Criminal Innovation and the Warrant Requirement: Reconsidering the Rights-Police Efficiency Trade-off

Tonja Jacobi, Northwestern University
Jonah Kind, Northwestern University

Available at: https://works.bepress.com/tonja_jacobi/8/
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 police 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 police resources to develop countermeasures, police 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 police 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 non-criminal privacy concerns may be better promoted by maintaining the warrant requirement.

Introduction ......................................................... 2
I. The Role of the Fourth Amendment in Police Investigations ................................................. 7
   A. The Warrant Requirement, and the Manipulation of Definitions of a Search ......................... 7
   B. The Distorting Effect of the Assumption that Warrants Impede Investigations ................. 12
II. Criminal Innovation ................................................ .......................................................... 16
   A. Existing Scholarship on Criminal Innovation ................................................................. 16
   B. Criminal Innovation and the Police Efficiency Assumption ......................................... 19
III. An Economic Model of Criminal Innovation and the Warrant Requirement .................... 20
   A. Criminal Utility ................................................................................................................. 21
   B. Police Activity .................................................................................................................. 23
   C. Game Theoretic Solutions ............................................................................................... 25
   D. When is the Assumption Violated? .................................................................................. 28
IV. Discussion and Policy Implications ....................................................................................... 31
   A. General Implications ......................................................................................................... 31
   B. Application to Private Communication in the Digital Age ............................................... 34

* Professor of Law, Northwestern University School of Law. t-jacobi@law.northwestern.edu.
# JD Candidate, Northwestern University School of Law. j-kind2014@nlaw.northwestern.edu.
<table>
<thead>
<tr>
<th>1. Email and Encryption</th>
<th>34</th>
</tr>
</thead>
<tbody>
<tr>
<td>2. Data Destruction Programs</td>
<td>39</td>
</tr>
<tr>
<td>3. Switching Costs and the New Context: Mass NSA Searches</td>
<td>42</td>
</tr>
</tbody>
</table>

V. Conclusion .................................................................................................................................................. 45

Introduction

“Little” Melvin Williams was an infamous heroin and cocaine trafficking kingpin in Baltimore in the 1970s and early ‘80s.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 Supreme Court doctrine allows police, without a warrant, to monitor telephone numbers dialed on the public payphones the gang used to send messages to the pagers; the content of the messages was the telephone number that the recipient was supposed to call.⁴ So 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.

It made sense to invent a code for pager messages and to teach the code to every gang member because the gang knew the police could otherwise identify the pager numbers without the cost and evidentiary burden of acquiring a warrant.⁵ Police are more likely to undertake an investigative technique—such as tracking telephone calls—when they do not have to suffer the costs of obtaining a warrant, as it will be more likely that the expected benefits of the investigation (the possibility of finding evidence) will outweigh its costs (the time and effort expended in the action itself), plus the possibility of failing to gain a warrant. But when faced with a higher likelihood that police will investigate their crimes, criminals have a greater incentive to try to cover up the crime—to innovate. That criminal innovation, inspired by the lack of a warrant requirement, can potentially slow down an investigation as much as having to get a warrant. The Williams gang’s innovation made the police investigation much more difficult: the police created “clone” pagers, which shared the same telephone numbers as the

---

² Much of the first season of the HBO drama “The Wire” is based on this investigation. RAFAEL ALVAREZ, THE WIRE: TRUTH BE TOLD 46 (2004).
³ Id. at 47.
⁴ Smith v. Maryland, 442 U.S. 735 (1979) (allowing use of a pen register even on a home telephone).
⁵ 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 the public payphones. Given that Katz v. United States, 389 U.S. 347 (1967), had found that there was a reasonable expectation of privacy in a public telephone being used to make phone calls, a judge would be more reluctant to allow surveillance of a public phone, usable by anyone, than a private beeper used by a suspected criminal. Even if the police 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.
gang members’ pagers. The police were eventually able to crack the code, but the innovation significantly delayed the police investigation, and could easily have derailed it entirely.

Nowadays, instead of pager codes, it is common for criminal conspiracies to use prepaid cell phones for communication because those devices are harder for the police to trace or to tie to specific people. Prepaid phones are inexpensive, allowing criminals to dispose of them frequently to avoid being linked to the calls made; they are also more difficult to trace because purchasers can provide false names and addresses to phone providers. But pager codes and 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 would be familiar with many other mechanisms of classic crime detection avoidance: bank robbers use masks to prevent identification by witnesses, burglars use gloves to hide their fingerprints, and gunmen use silencers so that their crime does not attract attention.

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, and 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, has multiple mechanisms to avoid police 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. Only the unregulated electronic currency “Bitcoin” is accepted and sellers are required to delete all unique buyer information after confirmation of an item’s arrival. All of these mechanisms provide additional assurances of anonymity.

Criminal innovations, clearly, can take many forms, including new business methods, as well as traditional masking techniques. Whatever their form, innovations are costly in time and effort, yet they are undertaken because they significantly reduce the likelihood that criminal participants will be caught. This need is intensified if investigators can undertake warrantless investigations. For example, some of the Silk Road innovations are designed specifically to avoid warrantless police investigations. The police 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]...

---

6 A process that did itself require warrants.
7 Alvarez, supra note 2, at 47 (describing the process of breaking the beeper code).
8 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 cellphones).
10 Id.
11 Spapens, supra note 9, at 28-29.
12 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).
13 Emma Moore, Online Subterfuge: Silk Road, Tor and Bitcoin, BROWN POLITICAL REVIEW (Nov. 13, 2013, 11:00 AM), http://www.brownpoliticalreview.org/2013/11/online-subterfuge-silk-road-tor-and-bitcoins/.
15 Id.
visited and the total volume of information sent to or from [a suspect’s Internet] account."16 In addition, 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.17 The Silk Road’s built-in protections from such warrantless investigatory powers makes the job of investigators much more difficult—perhaps as difficult as it would be if the warrant requirement were applied to tracking IP addresses.18

From balaclavas to computer encryption, all of these criminal behaviors decrease, to a greater or lesser extent, the probability that the police 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 that a criminal can take following an arrest to avoid conviction, such as influencing witnesses or consulting experts.19

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 police can do little to counteract their effectiveness. For a criminal robbing a bank, wearing a mask is obviously an optimal choice, as this tool of innovation is easy to obtain, inexpensive, will make it much more difficult for witnesses to identify the robber, and there is little police can do to lift such a veil. More interesting are marginal innovations, which criminals will make only in some situations. For example, it only makes sense to use prepaid cellphones if the decreased likelihood of police 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 police counter-measures.20 It is obvious that criminals will want to innovate, but since innovation is often costly, the interesting question is: when will innovation be worthwhile?

We show that a major factor in that calculation is whether the warrant requirement applies to the police countermeasures. The Fourth Amendment generally requires the police to obtain a warrant before conducting a search,21 but the courts consider many types of police activity not to be searches for Fourth Amendment purposes, and so the police do not need to obtain warrants to

16 United States v. Forrester, 512 F.3d 500, 505 (9th Cir. 2007).
17 James Ball and Spencer Ackerman, NSA Loophole Allows Warrantless Search for U.S. Citizens’ E-mails and Phone Calls, THE GUARDIAN (Aug. 9, 2013, 12:08 PM).
18 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.COM (Nov. 18, 2013, 6:30 AM), http://www.wired.com/threatlevel/2013/11/silk-road/.
19 See Nussim & Tabbach, supra note 12, at 45.
21 See, e.g., Johnson v. United States 333 US 10, 14 (1948) (“When the right of privacy must reasonably yield to the right search is, as a rule, to be decided by a judicial officer, not by a policeman. . .”)
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 no warrant requirement applied. If the police can ping a cell phone or track it via GPS without going through the effort of obtaining a warrant, they will be more likely to so investigate, and an enterprising criminal will have greater incentive to innovate in order to prevent this type of investigation from being successful, for example by buying prepaid phones without GPS technology, altering the phones to prevent tracking through pinging, or turning to masked electronic communications. Police investigation of crime is a constant back-and-forth between criminal innovation and police counter-measures, response and counter-response.

We challenge the assumption that requiring the police to obtain a warrant prior to undertaking a particular action will always make it more difficult for the police to investigate and prosecute crime. Often, perhaps even usually, not needing a warrant will be better for the police, 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. However, because criminals can innovate, the assumption of greater police efficiency in the absence of the warrant requirement can be wrong.

When police do not need a warrant, they will be more likely, all other things being equal, to undertake an investigation because the costs of investigation are lower. However, this lowered cost of investigation will incentivize criminals to innovate more often, because innovations lower the likelihood of detection in the event of a police investigation. In many cases, the gains to the police 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 simply lead criminals to innovate more regularly, making police investigations less likely to succeed. The police will not increase their rate of investigation and will not capture more criminals.

