing in this type of technology is constantly changing, as is the relative power between criminals and investigators. This uncertainty in technological parity perpetuates the uncertainty for criminals as to whether LEOs will be able to effectively investigate,[270] as well as the corresponding uncertainty of LEOs as to whether criminals will innovate with new techniques. Consequently, we will regularly find ourselves in the scenario of probabilistic strategies being played. Our model showed that in this common scenario, perverse incentives arise: law enforcement will not be better off without the warrant requirement, and the general public will have a significant loss of privacy for no real gain in law enforcement.

This criminal innovation-police counterresponse was starkly illustrated after Google's announcements that it was enabling full encryption of cell phones.[271] The director of the FBI, James B. Comey, warned that such encryption technologies would stymie law enforcement investigations, as criminals inevitably make use of the technology. As such, the government may legislate and regulate—in

266. *See Unsafe and Sound: Ciphers Can Now Be Broken by Listening to the Computers That Use Them*, ECONOMIST (Jan. 18, 2014), *available at* http://perma.cc/Q5SF-M3ZW [hereinafter *Unsafe and Sound*] ("Acoustic cryptanalysis works by listening to a computer's sonic signature—the noise its capacitors and coils make as they vibrate in response to the amount of power being drawn by its processor.").

267. *See id.* Similarly, "hackers have begun to use the power of modern graphics processing units ... to crack passwords." Arthur, *supra* note 261. This is possible because graphics processing units are designed to do one thing very quickly, unlike computers, which are designed to do many things relatively slowly.

268. *See Unsafe and Sound*, *supra* note 266.

269. *See id.*

270. *See* Zorz, *supra* note 255.

271. David E. Sanger & Brian X. Chen, *Signaling Post-Snowden Era, New iPhone Locks Out N.S.A.*, N.Y. TIMES, Sept. 27, 2014, at A1.

laws akin to the Communications Assistance for Law Enforcement Act of 1994, which forces telecommunications companies to build wiretap capacity into their systems—to enforce encryption bypass mechanisms, to unlock e-mail and other documents. However, commentators worry that such bypasses would also be available to hackers and foreign governments[272]—the fear is that in seeking to promote police efficiency, the state may lower not only privacy but national security.

Even greater problems arise with stronger forms of encryption, such as masking the user's identity and location by rerouting each person's Internet activities through a system such as Tor.[273] The advantage of Tor is that it is, at least currently, almost unbreakable, even by the NSA.[274] Although Tor is suitable for individual criminal activity, such as visiting the Silk Road to purchase narcotics, much like e-mail encryption, Tor is not a feasible alternative for daily use by ordinary users because by encrypting all Internet activity, Tor massively slows down the processing power of the entire machine.[275] As such, all forms of encryption seem to exacerbate, rather than solve, the problem raised by our model that innovation will offer little help to innocent users conducting ordinary electronic activity.

---

272. David E. Sanger & Matt Apuzzo, *F.B.I. Director Hints at Action as Google and Apple Lock Up Cellphone Data*, N.Y. TIMES, Oct. 17, 2014, at A19.

273. Tor prevents Internet surveillance done through "traffic analysis"—inferring who is talking to whom over a public network by the source and destination of Internet traffic—by distributing each Internet communication over several randomly selected relays. *See Tor: Overview*, TOR, https://www.torproject.org/about/overview [http://perma.cc/MMT5-FB6E] (last visited Feb. 22, 2015). Other mechanisms include "full disk encryption," which encrypts the contents of an entire hard drive, making it impossible for investigators to access the contents. *See* Eoghan Casey et al., *The Growing Impact of Full Disk Encryption on Digital Forensics*, 8 DIGITAL INVESTIGATION 129, 129 (2011). Another option is PGP, "Pretty Good Privacy," which is inconvenient because it requires the sharing of private keys, but which would hide data from even the NSA's spying techniques. *See* Lee, *supra* note 264. In a new twist on an old technology, the Zetas Mexican drug cartel has been using an encrypted radio network since 2006. *See* Spencer Ackerman, *Radio Zeta: How Mexico's Drug Cartels Stay Networked*, WIRED (Dec. 27, 2011, 3:41 PM), http://www.wired.com/2011/12/cartel-radio-mexico/ [http://perma.cc/VB75-3YAB].