One means by which the warrant requirement is avoided is by narrowing the range of police activities that are considered “searches,” and so entirely eliminating the application of the Fourth Amendment to those investigations. A Fourth Amendment search only occurs, and thus a warrant is only required, if it violates an individual’s “reasonable expectation of privacy.” The reasonable expectation of privacy test has been derided as circular, since an expectation of

22 In general, a police investigation is a search if it violates an individual’s “reasonable expectation of privacy.” Katz, 389 U.S. at 360 (Harlan, J., concurring); Smith v. Maryland, 442 U.S. 735, 746 (1979).
24 See 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)(discussing whether the warrant requirement applies to non-prepaid phones).
25 See infra, Part I.B.
26 This logic does not assume that criminals know when the police have or have not obtained a warrant, rather that criminals will know when the police 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.
27 Katz, 389 U.S. at 360 (Harlan, J., concurring).
28 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
privacy will depend on the extent to which police regularly breach that expectation; moreover, expectations of privacy will depend on legal decisions, which are supposed to be based on people’s expectations of privacy. 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 non-criminals, it was usually considered to at least have the beneficial effect of making it easier for the police to catch criminals. Our analysis, however, demonstrates that this advantage will often be illusory. Instead, increased surveillance may simply result in increased criminal innovation, such that the police will not have an easier time catching criminals. In the cat-and-mouse game between the police 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.

The dichotomy in the Fourth Amendment literature between police efficiency concerns and criminal right protections is therefore often a false one. We show that by removing the warrant requirement, police investigation can sometimes be easier, but often it will not be. In circumstances where there is significant uncertainty—by criminals as to whether police will investigate, and by police as to whether criminals will innovate—the police efficiency assumption is unsafe. Such uncertainty is likely to arise frequently; in such cases, removing the warrant requirement will not make police investigations more effective.

An extensive economic literature exists that analyzes the most efficient and effective mechanisms of deterring crime, by varying the extent of punishment, and other factors. But discouraging criminal behavior by changing incentives will in turn change the opportunity cost to police in choosing any given investigative priority. This in turn will change criminals’ expectations of being caught, and thus their incentive to innovate. The interactions between criminals and police must be considered dynamically, in terms of their feedback effects on one another. Unlike previous analysis, we account for this dynamic interaction, by employing a game theoretic model that allows us to simultaneously map the effect that criminal avoidance has on the police decision whether or not to investigate, and vice versa.

This Article describes the ‘Police Efficiency Assumption’—that police investigations are impeded when an investigation is considered a search and a warrant is required—and shows when that 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

---

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.”).


30 Richard A. Posner, The Uncertain Protection of Privacy by the Supreme Court, 1979 Sup. Ct. Rev. 173, 188 (“it is circular to say 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.”).

31 See e.g. A. Mitchell Polinsky & Daniel L. Rubinfeld A Model of Optimal Fines for Repeat Offenders, 46 J. Public Econ. 291 (1991) (showing that maximal deterrence may require variation in punishment levels by recidivism); Steven Shavell, A Model of Incapacitation, 77 Amer. Econ. Rev. 107 (1987) (same, factoring in the value of incapacitating likely re-offenders).
the existing literature on criminal innovation and discusses ways in which innovation can defeat the Assumption. Part III presents a game theoretic 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 email encryption and utilization of programs specifically made for destroying communication trails, such as Privnote\(^{32}\) and Snapchat.\(^{33}\) It finishes up with a discussion of the recent NSA mass data collection and analysis cases, showing that the non-application of the warrant requirement undermines Fourth Amendment rights more than that recent controversial governmental spying program. Part V concludes.

I. The Role of the Fourth Amendment in Police Investigations

The Fourth Amendment sets broad limits on federal and state police conduct during the investigation of crime,\(^{34}\) prohibiting “unreasonable searches and seizures,”\(^{35}\) and providing that “no Warrants shall issue, but upon probable cause. . . .”\(^{36}\) This seemingly straightforward language leaves many questions unanswered, including the definition of a “search,”\(^{37}\) and the relationship between the reasonableness clause and the warrant clause.\(^{38}\) 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 Amendment, it is unclear whether police are required to obtain a valid warrant in order to conduct a search.\(^{39}\) Read literally, the clause specifies only a limit on when warrants can issue—with probable cause—and presents a separate prohibition on unreasonable searches. 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 Amendment is relevant under this view only when the police wish to obtain a warrant prior to a search.\(^{40}\) Nonetheless, the Supreme Court has long considered warrantless searches to be presumptively unreasonable,\(^{41}\) and has also ordained that

\(^{32}\) See About Privnote, https://privnote.com/about/.

\(^{33}\) See http://www.snapchat.com/.


\(^{35}\) For simplicity of language, we refer to searches and seizures collectively as “searches” in this Article because the distinction is irrelevant to our analysis.

\(^{36}\) U.S. Const. amend. IV.


\(^{39}\) See, e.g., Grano, supra note 38, at 603; Bellin, supra note 38, at 8.

\(^{40}\) See, e.g., Akhil Reed Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 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.”).

\(^{41}\) 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 . . . .”) 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
reasonableness is ordinarily only satisfied through obtaining a warrant.\textsuperscript{42} Thus, the police are required to routinely obtain warrants prior to undertaking any search, unless the search falls into one of the well-delineated exceptions to the warrant requirement.

A requirement that police obtain a warrant for all searches raises the question of what constitutes a search under the Fourth Amendment. Many actions that police 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 police activity that, though considered not to be searches in the constitutional sense of triggering the protections of the Fourth Amendment, would be widely considered by laypeople to be a type of search.\textsuperscript{43} For instance, listening to a conversation via a wire worn by a confidential informant may be solid police work, but could easily be considered a search\textsuperscript{44}—contrary to Supreme Court doctrine.\textsuperscript{45} Similarly, having a professionally trained police narcotics detection dog sniff an airline passenger’s luggage\textsuperscript{46} or a person’s car trunk,\textsuperscript{47} in order to detect contraband secreted within, may be reasonable but it is nonetheless arguably a search,\textsuperscript{48} just as it would be if that dog was sniffing near the entrance of a house.\textsuperscript{49} Yet the Court has deemed that police-guided canine examinations are not searches at all in the first two situations, yet dog sniffs near the home are considered to be searches.

These distinctions are illustrations of a general doctrinal problem: many activities that would ordinarily be considered searches are deemed by the courts to not be such for Fourth Amendment purposes. The primary reason is that by refusing to acknowledge that a particular police investigation constitutes a search, the courts 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.\textsuperscript{50} The warrant requirement is typically assumed to


\textsuperscript{44} See United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (“More fundamentally, it may be necessary to reconsider the premise than an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.”).


\textsuperscript{46} United States v. Place, 462 U.S. 696, 707 (1983).

\textsuperscript{47} Illinois v. Caballes, 543 U.S. 405, 408 (2005).

\textsuperscript{48} See Jacobi, supra note 29, at 662 (criticizing the Court’s analysis in \textit{Place}).

\textsuperscript{49} Florida v. Jardines, 569 U.S. ___ (2013) (because it involves an intrusion upon the homeowner’s property).

\textsuperscript{50} See Jacobi, supra note 29, at 586.
so impede police efficiency that courts are often willing to judge whether an investigation constitutes a search, in order to avoid requiring a warrant.\(^{51}\)

In order to delineate between legal searches and commonsense searches, we use the term “investigations” as referring to any type of action taken by the police in order to obtain evidence. A subset of investigations includes “searches” under the Fourth Amendment, as well as “non-searches”—any police activity that is not considered to be a search under the Fourth Amendment, even if it may be considered a type of search by a layperson. Searches require a warrant in the absence of an exception to the warrant requirement, whereas police are not required to obtain a warrant for a non-search.

The Supreme Court’s primary test for distinguishing between searches and non-searches appears in *Katz v. United States*,\(^{52}\) the most influential expression of which comes from Justice Harlan’s concurrence.\(^{53}\) Under *Katz*, a police investigation is a search if it violates an individual’s “reasonable expectation of privacy,”\(^{54}\) 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.’”\(^{55}\) 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.\(^{56}\) Recently in *Jones*, the Supreme Court added to the *Katz* framework by specifying in addition that any physical trespass of a constitutionally protected area constitutes a search.\(^{57}\)

Both *Katz* and *Jones* expanded the definition of search—*Katz* by expanding a search beyond the physical penetration of constitutionally protected areas, and *Jones* by re-defining a physical penetration as sufficient, albeit not necessary after *Katz*, to constitute a search.\(^{58}\) Nevertheless, most doctrine pertaining to searches has used the definition of a search to exclude a wide variety of police investigations from the category of constitutionally recognized searches. Though there

---

51 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 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).

52 398 U.S. 347.


55 *Katz*, 389 U.S. at 361. This test was probably changed by the Court’s decision in United States v. Jones, 565 U.S. ___, 132 S.Ct. 945 (2012), which held that any police trespass on private property for the purpose of obtaining information is a search. *Jones* 132 S.Ct. 945, 949 (2012). This change does not change the analysis in the Article in any meaningful way, and does not disturb existing case law regarding the search/non-search distinction.

56 *Katz*, 389 U.S. at 352 (the Fourth Amendment protects “people not places”).

57 However, 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, *infra* note 77-79 and accompanying text, are not considered searches at all.

58 Justice Scalia, writing for the Court, claimed to be applying well-settled law that a trespass is sufficient to constitute a search. *Jones*, 132 S. Ct. at 940. However, numerous previous decisions explicitly rejected the trespass doctrine. *See, e.g.*, Rakas v. Illinois, 439 U.S. 128, 143 (1978); Kyllo v. United States 533 U.S. 27, 32 (2001).
are many types of non-searches, three different doctrines of non-search are especially illustrative of the efforts courts go to in order to avoid categorization of investigative practices as searches, and to thus avoid the application of the warrant requirement and its assumed interference with police efficiency.