274. *See* Grant Gross, *Report: NSA Has Little Success Cracking Tor*, COMPUTERWORLD (Oct. 4, 2013, 5:52 PM), http://www.computerworld.com/s/article/9242992/Report_NSA_has_little_success_cracking_Tor [http://perma.cc/QNH7-EL8H].

275. *See* Patrick Lambert, *Everything You Need to Know About Using TOR*, TECHREPUBLIC (June 28, 2013, 4:00 AM), http://www.techrepublic.com/blog/it-security/everything-you-need-to-know-about-using-tor/ [http://perma.cc/KM9C-N57B].

Encryption will only offer real benefit to criminals with more at stake in avoiding law-enforcement sanctions.

2. Data Destruction Programs

Encryption has been around in various forms for millennia,[276] so it is not surprising that it is the most commonly promoted response to e-mail violability.[277] Although there are significant moral hazards impeding the ISP market from meeting the demand for increased e-mail privacy protection, the broader online market has responded to demand for private communication in other ways. One response has been to design new technology that promotes privacy by the fleeting nature of its mode of communication—by destroying any record of communication, it becomes more difficult, though not impossible, for a third party to access the information.

One such program is Privnote, which offers the modern realization of the self-destruct message imagined in futuristic spy dramas, such as Mission Impossible. It passes encrypted messages between two individuals; the messages are sent as single-use URLs that expire after the first time they are accessed in any web browser.[278] The message creator crafts a note and sends the URL to the recipient, who clicks on the URL and reads the information and then the message is automatically destroyed. This system offers both practical and legal mechanisms of ensuring privacy as against state interception.

Practically, the system provides security against surveillance by destroying the message once it is read. Not even the sender or initial recipient can ever view the note again, because the link will no longer exist.[279] Of course that does not entirely replicate the scenario in which the message never existed. For example, the recipient could take a screenshot of the message before it is destroyed. However, trust in the recipient is unavoidable in almost any communication

276. *See The History of Encryption*, VISUAL.LY (May 3, 2012), http://visual.ly/history-encryption [http://perma.cc/3YKV-M4Y6].

277. *See* Lambert, *supra* note 253.

278. *See Privacy Policy*, PRIVNOTE, https://privnote.com/privacy/ [http://perma.cc/9P84-6JYG] (last visited Feb. 22, 2015).

279. *See FAQ*, PRIVNOTE, https://privnote.com/faq/ [http://perma.cc/4KZJ-5XXL] (last visited Feb. 22, 2015).

mechanism—as the Supreme Court has recognized[280]—particularly recorded messages.[281] In addition, though, the message could be intercepted and read by someone other than the intended recipient, such as by the government. Because the message takes the form of a URL, if a third party obtained knowledge of where to look, that third party could potentially read the message before the intended recipient.[282] In this scenario, although Privnote cannot prevent interception, the system enables the sender to detect it. Because the message is destroyed after being opened, only one person can view it. Although the sender cannot tell if it was the intended recipient who read the message, the sender can inferentially determine that fact by the recipient's subsequent inability to access the message. The act of interception destroys the message, leaving only a dog that cannot bark. Thus, Privnote seems well designed for both avoiding and detecting government eavesdropping.

Legally, Privnote also may offer the benefit of avoiding the application of the third-party doctrine. Unlike e-mail ISPs, the Privnote platform does not hold the content of the messages sent on its server in any readable format at any time.[283] The decryption key for each message is bound to the content through the link and the link is never sent to Privnote, but rather is generated in the user's browser.[284] However, the messages themselves are stored on the Privnote servers prior to being read.[285] It is questionable whether it is possible for anyone with access to the Privnote database, such as an employee, to access the content of the messages—even those with access to the database do not have the keys to decrypt individual

280. United States v. White, 401 U.S. 745, 752 (1971) ("Inescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police.").

281. There are reports of nude Snapchat photos being screenshot and then forwarded as a form of pornography. *See* Alexis Kleinman, *Snapchat Nudes Are Being Screenshot and Secretly Posted on Facebook*, HUFFINGTON POST (May 29, 2013, 3:08 PM), http://www.huffingtonpost.com/2013/05/28/snapchat-nudes_n_3348145.html [http://perma.cc/8DNM-J7QB].