First, information knowingly relinquished to someone else is not protected by the Fourth Amendment.59 The parties deemed to be involved in a communication include not only people participating directly in a conversation, but also third parties that receive information, such as a telephone company that keeps records of numbers dialed. 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.60 The doctrine has been applied to many circumstances. For example, it is not a search when an undercover agent or confidential informant speaks with a subject,61 even if the informant is wearing a wire that allows the police to simultaneously hear the conversation.62 Following this logic, the third-party doctrine precludes any expectation of privacy in the telephone numbers dialed by an individual, even from a home phone, despite the protections of the home.63 By simply 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.”64 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, exposes those records to state investigation without the protection of the Fourth Amendment. This includes a person’s banking information: since their bank has access to the records, the state is free to access those records without such access being considered a search.65 The third-party doctrine is controversial,66 and Justice Sotomayor recently proposed its reconsideration due to the breadth of its impact on daily personal activities;67 however, such considerations were recognized by the justices at the time of the doctrine’s development,68 and the goal of efficient policing was considered strong enough to overcome that concern.69

A second category of non-search covers situations in which the police, while observing actions occurring in plain sight in a public forum, “augment[] the sensory faculties bestowed

62 White, 401 U.S. at 753.
63 Smith, 442 U.S. at 744.
64 Id. (internal quotes omitted).
67 United States v. Jones, 132 S. Ct. 945, 957 (2012) (Sotomayor, J., concurring) (arguing that GPS data reveals intensely private information, such as trips to the psychiatrist, the abortion clinic, the AIDS treatment center, and that being watched chills associational and expressive freedoms).
69 We return to consideration of the third party doctrine in Part IV.B infra, when discussing electronic mechanisms that attempt to ensure digital privacy.
upon them by birth with such enhancement as science and technology afforded to them.™

This allows the police to fly airplanes ¹¹ or helicopters ¹² over the property of those suspected of growing marijuana without such conduct being categorized as a search, even if high-powered cameras are used. ¹³ The only significant limit on the capacity of the police to use enhanced technology is when it enables them to gain information of what is occurring inside the home. It still permits police to place radio transmitters in goods given to a suspect, as long as the transmitter allows the police to track only the suspect’s public movements, ¹⁴ and not the suspect’s movements within her home. ¹⁵ 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 police with information about activity inside that they would not be able to sense absent the device. ¹⁶ But otherwise, police are free to gain extensive information through utilizing powerful technology without such investigations being categorized as searches. While there may be good reason to distinguish between the level of protection that a home versus a public space should receive, it seems counter-intuitive to consider the use of the same technology to look for the same information in the same way to be considered a search in one case and a non-search in the other, simply due to the change in location. The reason for such a doctrinal contrivance is that the police efficiency of avoiding the warrant requirement—achieved by labeling such investigations outside the home to be non-searches—is assumed to be high enough to overcome the privacy lost through allowing police investigative freedom in public places, but not high enough to overcome the privacy costs of similarly liberalizing investigations of the home.

The protection of the home has nonetheless been mitigated by additional judicial artifices, as the Court has invoked a restrictive definition of what parts of private property constitute the home. This brings us to the third category of non-searches: an investigation that takes place in an “open field” surrounding the home is not a search. ¹⁷ To be classified as an open field, and thus for police investigations to be categorized as non-searches, the property in question need be neither open nor a field. An open field can include any unoccupied or undeveloped area outside of the “curtilage” of a home, ¹⁸ which is the land immediately surrounding the house and associated with it. ¹⁹ And 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. The Court held that there was no reasonable expectation of privacy even though the homeowner had posted “no trespassing” signs. ²⁰ In Dunn, even two sets of fencing isolating two barns from the outside world did not preclude warrantless entry by federal officers into the barns from constituting a non-search. ²¹ So even private property containing a home and other associated structures, and those structures themselves, can be

---

¹⁴ Knotts, 460 U.S. at 282.
¹⁶ And because the device is not in such public use as to make one reasonably expect that a private citizen would point one at a home. Kyllo v. United States, 533 U.S. 27, 40 (2001).
¹⁸ Id. at 180 n.11.
²⁰ Oliver, 466 U.S. at 179.
²¹ Dunn, 480 U.S. at 301.
searched at will by police officers under the rubric of non-searches, thus avoiding the jurisdiction of the Fourth Amendment altogether.

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

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

In the Fourth Amendment context, the facilitation of police investigations is often recognized as a central value in the debate over what the law should be and, to the extent that 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, while 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 police to investigate crime and obtain prosecutions. 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 police to effectively investigate crime. This type of balancing inquiry can be seen in the Supreme Court’s analysis of the warrant requirement,\(^82\) the search/non-search distinction,\(^83\) and various exceptions to the warrant requirement.\(^84\)

When deciding these types of Fourth Amendment questions, it is often assumed, by the Court and by commentators, that requiring police to obtain warrants will impede the investigation and ultimate prosecution of crimes. Requiring the police to obtain a warrant for a particular investigation will make it more difficult to find evidence, because warrants are costly in both time and effort\(^85\) and because if a warrant is required then probable cause must be established ex

---

82 See, e.g., Robbins v. California, 453 U.S. 420, 438 (1981) (Rehnquist, J., dissenting) (arguing that the warrant requirement should be reconsidered given its negative impact on law enforcement); Swire, supra note 41, at 59; Bernard E. Harcourt & Tracey L. Meares, Randomization and the Fourth Amendment, 78 U. CHI. L. REV. 809, 815 (2011). The Court has, however, at times denied using such a balancing inquiry regarding the warrant requirement: 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”).

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


85 Technology is making it easier for the police to attain a warrant quickly. Cecilia Chan, Search-Warrant Process for DUIS Faster for Phoenix Police, AZCentral.com (Apr. 11, 2013, 8:37 PM), http://www.azcentral.com/community/phoenix/articles/20130410phoenix-police-search-warrant-process-duis-faster-
Laying out the basis of police officers’ suspicion before a neutral magistrate can delay an investigation, and the magistrate’s potential failure to find probable cause can prevent the search taking place altogether. Allowing the police 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, or to the seizure of evidence unearthed in an investigation that would never have been found if there was no probable cause for a legal search.

The assumption that the warrant requirement impedes police efficiency is mentioned frequently by commentators critiquing the general warrant requirement or advocating possible exceptions to the requirement: they argue that warrants impede police investigations and that this cost outweighs privacy concerns. In juxtaposition, advocates of expansive Fourth Amendment rights argue that the concern about impeding police investigations is overstated, either because probable cause is a low bar for the procurement of a warrant, or because the time and effort costs of obtaining a warrant have not been shown to be prohibitively high. Even those commentators skeptical of the police efficiency justification, however, assume that a police investigation is impeded to some extent by the warrant requirement; they simply dispute by how much. Thus both sides of the debate make the police efficiency-rights trade-off assumption, they simply disagree about the normative value of each opposing possible outcome: warrantless searches and non-searches versus imposing the warrant requirement and delaying or even preventing some searches from occurring.

The Court has been inconsistent in its willingness to explicitly acknowledge that it has balanced an interest in facilitating police investigation against the privacy concern that Justifies the applicability of a warrant requirement. The Court most often uses the interest in police efficiency to justify holding that police were required to obtain a warrant, and has at times used the interest as part of a balancing test, but at other times has explicitly stated that “the mere fact that law enforcement may be made more efficient can never itself justify disregard of the Fourth Amendment.” However, the latter statement has largely become a catchphrase of dissenting

See infra Part III.D.


See, e.g., id.


Tokson, supra note 59, at 641 (“There is evidence to suggest that this concern is overstated... police may often be able to gather sufficient evidence for probable cause before obtaining [the evidence sought in a warrant]”).

Tomkovicz, supra note 86, at 1157.

See Tokson, supra note 56, at 640 (“requiring 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 86, at 1163 (“The deliberate warranted search process undoubtedly results in some lost prosecutions”).


See Steagald, 451 U.S. at 222 (balancing the impediment to police investigations against the intrusion into privacy of unwarranted searches).

Mincey, 437 U.S. at 393.
justices in opposing majorities’ implicit acceptance of the rights-police efficiency trade-off.\textsuperscript{95} In addition, even this opposing position only implies 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. Whether police efficiency is important enough to overcome privacy concerns, the justices commonly assume that police investigations are in fact impeded to some extent when warrants are required: “The investigation of crime would always be simplified if warrants were unnecessary.”\textsuperscript{96}

One area where 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 requirement. For instance, the Court in \textit{New York v. Belton}\textsuperscript{97} determined that the passenger compartment of a car is included in the “the one lunge area”\textsuperscript{98}—the area within the immediate control of the arrestee in a search incident to arrest.\textsuperscript{99} 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.\textsuperscript{100} The Court was willing to make an across-the-board 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.”\textsuperscript{101} This factual presumption was justified largely on the basis that “a policeman [cannot otherwise] know the scope of his authority.”\textsuperscript{102} The Court was concerned about the practical difficulties that would arise for police without such a bright line, and looked for a rule that would provide them certainty, and thus efficiency in investigating crime and making arrests.\textsuperscript{103} This warrant exception expansion was created out of the concern for effective police practice; that position was subsequently rejected in \textit{Arizona v. Gant},\textsuperscript{104} but on the basis that the factual claim in \textit{Belton} was no longer true, not because the Court rejected the Police Efficiency Assumption. The Court concluded that the \textit{Belton} decision itself had undermined its own factual claim, in that the police incentives created by the rule had changed police practices.\textsuperscript{105}

The assumption that warrant requirements impede police investigations also plays a role in cases defining the distinction between a search and a non-search, as described \textit{supra}. The Court

\textsuperscript{95} See, e.g., \textit{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).