282. *See Privacy Policy*, *supra* note 278 ("Depending on the communication channel of your choice (e.g., email, fax, SMS, phone, instant messaging), there may be a certain risk that third parties intercept your communication, get knowledge of the communicated URL and thus may be able to read your message.").

283. *Id.*

284. *See* FAQ, *supra* note 279.

285. *Id.*

messages.[286] Also, although it is possible that Privnote could insert code to intercept the content of the notes, the website and its creator swear they will not do so.[287] Even though these three caveats provide qualifications on the actual capacity for privacy invasion,[288] they do not adversely impact the legal privacy created by the design of the Privnote system—as long as those running the company can plausibly swear that they will have no access to the content of the messages, then Privnote users have not "knowingly shared" the content of their communications with the company that runs the service and the third-party doctrine will not kick in.[289]

Thus e-mail encryption may be clunky and impractical for the average noncriminal user aiming to protect his privacy, but more recent innovations may offer greater protection to innocents and wrongdoers alike from state scrutiny. But these advantages are highly fragile, subject to the ever-changing balance of power in the innovation-response game. That fragility is illustrated by the experiences of a company offering a similar service to Privnote: Snapchat.

Snapchat is a platform for sharing photos and videos, but that sharing only lasts between one and ten seconds after viewing, according to the sender's preference.[290] The program was designed to create a social networking site that provides greater privacy by making content temporary,[291] but there are a number of elements that make Snapchat less protective of privacy than Privnote.[292]

---

286. *See* Pablo Hoffman, *How Privnote Really Works*, PABLO HOFFMAN (July 6, 2008, 2:51 PM), http://pablohoffman.com/how-privnote-really-works [http://perma.cc/HX2K-F8D3].

287. *See id.*

288. In addition, some commentators have questioned Privnote's claim of *inability* to access the content of the messages, arguing that nothing is stopping the developers from "executing additional code to intercept notes before they're encrypted.... [A]s long as they continue to claim that they can't possibly read the contents of the notes being passed through their system, they're lying." Ryan Grove, *Privnote's Developers Are Confused*, WONKO.COM (July 6, 2008, 7:11 PM), http://wonko.com/post/privnotes-developers-are-either-stupid-or-malicious [http://perma.cc/UHC8-ZCDG].

289. In addition, because Privnote does not log IP addresses, see FAQ, *supra* note 279, it cannot deduce the identity of any sender, and thus it may be harder for agencies, such as the NSA, to obtain a subpoena for user-identification records.

290. Larry Magid, *What Is Snapchat and Why Do Kids Love It and Parents Fear It* (*Updated*), FORBES (May 1, 2013, 4:14 PM), http://www.forbes.com/sites/larrymagid/2013/05/01what-is-snapchat-and-why-do-kids-love-it-and-parents-fear-it/ [http://perma.cc/UR7J-F3Z8].

291. *Id.*

292. Other websites, even those primarily used for anonymous sexual hookups, such as

Unlike Privnote, Snapchat delivers messages to individuals on a sender's friends list;[293] thus, the platform has user and communication identification capability. Although Snapchat claims to automatically delete all photos from its servers such that they can no longer be retrieved by anyone for any reason,[294] forensic analysts have actually determined that photos can be "undeleted."[295] In addition, the messages are saved on Snapchat's servers for up to thirty days (if unopened),[296] meaning that users have actually relayed the content of the messages to the company. Moreover, Snapchat introduced a feature that allows a once-a-day exception for certain recipients, granting them limited playback for up to twenty-four hours. Finally, perhaps as a result of Snapchat's popularity,[297] the app Snaphack has been developed that lets people look at old snapchats; it is expected that there will soon be a version that will allow forwarding to third parties.[298] These are exactly the sort of capabilities that justified the third-party doctrine in the first

---

Grindr, which are likely also being used for prostitution, nonetheless offer even less protection: Grindr keeps significant amounts of information about its users and shares it with third parties. It even retains the instant messages sent through the app, including (often explicit) pictures, location, and audio/video. *Grindr Terms of Service*, GRINDR, http://grindr.com/terms-of-service [http://perma.cc/LTF2-LRE5] (last visited Feb. 2, 2015).

293. *See How to Find and Add Friends*, SNAPCHAT, https://support.snapchat.com/a/find-friends [http://perma.cc/84F5-33KR] (last visited Feb. 2, 2015).

294. *How Snaps Are Stored and Deleted*, SNAPCHAT (May 9, 2013, 7:23 PM), http://blog.snapchat.com/post/50060403002/how-snaps-are-stored-and-deleted [http://perma.cc/FX2K-MKDQ].

295. Kashmir Hill, *Snapchats Don't Disappear: Forensics Firm Has Pulled Dozens of Supposedly-Deleted Photos from Android Phones*, FORBES (May 9, 2013, 4:51 PM), http://www.forbes.com/sites/kashmirhill/2013/05/09/snapchats-dont-disappear/ [http://perma.cc/DJ9V-E9BQ] ("[I]t's possible to pull Snapchat photos from Android phones simply by downloading data from the phone using forensics software and removing a '.NoMedia' file extension that was keeping the photos from being viewed on the device.").

296. *How Snaps Are Stored and Deleted*, *supra* note 294.

297. Jordan Crook, *Snapchat Sees More Daily Photos Than Facebook*, TECHCRUNCH (Nov. 19, 2013), http://techcrunch.com/2013/11/19/snapchat-reportedly-sees-more-daily-photos-than-facebook/ [http://perma.cc/79TQ-KFW9].

298. Ellie Zolfagharifard, *Beware What You Snapchat: App Lets You Save and Re-Open Pictures You Have Received Without the Sender Ever Knowing*, DAILY MAIL (Oct. 14, 2013, 10:26 AM), http://www.dailymail.co.uk/sciencetech/article-2458852/Snapchat-SnapHack-App-lets-save-open-pictures-received.html [http://perma.cc/46F9-PZF5].

place;[299] thus, Privnote's legal advantage is unlikely to apply to Snapchat.[300]

The irony of an outcome in which Privnote messages receive greater constitutional protection than Snapchat photographs is that wrongdoers seem much more likely to use Privnote than Snapchat. Snapchat involves people (mostly teens) who know each other well enough to be "friend" contacts and pass messages back and forth—a mechanism no doubt regularly used for online sexting but also plausibly used for everyday conversation among a generation used to chatting online.[301] Privnote, on the other hand, is designed to maximize untraceability, enabling the sending of illicit messages. Once again, this platform could be attractive for sexual interactions and other noncriminal private communications, but it is inherently well-suited to masking criminality,[302] and far less convenient for back-and-forth conversation.

Unlike e-mail encryption, which is only likely to be attractive to serious criminals because of the high convenience costs, programs such as Privnote and Snapchat are seemingly innately suited to small-time criminality. They offer considerable privacy, but primarily by keeping crime under the radar; the main way Privnote and Snapchat protect criminality is through masking it, which will be effective as long as LEOs do not know where to look. But these programs offer less protection for more serious crimes, which are subject to more thorough investigation, because the government can request access to them: Snapchat has received warrants requesting

299. The logic of the third-party doctrine is that if an individual reveals information to a third party, betrayal is a known risk, and thus it is no different from giving the police access to the communication itself. United States v. White, 401 U.S. 745, 752 (1971). If Snapchats are continually accessible, the sender has no guarantee that the recipient of a message will not reveal its contents to the police.

300. Seemingly in recognition of the dangers encapsulated by the third-party doctrine, Snapchat warns its users that although it will attempt to ascertain if anybody takes a screenshot of their snap, they should not use the program if they are worried about the recipient keeping a copy of messages. *Privacy Policy*, SNAPCHAT, https://www.snapchat.com/privacy [http://perma.cc/4RVM-XT9P] (last updated Nov. 17, 2014).