\textsuperscript{96} \textit{Mincey}, 437 U.S. at 393. \textit{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. \textit{See Arkansas v. Sanders}, 442 U.S. 753, 767 (Burger, CJ., concurring) (“warrant requirement is not so onerous”); \textit{United States v. Harris}, 331 U.S. 145, 171 (Frankfurter, J., dissenting) (degree to which Fourth Amendment impedes effective law enforcement is grossly exaggerated).

\textsuperscript{97} 453 U.S. 454 (1981).


\textsuperscript{99} \textit{Belton}, 453 U.S. at 462.

\textsuperscript{100} \textit{Id.} at 460.

\textsuperscript{101} \textit{Id.}

\textsuperscript{102} \textit{Id.}

\textsuperscript{103} \textit{Id.}

\textsuperscript{104} 556 U.S. 332, 341-44 (2009)

\textsuperscript{105} \textit{Id.} at 342-43. This interactive dynamic is returned to in Part III.A. \textit{infra}. 
often presents this trade-off in terms of the value to the police of using bright-line rules.¹⁰⁶ For instance, in defining what constituted an open field, the Court majority explicitly rejected a case-by-case test proposed by the dissent¹⁰⁷ because the lack of an ex ante rule would be unworkable for the police.¹⁰⁸ Consequently, even “no trespassing” signs and the field not being visible from the air did not prevent land from being an open field—a rule that prevented even unreasonable police investigations from triggering Fourth Amendment protection.¹⁰⁹

For the same reason, the Court has considered police efficiency when considering 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 to search) versus other objects in a car (which could be searched without a warrant);¹¹⁰ but in California v. Acevedo, the Court recognized that this rule “provided only minimal protection for privacy and [] impeded effective law enforcement.”¹¹¹ The Court was attempting 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.¹¹² It was concerned that the rule “confused courts and police officers and impeded effective law enforcement. . . We have noted the virtue of providing clear and unequivocal guidelines to the law-enforcement profession . . . [and so w]e conclude that it is better to adopt one clear-cut rule to govern automobile searches”—and to expand the automobile warrant exception to include containers in a car.¹¹³

A final illustration: the Court has also acknowledged the influence of police efficiency in their analysis when defining the threshold that police must satisfy in order to gain a warrant: the probable cause test. Illinois v. Gates laid out the modern totality of the circumstances test of whether probable cause has been established.¹¹⁴ In Gates, the Court justified its willingness to flexibly trade off the two prongs that had previously been rigidly applied to this question¹¹⁵ out of recognition of the practical difficulties that police face in the field: police affidavits for search warrants “are normally drafted by non-lawyers 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.”¹¹⁶ In this way, the Court made probable cause easier for the police to establish, out of recognition of the need for police efficiency under trying circumstances.

¹⁰⁶ For an example of bright-line rules in search/non-search cases, see Kyllo v. United States, 533 U.S. 27, 40 (2001).
¹⁰⁷ United States v. Oliver, 466 U.S. 170, 189 (1984) (Marshall, J., dissenting) (“we have traditionally looked to a variety of factors in determining whether an expectation of privacy asserted in a physical space is ‘reasonable.’”).
¹⁰⁸ Id. at 181 (“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.”).
¹⁰⁹ This interactive dynamic is returned to in Part III.A. infra.
¹¹⁰ United States v. Chadwick 433 U.S. 1 (1977)
¹¹² Acevedo, 500 U.S. at 576-79. This exception applies where the police have probable cause to believe the container holds contraband or evidence. Id. at at 579, 589.
¹¹⁵ Gates, 462 U.S. at 235.
The Police Efficiency Assumption makes a great deal of intuitive sense: undoubtedly, a warrant requirement will in many cases make it more difficult for the police 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. That is why the Assumption has long gone unquestioned. However, this Article shows that, in many circumstances, requiring the police 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 the police from finding evidence in an investigation.117 As we show infra,118 allowing the police to investigate without warrants will often provide criminals with a greater incentive to innovate. This innovation will decrease the likelihood that the police will find evidence during an investigation, and, under certain conditions, will offset the benefit that police gain 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.119 Modern empirical research has shown that increased expected punishments deter crime.120 Yet punishment can cause criminals to change their behavior in ways other than deciding whether or not to commit a crime, including by innovating. Criminal innovation occurs when a criminal changes his or her behavior in a strategy designed to decrease the likelihood that the police obtain admissible evidence of a completed or planned crime. Though this phenomenon has been addressed in the economic literature, 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, rather than considering 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 of committing the crime—the probability of being convicted multiplied by the punishment that comes with conviction.121 Thus, both public policy and the law place a high value on protecting and enhancing the ability of the police to investigate crime and obtain prosecutions.

117 See infra Part II.
118 See infra Part III.
119 JEREMY BENTHAM, AN INTRODUCTION TO THE PRINCIPLES OF MORALS AND LEGISLATION, 339 (1907) ("[T]he 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.").
120 For a survey of this research, see Daniel S. Nagin, Criminal Deterrence Research at the Outset of the Twenty-First Century, 23 CRIME & JUSTICE 1, 8-12 (1998).
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. Avoidance behaviors can occur before a crime has been committed, after the crime but before arrest, or after indictment. Collectively, these behaviors are known in the literature as “detection avoidance.” Simple examples of anticipatory detection avoidance include wearing gloves or installing a radar detector in one’s car, which occur while a crime is being committed; more complex mechanisms also exist, such as email encryption, and are explored in Part IV.B. Detection avoidance occurring after indictment includes providing false testimony in court, or escaping from custody. Because this Article concerns police investigations and the warrant process, we focus only those detection avoidance innovations that occur prior to arrest.

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:

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.

More recently, scholars have begun to 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 Malik in 1990. 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—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.

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

---


123 Nussim & Tabbach, supra note 12, at 45

124 Sanchirico, supra note 122, at 1.

125 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 Part V.

126 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 would generally have taken place prior to the arrest.

127 Sanchirico, supra note 122, at 3. 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.”).


129 Becker, supra note 121, at 193.

130 Malik, supra note 128, at 342.
avoidance is possible. A subsequent article by the same authors looked at the possibility of punishing avoidance behaviors as a way to deter them. Their model showed that, while 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. 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. This is even more difficult for ex ante regulation, because many things used for avoidance—such as ski masks or prepaid cellphones—have legitimate as well as criminal uses. Furthermore, sanctioning avoidance simply creates an incentive for criminals to avoid detection of this avoidance.

This Article differs from earlier work on criminal avoidance in two respects. First, it analyzes the interaction of criminal avoidance with the warrant requirement, a topic that has not previously been addressed. Second, it considers the effects that criminal avoidance may have on the decision of the police whether or not to investigate. Because this inquiry is two-sided, our analysis employs game theory rather than a simple economic model of crime. Like the Becker model, 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—but instead of only examining the utility of the criminal facing possible punishment, we consider the interwoven incentives of the police to investigate more or less vigorously. We analyze not only the “best response” of the criminal to crime enforcement policies, but also the best response of the police to criminal innovation in response to those policies, and the best response of criminals to the responses of the police, and so on. This allows us to predict outcomes in a dynamic interaction, representing the ongoing cat and mouse game between criminals and police.

132 Nussim & Tabbach, supra note 12, at 45.
133 Id. at 62.
134 Sanchirico, supra note 122, at 18.
135 Nussim & Tabbach, supra note 12, at 48.
136 Sanchirico, supra note 127, at 1339-40.
137 See, e.g. RICHARD A. POSNER, ECONOMIC ANALYSIS OF LAW 4-6 (5th ed. 1998). This is sometimes contrasted to 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). While behavioral economics analysis is very valuable, it is necessarily secondary: it is first essential to 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.
138 In game theory, a “best response” is the strategy (or strategies) that produces the most favourable outcome for a player, taking the other players’ strategies as given. PETER C. ORDESHOOK, GAME THEORY AND POLITICAL THEORY 115 (1986).
B. Criminal Innovation and the Police Efficiency Assumption

The ability of criminals to innovate can defeat the Police Efficiency Assumption in certain situations. This occurs because 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 police to investigate without a warrant. Ultimately, the police may be no better off in terms of their ability to catch criminals in a world where warrants are required than when they are not, because the extent of criminal innovation can overwhelm the reduced costs of not needing a warrant.

The interaction between criminals and police incentives is dynamic. Criminals will have an increased incentive to innovate when the police have to incur lower effort costs in order to conduct an investigation because, absent this innovation, the police would otherwise investigate more often. This increased innovation will lead to the failure of the Assumption when the gains to the police 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. It is important to note that this is not simply like saying that better cars lead to worse driving; rather, the dynamic is iterative, and key to that iteration is that the conduct of both criminals and police depend on the other, and in a context of uncertainty. If the criminal knows that the police will investigate regardless, the criminal’s innovation will not differ based on the warrant requirement; the same is true if the police are sure not to investigate. If the police decide to always investigate when they do not need a warrant, but never investigate when they do need a warrant, due to the higher cost, this may also lead the criminal to innovate. While this situation does violate the Assumption, innovation does nevertheless reduce police gains from not having to obtain a warrant.

The importance of understanding the dynamic nature of police-criminal interactions has been a lesson learned painfully by the Supreme Court justices in the development of various exceptions to the warrant rule. For instance, as discussed infra, the Court previously deemed that different levels of protection applied to evidence located in containers in cars versus evidence located in the car itself, even when in a part of the car that itself forms a kind of container, such as the glove box or the trunk. 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 became unworkable. Similarly, as noted infra, 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. But another perverse incentive was created for the police: standard practice became 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. The difficulty for reversing this assumption was that doing so could incentivize police to put themselves in danger, by leaving the arrestee un-handcuffed and near the car, in order to gain the

---

139 See infra, Part III.
140 See infra, Part III.
142 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.”).
power to search the car.\textsuperscript{144} Similarly, since police surveillance flights have been considered to not breach any reasonable expectation of privacy—because they have been taken to provide information only about open fields and not the home—criminals have been incentivized to innovate by growing marijuana inside hydroponically, so that overhead airplanes and helicopters cannot view the plants.\textsuperscript{145} 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 the police to obtain bank records without a warrant encourages criminals to keep their funds in less official financial institutions—money laundering is 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.\textsuperscript{146} Each of these innovations creates significant potential hurdles to the ability of the police to catch these criminals. The question is: can those investigatory impediments offset the advantage to the police 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—when the police will not 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 police choice in two different scenarios: one, under the “Warrant” condition, where a court has determined that a particular investigation is a search; the other, under the “Non-Warrant” condition, where a court has determined that the investigation is a non-search. For example, if an investigation that was previously widely considered to be a search is then found to be a non-search by a court, or vice versa, we can compare the effect on police efficacy of the rule change: if the police do not gain from the change away from the warrant requirement, the Assumption fails. In economic language, the Assumption fails if the police’s expected utility\textsuperscript{147} under the warrant condition is greater than or equal to that in the non-warrant condition.

Economic models enable us to formalize the incentives of both criminals and the police, 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 the police and the criminal,

\textsuperscript{144} 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. Tejada, 524 F.3d 809, 812 (7th Cir. 2008)).

\textsuperscript{145} See Glenn Smith, Marijuana Bust Shines Light on Utilities, THE POST AND COURIER (Jan. 29, 2012, 12:01 AM), http://www.postandcourier.com/article/20120129/PC1602/301299979. Arguably, the result has been stronger strains of marijuana, but this is subject to ongoing debate. See Potency of Marijuana, UNIV. OF WASHINGTON ALCOHOL & DRUG ABUSE INSTIT., http://adai.uw.edu/marijuana/factsheets/potency.htm.

\textsuperscript{146} See Part IV.B, infra.

\textsuperscript{147} 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).
since they influence each other. The likelihood that the police will conduct an investigation depends upon the amount of innovation by criminals, because this impacts the chances that an investigation will find evidence. Likewise, the incentives for criminals to innovate will increase when police 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 or not to innovate. These papers have treated a criminal’s likelihood of being caught as being a function of the amount of criminal innovation and the amount of resources society devotes to detecting crime. However, this overlooks the fact that the decision by police to investigate a particular crime is not fixed, but rather depends on the likelihood that an investigation will be successful—that it will reveal admissible evidence. Increased criminal innovation leads not only to a smaller chance of the police finding evidence if they conduct an investigation, but also to a smaller likelihood that the police will investigate at all, given the fact that the police know criminals may innovate. Thus, it is crucial to look at both of these effects when analyzing a criminal’s decision whether or not to innovate.

This Part begins by discussing the variables that influence the decision by the police whether or not to search and the decision by the criminal whether or not to innovate. It then lays out the games and solves them to determine the likelihood that the police 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. 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

---

148 See, e.g., MARTIN J. OSBORNE, AN INTRODUCTION TO GAME THEORY 7 (2004).
149 See, infra Part II.
150 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.
151 The police will be able to innovate as well, through 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 an exogenous variable when police decide whether to innovate. Second, the warrant requirement does not affect the police decision to innovate, as the need for, and effectiveness of, police innovation depends on criminal innovation, not the warrant requirement. An exception would be 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.
152 Becker, supra note 121.
the punishment that comes with detection. 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 or not 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 only applies to crimes that will not be deterred by a transition from the Warrant condition to the Non-Warrant 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 Non-Warrant condition through a reduction in the overall level of crime. 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.

Second, we assume that the criminal can engage in innovation that reduces the likelihood that police will find evidence of crime in the event of a police investigation. 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, 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 or not 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 non-zero amount of innovation; this preexisting innovation is encapsulated in the probability that the police will find evidence in a search.

Third, importantly, unlike in the Becker model, the likelihood that the police will investigate a crime is not fixed for any given crime, but instead changes depending on whether or not the criminal innovates. The exact manner in which innovation changes the police decision whether or not to investigate depends upon the incentives that the police face, but it is clear that police will be less likely to investigate if criminals innovate because the likelihood of finding evidence is reduced. This interaction between the police 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.

153 Id., 181.
155 William J. Stuntz, Local Policing After Terror, 111 YALE L.J. 2137, 2144-45 (2002) (“The police help to restrain crime. Rules that restrain the police thus tend to remove restraints on crime. . . . Restrictions on police authority act as a tax; they make criminal investigations more expensive than it otherwise might be.”).
156 See, e.g. Malik, supra note 128, at 342.
157 Id.
158 Becker, supra note 121, at 181.
The criminal will aim to maximize his expected utility, which will change depending on whether he innovates and whether the police investigate:

**Figure 1: Criminal’s Payoffs**

<table>
<thead>
<tr>
<th>Criminal’s Choice</th>
<th>Innovate</th>
<th>Not Innovate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Police Action</strong></td>
<td>Investigate</td>
<td>Not Investigate</td>
</tr>
<tr>
<td>Investigate</td>
<td>$-c - \alpha^L$</td>
<td>$-c$</td>
</tr>
<tr>
<td>Not Investigate</td>
<td>$-\alpha^H$</td>
<td>0</td>
</tr>
</tbody>
</table>

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

Criminal utility is a function of $c$, the cost of innovation, and $\alpha$, the probability that the police will find a particular piece of evidence if they investigate, with the probability being high ($\alpha^H$) if the criminal does not innovate, and low ($\alpha^L$) 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 the police, for the criminal, the payoffs are the same in the Warrant and Non-Warrant conditions, so only one matrix is shown.

**B. Police Activity**

Unlike most models of criminal innovation, which consider the likelihood of a police investigation to be fixed, police 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 police utility. Unlike criminal utility, which is obviously the profits of crime, in these models it is standard to treat police 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 police investigation, in terms of other investigations not undertaken or delayed; rationally, the police will prioritize investigations likely to lead to positive results. Viewed in these terms, it follows that police will have an

---

159 We make the standard assumption that the criminal and the police are risk-neutral. See, e.g., Sanchirico, supra note 122, at 3 n.8.; Malik, supra note 128, at 341.

160 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 criminal utility matrix.

161 See, e.g. Malik, supra note 128, at 342.
incentive to search less often if criminals innovate, because the likelihood of finding evidence in a search will be smaller.

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

Further complicating the situation here, we must consider the different payoffs to the police first under the condition in which a warrant is required for the investigation, and then in a world where no warrant is required:

**Figure 2: Police Payoffs**

**A. Warrant Condition**

<table>
<thead>
<tr>
<th>Police Choice</th>
<th>Investigate</th>
<th>Not Investigate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criminal’s Action</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Innovate</td>
<td>$-z - w + g \alpha^L$</td>
<td>0</td>
</tr>
<tr>
<td>Not Innovate</td>
<td>$-z - w + g \alpha^H$</td>
<td>0</td>
</tr>
</tbody>
</table>

**B. Non-Warrant Condition**

<table>
<thead>
<tr>
<th>Police Choice</th>
<th>Investigate</th>
<th>Not Investigate</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Criminal’s Action</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Innovate</td>
<td>$-z + g \alpha^L$</td>
<td>0</td>
</tr>
<tr>
<td>Not Innovate</td>
<td>$-z + g \alpha^H$</td>
<td>0</td>
</tr>
</tbody>
</table>

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 police resources. Warrants are directly costly to obtain because of the time and resources necessary to obtain a warrant, and are also indirectly costly—i.e. 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.\(^{162}\) 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 Non-Warrant condition.

\(^{162}\) A cost that was previously more considerable than it is now, in an era of electronic warrants. See supra, Note 85.
The variable $g$ signifies the gain to the police 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 crime, the punishment of past crime, and the successful return of money or goods that were taken in a crime. Finally, $\alpha$ 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 Non-Warrant conditions as simplified as possible: warrants increase the cost for police, but have no other effect. This is establishing the easiest possible test for the Police Efficiency Assumption. If we can show that the Assumption fails sometimes under these conditions, then it should fail under more complex conditions where 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 police response, given that a criminal’s utility depends not only upon his own decision whether or not to innovate, but also upon the decision of the police 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.\textsuperscript{163} It defines the best strategy of each party for every possible choice, given the expected action of the other party.