301. Magid, *supra* note 290.

302. However, there are legitimate uses for Privnote that require strong privacy protection, such as "web forums for rape and abuse survivors, or people with illnesses," as well as journalists and NGOs communicating with whistleblowers and dissidents. *See Tor: Overview*, *supra* note 273.

unopened images.[303] These programs will be inadequate for serious criminals, but they will be quite effective at protecting criminals from the type of scrutiny that would allow LEOs to know where to look. LEOs may be as well off if they had to develop probable cause and obtain a warrant before searching a criminal's e-mail versus if they had no warrant requirement but, as a result of even petty criminals turning to this kind of innovation, had to figure out which platform a criminal was using and try to find the incriminating messages before they were destroyed.

Without a warrant requirement, the end result may be that programs like Snapchat, most likely to be used by noncriminals, will receive little protection; Privnote and programs of its ilk that are inherently amenable to small-time criminality will offer significant protection, but be permeable; and serious criminals will use more complex innovations, such as Tor or e-mail encryption, which will be far more costly, but extremely hard to crack. The heightened fear of investigation due to the lack of warrant requirement will, as our model predicted, undermine the privacy interests of innocents, but the main effect on criminals will be to encourage use of electronic innovations, which may make criminal investigations as hard as the warrant requirement would.

3. Switching Costs and the New Context: Mass NSA Searches

We have shown that whether innovations like encryption or self-destruct messaging are feasible depends largely upon various practicalities, such as convenience, cost, and degree of privacy needs. For serious criminals, the heightened need to avoid detection may outweigh even the high costs of encryption, whereas innocent users are more likely to utilize the lower-privacy protection offered by programs such as Snapchat. There will always be a cost-benefit equation in the innovation-response relationship, but that calculation will depend on whether switching costs are adequately low.

For instance, if law enforcement profiles individuals who wear black-and-white scarves because they are associated with approval

303. Amanda Holpuch, *Snapchat Admits to Handing Unopened "Snaps" to US Law Enforcement*, GUARDIAN (Oct. 15, 2013, 3:35 PM), http://www.theguardian.com/world/ 2013/ oct/ 15/snapchat-hands-snaps-pictures-to-federal-law-enforcement [http://perma.cc/K2SD-7LG3].

of terrorist methods,[304] then these searches can easily be avoided by switching apparel, perhaps with free speech costs. If the government targets red cars for additional scrutiny because they believe these cars are more dangerous,[305] drivers can avoid such additional scrutiny only to the extent that they can absorb the transaction costs of switching or painting their cars. And if LEOs profile based on an immutable characteristic such as race, then switching is impossible.

The cost-benefit equation in the Fourth Amendment context is made more complex than in other contexts by the circularity of *Katz*'s logic. The difficulty of *Katz* is that its identification of an investigation as a search is based on subjective individual and objective social expectations of privacy; but those expectations themselves depend on how often and how extensively such investigations take place. If the public knows that the government can and does access its e-mail, its expectation of privacy in e-mail is reduced, and the likelihood of that investigation being a search is reduced. The lower the switching costs, the more self-reinforcing government targeting will be.

Thus *Katz* encourages criminal innovation; but the possibilities for innovation are not always unlimited. This Article has shown that the cost-benefit equation will often be perversely related to criminality. Consequently, it will often be worthwhile for criminals to innovate, but, without the payoff of crime, the switching costs will be too high for innocents, who will be left to bear the costs of additional searches. This is illustrated by the changed context of the mass NSA spying regime.

Pursuant to an order issued by the Foreign Intelligence Surveillance Court (FISC),[306] the NSA has been capturing, siphoning,

304. Wearing the keffiya, a black-and-white checked scarf, is an expression of solidarity with the Palestinian Liberation Organization. Sonja Sharp, *Your Intifada: Now Made in China!*, MOTHER JONES (June 22, 2009, 3:34 PM), http://www.motherjones.com/riff/2009/06/your-intifada-made-china [http://perma.cc/RC5F-JGVU].

305. Some cars are more likely to get pulled over than others, though it may be that people who have these cars are worse drivers. Hannah Elliott, *Cars Most Likely to Get a Ticket*, FORBES (Oct. 13, 2010, 5:30 PM), http://www.forbes.com/2010/10/13/cars-that-get-ticketed-most-police-speeding-lifestyle-vehicles-violations.html [http://perma.cc/N8E2-2AS2].

306. Spencer Ackerman, *FISA Court Order That Allowed NSA Surveillance Is Revealed for First Time*, GUARDIAN (Nov. 19, 2013, 10:09 AM), http://www.theguardian.com/world/ 2013/nov/19/court-order-that-allowed-nsa-surveillance-is-revealed-for-first-time [http://perma.cc/N39W-TLT8].

storing, and cross-referencing vast swathes of personal data, including collecting the call-detail records of all customers of the major telecommunications companies, data mining billions of e-mails each day, and analyzing them for patterns and connections.[307] This metadata includes all "non-content" information of phone calls, including the numbers dialed, duration of calls, and the location information of cell phones.[308] The FISC order allows the NSA to search the database for information; no warrant is necessary—only "reasonable suspicion" that the search will reveal information relating to a terrorist plot. The NSA asserts that it does not even need FISC approval, and thus presumably can bypass even reasonable suspicion.[309] As discussed, this is arguably legal under existing Fourth Amendment doctrine, as the third-party doctrine allows for the warrantless collection of metadata released to third parties, such as a telephone company.[310] The core of the controversy of the NSA searches is that they alter the basic principle that the Fourth Amendment limits law-enforcement investigation methods by requiring specificity and reliability of law-enforcement knowledge of alleged criminal conduct. This has three main repercussions.

First, switching behavior to avoid NSA surveillance is extremely difficult, both because of the breadth of the spying program and its lack of association between criminality and scrutiny. The fact that the program covers most telephone conversations and e-mail communications makes switching to alternative means of communication dependent on some form of technology—such as those described

307. *See, e.g.*, *How the NSA's Domestic Spying Program Works*, ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/nsa-spying/how-it-works [http://perma.cc/4AY9-9S7N] (last visited Feb. 22, 2015).

308. Orin Kerr, *Metadata, the NSA, and the Fourth Amendment: A Constitutional Analysis of Collecting and Querying Call Records Databases*, VOLOKH CONSPIRACY (July 17, 2013, 3:54 AM), http://www.volokh.com/2013/07/17/metadata-the-nsa-and-the-fourth-amendment-a-constitutional-analysis-of-collecting-and-querying-call-records-databases/ [http://perma.cc/82UJ-32P6].

309. Under the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1861 (2012), the NSA is supposed to convince the Foreign Intelligence Surveillance Court that it has reasonable suspicion that any query of the data will reveal information relating to activities such as terrorist plots, but the NSA interpreted this as authorizing it to spy on domestic phone calls and e-mails without a FISC approval or a warrant. NAT'L SEC. AGENCY, OFFICE OF THE INSPECTOR GEN., ST-09-0002 WORKING DRAFT 8 (2009), *available at* http://perma.cc/RR7T-BRZV.

310. *See supra* Part I.A.

in the previous two Sections—even the most accessible of which may be cost-prohibitive to the less technologically savvy. We might anticipate demand for further innovations that would interfere with the ability of the NSA to ascertain who is being called, for example by rerouting calls through an intermediary as Tor does with Internet communication, or by rerouting telephone calls over Wi-Fi and other channels to avoid any creation of a call log.[311] These technological fixes are currently only theoretical. Even if they eventuate, it will create an increasingly high pressure to innovate, not only by criminals but also by ordinary citizens.[312]

Second, the constitutionality of the NSA searches hinges on the same considerations described above in relation to privacy in e-mail and other forms of communication: the application of the third-party doctrine. Thus far, two district courts have ruled on preliminary injunction motions challenging the constitutionality of the spying program, and have come to opposite conclusions.[313] In the United States District Court for the District of Columbia, Judge Leon held that the NSA's bulk collection of telephone metadata is likely unconstitutional.[314] Judge Leon distinguished *Smith v. Maryland* by stating that it was no longer applicable to modern-day circumstances in which people use their telephones for much more than making calls and the government has developed exceedingly efficient techniques for storing and analyzing the metadata of millions of people.[315] The opinion struck many as incorrect: the added capabilities of cellular phones arguably should not matter because the metadata being collected by the NSA is the same that was collected thirty-four years ago in *Smith*. Moreover, the Supreme Court has repeatedly said that achieving an outcome that was previously judicially approved in a more efficient manner does not render a

311. David Goldman, *Apps Claim They Can Keep Phone Records Secure*, CNN (June 6, 2013, 1:19 PM), http://money.cnn.com/2013/06/06/technology/security/verizon-call-logs/ [http://perma.cc/D7V4-397Z].