Broadly speaking, games can be either sequential or simultaneous. In a sequential game, one player chooses her action before the second player; 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 or not to innovate before the police decide whether or not to investigate. However, often the police officer will also not initially know whether the criminal has masked his crime through innovation,\textsuperscript{164} and thus she cannot base her investigation decision on the criminal’s innovation decision, and the criminal will not know whether the police are likely to investigate. Therefore, the game ought to be modeled as a simultaneous game: 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 Non-Warrant condition; in the latter, police 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 police. Each has two possible actions: the criminal can innovate or not innovate; the police can investigate or not

\textsuperscript{163} \textit{OSBORNE, supra} note 148, at 7.

\textsuperscript{164} Interestingly, the criminal may sometimes have an incentive to signal to the police that he has innovated. If this information is considered by the police to be credible, and not a bluff, it could convince the police not to investigate, given that they know that the likelihood of finding evidence is small. In the absence of actual innovation, the criminal may have an incentive to bluff. Of course, a criminal’s signal that he has innovated can also serve as a signal to police that he has committed a crime that needs covering up. Bragging to the police about your brilliant cover-up is probably only worth the risk if it truly is brilliant.
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 the police do—(Innovate, Investigate), (Innovate, Not Investigate).\(^\text{165}\) 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 Non-Warrant conditions, we can determine if (or how often) the criminal will innovate and the police 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.\(^\text{166}\) For example, (Innovate, Not Investigate) is a Nash equilibrium if (a) the criminal is better off innovating than not innovating, assuming that the police don’t investigate, and (b) the police are 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 one player will be better off by unilaterally changing his or her strategy.\(^\text{167}\) A game can have one Nash equilibrium, many, or none.\(^\text{168}\) 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.\(^\text{169}\) 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.\(^\text{170}\) For example, there could be a mixed strategy Nash equilibrium where the criminal innovates with a probability of one-third (and does not innovate with a probability of two-thirds), and in which the police investigate with a probability of three-fourths (and do not investigate with a probability of one-fourth). Conceptually, this means that the police do not know whether or not 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, police utility in the Nash equilibrium under the Warrant condition is greater than or equal to police utility in the Nash equilibrium under the Non-Warrant 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

\(^{165}\) The first part of the parenthetical is the criminal’s action, and the second part is the police action.

\(^{166}\) MORROW, supra note 147, at 80.

\(^{167}\) 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 an accurate prediction of human behavior. See, e.g., George J. Mailath, Do People Play Nash Equilibria? Lessons from Evolutionary Game Theory, 36 J. ECON. LIT. 1347, 1348 (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. Id.; Mailath at 1352.

\(^{168}\) OSBORNE, supra note 148, at 7.

\(^{169}\) ORDESHOOK, supra note 138, at 117.

\(^{170}\) Id. at 133.
each possible outcome, and our overall results. There are three possible pure Nash equilibria in the warrant world. Only one of the equilibria can actually occur at a time; which will occur will depend on the values of different variables within the model.

- (Innovate, Investigate) is a Nash equilibrium if \( c < \alpha H - \alpha L \) and \( w + z < g \alpha L \). 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 the police from investigating are larger than the fixed costs of the investigation and warrant.
- (Not Innovate, Investigate) is a Nash equilibrium if \( c > \alpha H - \alpha L \) and \( w + z < g \alpha L \). 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 \( g \alpha H > z \), meaning that the gain to police from investigating is smaller than the costs, even if the criminal does not innovate.

Note that the outcome (Innovate, Not Investigate) is never a Nash equilibrium because if the police 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 \( \lambda = \frac{1}{g \alpha H - \alpha L} \) [ \( \alpha H - \frac{w + z}{g} \)], and police investigate with probability \( \emptyset = \frac{c}{g \alpha H - \alpha L} \). This Nash equilibrium occurs when \( c < \alpha H - \alpha L \) and \( g \alpha L < w + z < g \alpha H \). Intuitively, this means that the police 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, 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.

There are also four Nash equilibria in the Non-Warrant condition. These are the same as the Warrant condition Nash equilibria, except without the “\( w \)” warrant cost terms:

- (Innovate, Investigate) if \( c < \alpha H - \alpha L \) and \( z < g \alpha L \).
- (Not Innovate, Investigate) if \( c > \alpha H - \alpha L \) and \( z < g \alpha L \).
- (Not Innovate, Not Investigate) if \( g \alpha H > z \).
- The criminal innovates with probability \( \lambda = \frac{1}{g \alpha H - \alpha L} \) [ \( \alpha H - \frac{z}{g} \)], and police investigate with probability \( \emptyset = \frac{c}{g \alpha H - \alpha L} \) when \( c < \alpha H - \alpha L \) and \( g \alpha L < z < g \alpha H \).

171 The criminal prefers to innovate if the police investigate only if \( c < \alpha H - \alpha L \). Likewise, the police prefer to investigate if the criminal innovates if \( g \alpha H > w + z \). (Innovate, Not Investigate) is not an equilibrium because, if the police don’t investigate, the criminal will choose not to innovate, since \( b > b - c \).

172 Thus, the criminal will mix if \( EU_C(\text{Innovate,Investigate}) \cdot p_p(\text{investigate}) + EU_C(\text{Innovate,Not Investigate}) \cdot [1 - p_p(\text{Investigate})] = EU_C(\text{Not Innovate,Investigate}) \cdot p_p(\text{investigate}) + EU_C(\text{Not Innovate,Not Investigate}) \cdot [1 - p_p(\text{Investigate})] \)
D. When is the Assumption Violated?

The Police Efficiency Assumption is violated if, for a given set of constants \((z, w, c, g, \alpha^L, \text{and } \alpha^H)\), the expected utility of the police under the Non-Warrant condition is not greater than it is under the Warrant condition, as is commonly assumed and used to justify non-application of the warrant requirement. This section shows that the Assumption sometimes fails—sometimes the police do not benefit from not being required to acquire a warrant before conducting a search, or from an investigation not being considered a search at all. We show when the Assumption will fail, and when it will not. We then show that the circumstances where the Assumption fails are likely to be quite significant.

We begin with two simple outcomes—one where the Assumption holds, and one where 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 Non-Warrant condition. If we were to move from the Warrant condition to the Non-Warrant condition—for instance if the law became less stringent for the police—the police would face lower costs because they would not have to bear the costs of seeking a warrant; furthermore, since under this set of strategies, the criminal is already innovating, the police would also encounter no greater difficulty in finding evidence. Thus, the assumption is not violated: elimination of the warrant requirement would simply lower police costs.

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

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 \(c < \alpha^H - \alpha^L\) and \(g^L < z < w + z < g^H\). The latter term requires that \(w < g^H\) and \(z < g^L\). If the Nash equilibrium in both conditions is mixed, we can test the Assumption by determining when police expected utility in the Warrant condition is greater than or equal to the expected utility in the Non-Warrant condition, with both actors mixing with the probabilities given by the equilibrium. It turns out that, in this mixed Nash equilibrium, the police gain no benefit from not having to obtain warrants.

That the Assumption fails 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 best off innovating if the police are going to investigate but that they will not bother incurring the cost of innovating if the police are not going to investigate; but since the criminal will have to make that decision without knowing what the police will in fact do, he will usually be better off varying his strategy, i.e. playing a mixed strategy. Similarly, if criminals generally know that the police will always investigate when they innovate, the criminals will have an advantage; therefore, the
police 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, the police will be no better off by not being lawfully required to obtain a warrant before investigating—warrants 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. This situation will occur when $c < \alpha^H - \alpha^L$ and $g^L < z < g^H < w + z$. Conceptually, this result shows that criminals will increase their innovation when the police do not have to obtain a warrant.

The failure of the Assumption in these circumstances should not be seen as 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 are likely to characterize a large percentage of potential police 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 the police will investigate, but innovating is not worthwhile if the police are definitely not going to investigate. Obviously, the criminal has no reason to innovate if the police are not going to investigate, since 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 would only rule out innovations that are costly yet bring few gains—we discuss specific applications of this conclusion in the next Part. For the police, the mixed Nash equilibrium simply means that the police 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 many real-life cases, in which criminal innovation can turn a worthwhile police 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:

$$(1) \; c < \alpha^H - \alpha^L, \text{ and } g^L < z < w + z < g^H$$

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 the police will find a particular piece of evidence if they investigate; and for the police, the cost of obtaining a

---

173 If the police 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 the police stop investigating, the criminals will stop innovating. But, since the probability of finding evidence then rises, the police will start investigating (sometimes)—putting us back where we started.
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.

In addition, the Police Efficiency Assumption is also violated if instead:

\[ (2) \quad c < \alpha^H - \alpha^L, \text{ and } g^L < z < g^H < w+z \]

This second result means that the Assumption is also 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 that 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 police outweigh the benefits of a probabilistically successful search, and also when they do not, as long as the other requirements hold.

Third, the Assumption is also violated if the police do not search in either condition. This occurs when:

\[ (3) \quad g^H < z. \]

This means that the gains of a successful investigation are less than the cost of investigation, which makes it not worthwhile for the police to search, regardless of whether they need a warrant or not.

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\(^\text{174}\) that allow us to show how the likelihood that the Assumption is violated varies with such changes.

Changes could take place that affect the incentives of criminals, which in turn affects the incentives of police. 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 chances of a successful investigation decreases, and the police are less likely to investigate even without the warrant requirement. Second, a greater innovation-created reduction in the likelihood of the police finding evidence in an investigation \( (\alpha^H - \alpha^L) \) 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 the police more directly. First, while the cost of seeking a warrant \( (w) \) does not determine when the Assumption is violated, it does matter when assessing the gains to police when the Assumption \emph{is not} violated. If the police 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

\(^{174}\)“Comparative statics is the method of analyzing the impact of a change in the parameters of a model by comparing the equilibrium that results from the change with the original equilibrium.” The New Palgrave: Dictionary of Economics 517 (John Eatwell et al. eds., 1987).
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 only be worthwhile to do some of the time, warrant or not, and the Assumption fails. Additionally, the Assumption is also violated if $z$ is so high that the police never investigate.

**IV. Discussion and Policy Implications**

This analysis has significant implications for current Fourth Amendment thought. We first consider the general implications of our results, then consider the specific application of electronic privacy.

**A. General Implications**

First, the assumption that the job of the police 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, the police are not in fact better off when they do not need to obtain a warrant. This includes the most likely scenario—in which the police will investigate sometimes, but not all the time, in both the Warrant and the Non-Warrant conditions. Additionally, while there are circumstances in which the police will be better off without having to obtain a warrant, the degree to which the police gain is smaller in some of these situations if criminals are able to innovate.

The Police Efficiency Assumption is a key part of the balancing inquiry when courts determine whether or not to require a warrant for a particular investigation. The results of this analysis show that the weight of this Assumption in the balance should be significantly lowered.

Second, ridding the police of the necessity of obtaining a warrant does not just affect criminals: it does great harm to people who have not committed a crime. The Fourth Amendment is meant to apply when the police wrongly suspect someone. In such a case, the two parties will have differing information: while the civilian knows that she has committed no crime, the police will wrongfully suspect her. In that case, the suspect—who is actually innocent—is unlikely to innovate. The police, however, will be more likely to investigate in the Non-Warrant condition because the investigation is less costly; thus, there will be a greater number of investigations of innocent suspects without a warrant requirement. The privacy interests of innocent people are harmed when the police are not required to obtain a warrant for an investigation. We have shown that the Police Efficiency Assumption is fragile even ignoring these effects; considering these important privacy ramifications weighs further against the weakened Assumption when determining whether or not an investigation should be termed a search. We explore this in greater detail with reference to specific applications, in the next section.

---

175 Specifically, the gain to the police is not diminished by innovation where they would search with certainty in the Warrant condition; this is when (Innovate, Investigate) is a Nash equilibrium in this condition. The police’s gain will be diminished by innovation in a switch to or from the mixed strategy Nash equilibrium.

176 See supra Part I.


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 supra, the reasonable expectation of privacy test has often been derided as circular, because police actions—as well as court decisions and legislation—shape societal expectations. This allows the state to gradually shift the boundaries of what police are 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. 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. As more and more techniques of surveillance become expected, the privacy of all—criminal and non-criminal alike—recedes. The standard response to this critique is that such diminished privacy will make it easier for the police to catch criminals, yet our analysis shows the weakness of this assumption. In particular, while increased police 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.

Combining these last two implications means that there will be an increased need for non-criminals to innovate. Without the warrant requirement, with a decreasing realm of privacy and less costly police investigations, innocent people may face a stark choice: either acquiesce to increased police 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 the police, but rather of measures taken to legitimately protect one’s privacy from intrusion. 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 the police will not gain. We discuss how this is exacerbated in the new context of mass NSA searches in the next section.

The results of our model also alter the analysis of Fourth Amendment search/non-search distinction. There are three main possible policy implications of these results. First, courts could decide to give the Police Efficiency Assumption less weight when deciding whether to term an investigation a search or a non-search. This outcome 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 non-search have on innocent suspects. However, our analysis also shows that allowing police to investigate without a warrant does make the job of the police easier in a significant amount of situations. Thus, although our results do not necessarily show that the Assumption should be entirely eliminated, they do show that the weight accorded to it should be diminished.

Second, courts could tailor their analysis by giving the Assumption less weight in situations where it is least likely to hold. The main problem with this approach is that courts will often be unable to discern the impact of the Assumption for a specific type of investigation due to the

179 See supra notes 28-30 and accompanying text.
large amount of information necessary—courts would need to determine the precise costs of warrants, investigations, and criminal innovations, as well as the decreased probability that police would find evidence caused by an innovation. Even more problematic, the values for different constants in this model can vary widely between different crimes, even for the same type of investigation. For example, consider a specific investigation: a canine sniff of an air passenger’s luggage. It is possible that the costs of preventing the detection of marijuana (through selective plant breeding or cloaking scents) could be very different than preventing the detection of cocaine. Thus, the Assumption could be violated when a certain type of investigation targets one crime, but not violated when it targets a different crime. However, this model shows that the Assumption is more likely to hold when the gains to the police of a conviction are particularly high\(^{181}\)—or, put differently, when the severity of the crime is high. It is commonly argued that courts should “incorporate the severity of the crime being investigated into determinations of constitutional reasonableness” when deciding whether or not a warrantless search is reasonable, or whether an investigation is a search at all.\(^{182}\) The question of whether to consider the seriousness of the offense is before Supreme Court this Term.\(^{183}\) While there are problems\(^{184}\) with this type of “crime severity analysis,”\(^{185}\) it would result in courts giving more weight to the Assumption in cases in which it is more likely to hold. The model also demonstrates that the Assumption is particularly likely to hold when warrant costs are high, suggesting that making warrants easy for the police obtain is not necessarily the right response.

Finally, policy changes could be made that would reduce the frequency of situations in which the Assumption does not hold. One route would 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 of economic models of crime.\(^{186}\) However, either of these responses would make it more likely that the Assumption will fail, because the criminal will be more likely to innovate.\(^{187}\) An alternative to ex post punishment of innovation is ex ante regulation of criminal innovation through taxes. Taxation is likely to be more effective than increased punishment because it reduces both innovation and crime. 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.\(^{188}\) This 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 police

\(^{181}\) This is because the police will investigate with or without needing to obtain a warrant, while the criminal will not change her innovation behavior. See supra Part III.
\(^{182}\) Bellin, supra note 38, at 6.
\(^{183}\) Navarette v. California Docket No. 12-9490. 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—available at http://www.oyez.org/cases/2010-2019/2013/2013_12-9490.
\(^{184}\) See, Slobogin, supra note 177, at 2.
\(^{185}\) See id.
\(^{186}\) See, e.g., Polinsky & Rubinfeld, supra note 31 (arguing that maximal deterrence may require increasing punishment levels for recidivists); James Andreoni, Reasonable Doubt and the Optimal Magnitude of Fines: Should the Penalty Fit the Crime? 22 RAND J. ECON. 385 (1991) (critiquing maximum punishments for decreasing the probability of conviction).
\(^{187}\) Nussim & Tabbach, supra note 12, at 46.
\(^{188}\) Id. at 48.
detection, such as encryption software. A separate problem is that punishing innovation creates an incentive for the criminal to innovate further, to cover up the initial innovation.\textsuperscript{189} Finally, raising the costs of innovation also raises barriers to use these mechanisms 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 where the central result of our model—the challenge to the orthodoxy that the police will always be better off without a warrant requirement—is likely to have a significant impact. We demonstrate that the most normatively unattractive outcome, where innocent individuals suffer from the lack of a warrant requirement yet the police 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 will nonetheless be attractive to wrongdoers if warrants are not required for the police to search. We consider first email encryption, and show why it is impractical for the average non-criminal user. Then we describe new alternative means of electronic identification- and content-masking, such as Privnote and Snapchat; these programs offer less protection than email encryption, but are considerably more practical. Finally, we assess how the negative repercussions we describe compare to the privacy incursions posed by the NSA spying program.

1. *Email and Encryption*

Although email constitutes one of the central mechanisms of modern communication for private individuals, the constitutional privacy status of the trillions of emails\textsuperscript{190} sent annually in the United States is ambiguous.\textsuperscript{191} The primary reason for the potential lack of privacy from state incursions\textsuperscript{192} is the operation of the third-party doctrine. Most individuals’ emails are sent through massive Internet Service Providers (ISPs), such as Gmail, Hotmail or Yahoo.\textsuperscript{193} 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.\textsuperscript{194} 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 emails is lawful, and, as mentioned, at least one justice is questioning whether the breadth of the doctrine is appropriate in the digital age.\textsuperscript{195} However as precedent stands,\textsuperscript{196} email is unprotected from state surveillance.\textsuperscript{197}

\textsuperscript{189} Sanchirico, supra note 127, at 1339..  
\textsuperscript{191} See Matthew J. Tokson, The Content/Envelope Distinction in Internet Law, 50 WM. & MARY L. REV. 2105, 2110 (2009). 
\textsuperscript{192} There is also the possibility that private individuals may be able to access this information; this possibility likewise encourages the type of innovation we explore below. 
\textsuperscript{193} Email Security and Anonymity, ANONIC.COM, http://www.anonic.org/email-security.html. 
\textsuperscript{194} See supra Part I.A. 
\textsuperscript{195} See supra note 67. 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
Both innocents and wrongdoers who wish to keep their emails private, then, may consider potential innovations to counter the transparency of email systems. The most commonly contemplated response is encryption, but understanding how both email systems and encryption work reveals the impracticality of this for the average email user. Even after learning about the NSA’s spying program, most ordinary email users do not use encryption; in fact, use of encryption is so rare that the NSA considers that the fact of an email being encrypted makes that message a priority for its scrutiny. The reason for this lack of use of encryption is that it is costly in numerous ways. For starters, each recipient of each email sent by the user has to have the tools to decrypt any message sent to them. While 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 email, since the person at the other end has to have the same program as the sender. Thus while encryption may be worthwhile for specific messages that require particular privacy—such as criminal action, discussed below—it is impractical for everyday use by ordinary users emailing a plethora of recipients.