312. As the head of security at Google described, "At first we were in an arms race with sophisticated criminals .... Now we're in an arms race with the best nation-state actors." Steven Levy, *How the U.S. Almost Killed the Internet—and Why It Still Could*, WIRED, Feb. 2014, at 62, 66.

313. ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013); Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013).

314. *Klayman*, 957 F. Supp. 2d at 9.

315. *Id.* at 31-37.

state action unconstitutional.[316] In contrast, Judge Pauley of the Southern District of New York held that the program was constitutional under the controlling precedent of *Smith*.[317] Thus, the unconstitutionality of the NSA searches hinges on the willingness of the Supreme Court to overturn or massively limit *Smith v. Maryland*. But if the Court is not willing to do that, then e-mail communications and their brethren are not protected from any state scrutiny; they will not just be subject to the relatively nonintrusive scanning of metadata, but to individualized content analysis.

Third, and more generally, the fundamental objection that the NSA program undermines the connection between established criminality and level of scrutiny is not unique to that program; it is true of all law-enforcement investigations that are categorized as nonsearches. Although the NSA mass searches garner significant headlines, the same effect is achieved by avoiding the warrant requirement for ordinary police investigations. In fact, at least theoretically, NSA searches are subject to the restraint of reasonable suspicion, whereas if a law-enforcement investigation is categorized as a nonsearch, Fourth Amendment protections do not apply at all. The NSA controversy is just a high-profile example of what the law enforcement has long been able to do in investigations not categorized as searches.

CONCLUSION

Throughout Fourth Amendment law, courts assume that requiring law enforcement to obtain a warrant for an investigation will greatly harm LEOs' ability to solve crime and prosecute criminals. This assumption appears in debates about the search/nonsearch distinction, about possible exceptions to the warrant requirement, and about the warrant requirement itself. Yet it is often not true.

In some situations, LEOs will indeed be better able to investigate crime when they do not have to incur the costs of obtaining a warrant. However, when criminals are able to innovate in ways that reduce the likelihood of law-enforcement detection, requiring LEOs

316. *See* Orin Kerr, *Preliminary Thoughts on Judge Leon's Opinion*, VOLOKH CONSPIRACY (Dec. 16, 2013, 6:54 PM), http://www.volokh.com/2013/12/16/preliminary-thoughts-judge-leons-opinion/ [http://perma.cc/8K6V-7ED9].

317. *Clapper*, 959 F. Supp. 2d at 752.

to obtain a warrant will do little or no harm to law-enforcement investigations in many cases. Reduced costs of law-enforcement investigation will incentivize criminals to innovate more often. This increased innovation will often completely offset the gains LEOs receive from not having to obtain a warrant.

Other than differences in constitutional interpretation,[318] the main argument in favor of doing away with the warrant requirement is that obtaining a warrant makes police work much more difficult.[319] Yet when criminal innovation is taken into account, it is clear that this argument is greatly oversold. For too long, Fourth Amendment jurisprudence has overlooked the fact that criminals will work harder to hide their crimes if LEOs do not have to work as hard to investigate them. Law enforcement has long recognized the need to anticipate and respond to potential criminal innovation, and investigation strategies are commonly structured around the expectation that criminals will innovate. It is time the courts recognize this interaction.

When criminal innovation is taken into account, many of the assumptions of Fourth Amendment law become less clear, and many of the strange doctrinal innovations that the Court has made to account for police efficiency look foolhardy. This Article has shown that, contrary to common beliefs, law enforcement will often realize no gain when an investigation is classified as a nonsearch or is otherwise exempt from the warrant requirement. These outcomes will only occur more often as use of electronic technology increases. Courts deciding Fourth Amendment questions must begin to take into account the incentives that cause criminals to innovate, and give less weight to the claim of police efficiency when deciding whether the warrant requirement applies.

318. Amar, *supra* note 53, at 804-05.

319. *See, e.g.*, Robbins v. California, 453 U.S. 420, 438 (1981) (Rehnquist, J., dissenting).