In addition, users cannot generally use encryption with standard service providers, such as Gmail. The reason is that email sent through ISPs such as Google typically travel from the user to their ISP, to the recipient’s ISP, and then to the eventual recipient. Consequently, even if the message is initially encrypted, it will not stay encrypted when in the ISP system. Any email user who wants to use encryption as a standard privacy-protection mechanism would have to use a platform other than the common commercial ISPs—a significant inconvenience. One might expect, then, that the market would respond to solve this failure: if enough individuals want 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).

As described infra in Part IV.B.3, the court that held the NSA’s actions to be presumptively unconstitutional did so by concluding that Smith v. Maryland no longer applies.

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


Instead, the user could potentially attach encrypted files, but this has its own inconveniences.
privacy protection through encryption, at least one of the major ISPs should start providing that service.\textsuperscript{204} However, the aforementioned path traveled by emails through the ISP system also explains why we cannot expect this failure to be solved by the market. The income model of ISPs such as Google is based on advertising.\textsuperscript{205} While Google may be willing to encrypt information in the ISP to ISP stage of delivery, it is unwilling to allow encryption to remain in effect between itself and its users, because Google develops its ads by scanning the content of users’ emails.\textsuperscript{206} Gmail is not free—you pay for it partly by subjecting yourself to advertising and by providing Google with useful data at the aggregate (and possibly the individual) level. Fully encrypting emails would require a very different quid pro quo. Therefore, in order for a Google competitor to fulfill the demand for encrypted email in its system, it would not only have to develop a competitive email 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,\textsuperscript{207} but also an alternative, viable revenue stream. Even then, spam filtering would become impossible with encryption between the user and the ISP—users would have to be very sharply protective of their privacy to be willing to give up spam filtering.

It is not surprising, then, that encryption is rarely used for emails by private individuals.\textsuperscript{208} 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 non-electronic crimes.

With the warrant requirement, the gains of masking emails pertaining to high risk, high reward criminal activity may consistently overcome the costs of innovation—and so the warrant requirement would simply add additional costs to police investigation, since such criminals would innovate either way. However, 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 smalltime 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 other times it will not be worthwhile. Either way, as shown in our model, this could result either in police not searching, or police investigating and the criminal innovating or not innovating—all three


\textsuperscript{205} See id.

\textsuperscript{206} Google Apps Documentation & Support, https://support.google.com/a/answer/60762?hl=en (“Our systems scan and index emails . . . ; this scanning is 100% automated and cannot be turned off . . . Th[is] enable[s] us to display contextually relevant advertising.”).

\textsuperscript{207} As of late 2012, over 95% of Americans used either Yahoo, Gmail, or Hotmail for email service. Rani Molla, \textit{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/.

outcomes are Nash equilibria. So with the warrant requirement, both good and bad outcomes will occur in terms of effective law enforcement.

Those bad outcomes in which the criminal gets away with his crime, however, may occur more often where there is no warrant requirement. Without the warrant requirement, criminals will not have any expectation of warrant protection, and using email encryption will be sensible in many more cases. This will be a bad outcome in terms of the capacity of the police to catch criminals. Counter to popular belief, although the NSA can break most encryption programs, it is practically almost impossible for regular police to break encryption programs. 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). The factors are the keys to the product, which is the lock. Since both factors are prime numbers, there is only one solution to open the lock. 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, because it takes considerably less time and computing power to generate the product—to encrypt—than to reverse engineer the factors—to decrypt. 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 17 million digits and took 39 days of continuous computing calculation to initially verify it.

Encryption codes can, nevertheless, be cracked—it just takes considerable computing power. “Brute force decryption” can reverse engineer the factors simply by 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. 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.”

That quote illustrates two important elements at work here. First, decryption is not a practical option for the average police investigation. With enough computing power, even 256 bit encryption can be cracked in less than 1000 years, but it would cost millions of dollars in computing technology. So brute force decryption will realistically only be available to high end


\[212\] Id.

\[213\] Id.

\[214\] Id.

\[215\] Id.

\[216\] Id.

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. As such, if courts are concerned with police efficiency, in such instances they would be better off retaining the warrant requirement, so as to avoid making such effective criminal innovations worthwhile.

That does not mean, however, 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 police counter-response, is a back-and-forth, cat and mouse game of innovation and counter-innovation. 218 For instance, acoustic cryptanalysts have recently discovered that encryption keys can be ascertained simply by listening to a computer decrypt an encryption program. 219 Cryptanalysts were able to extract even 4096-bit keys from a laptop in less than an hour. 220 But it was soon discovered that this innovation in turn could be undermined by various noise creation mechanisms. 221 Clearly then, as with so many criminal innovations and police 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.” 222

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 police will be able to effectively investigate, as well as the corresponding uncertainty of the police 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: police 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.

Even greater problems arise with stronger forms of encryption, such as by masking the user’s identity and location by rerouting each person’s Internet activities through a system such as Tor. 223 The advantage of Tor is that it is, at least currently, almost unbreakable, even by the

---

218 Encryption may also 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 199.

219 Unsafe and sound: Ciphers can now be broken by listening to the computers that use them” THE ECONOMIST (Jan. 18, 2014), available at http://www.economist.com/news/science-and-technology/21594240-ciphers-can-now-be-broken-listening-computers-use-them-unsafe (“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.”).

220 Similarly, “hackers have begun to use the power of modern graphics processing units . . . to crack passwords.” Arthur, supra note 217. 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.

221 Id.

222 Id.

223 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, https://www.torproject.org/about/overview. Other mechanisms include “full disk encryption,” which encrypts the contents of an entire hard drive, making it impossible for investigators to access the contents. Eoghan Casey et al., The Growing Impact of Full Disk Encryption on Digital Forensics, Vol. 8 Issue 2 DIGITAL INVESTIGATION 129, 129 (Nov. 2011). Another option is PGP (“Pretty Good
NSA. But while Tor is suitable for individual criminal activity, such as visiting The Silk Road to purchase narcotics, much like email 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. 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 and 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, so it is not surprising that it is the most commonly promoted response to email violability. But while there are significant moral hazards impeding the ISP market from meeting the demand for increased email privacy protection, the broader online market has responded to demand for private communication in other ways. One response has been to design new technology which 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. The message creator crafts a note, sends the URL to the recipient, who clicks on it, 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, since the link will no longer exist. Of course that does not entirely replicate the scenario where the message had 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 mechanism—as the Supreme Court has recognized—something particularly true of recorded

---


229 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.”).
messages. In addition, though, the message could be intercepted and read by someone other than the intended recipient, such as by the government: since the message takes the form of a URL, if a third-party obtained knowledge of where to look, they could potentially read the message before the intended recipient. But in this scenario, although Privnote cannot prevent interception, the system enables the sender to detect it: since the message is destroyed after being opened, it can only be viewed by one person; while 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 may also offer the benefit of avoiding the application of the third-party doctrine. Unlike email ISPs, the Privnote platform does not hold the content of the messages sent on its server in any readable format at any time. 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. However the messages themselves are stored on the Privnote servers prior to being read. 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 messages. Also, while it is possible that Privnote could insert code to intercept the content of the notes, the website and its creator swear that will not be done. While these three caveats provide qualifications on the actual capacity for privacy invasion, 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 so the third-party doctrine does not kick in.

Thus while email encryption may be clunky and impractical for the average non-criminal user aiming to protect his or her privacy, more recent innovations may offer greater protection to

---

230 There are reports of nude Snapchat photos being screenshot and then forwarded as a form of pornography. 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.

231 Privacy Policy, https://privnote.com/privacy/ (“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”).

232 Id.


234 Id.


236 Id. (comments section).

237 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… I have no reason to believe they’re doing this… but as 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.” Wonko.com, Update: Privnote’s developers are confused, (July 06, 2008, 7:11 PM) http://wonko.com/post/privnotes-developers-are-either-stupid-or-malicious

238 In addition, since Privnote does not log IP addresses, FAQ, https://privnote.com/faq/, 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.
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 1 to 10 seconds after viewing, according to the sender’s preference.239 The program was designed to create a social networking site providing greater privacy by making content temporary.240 But there are a number of elements that make Snapchat less privacy-protective than Privnote.241 Unlike Privnote, Snapchat messages can only be sent to a sender’s online friends list; thus the platform has user and communication identification capability. In addition, although Snapchat claims to automatically delete all photos from its servers such that they can no longer be retrieved by anyone for any reason,242 forensic analysts have actually determined that photos can be “undeleted.”243 In addition, the messages are actually saved on Snapchat’s servers for up to 30 days (if unopened),244 meaning that users have actually relayed the content of the messages to the company. Finally, perhaps as a result of Snapchat’s popularity,245 an app has been developed, SnapHack, that lets people look at old snapchats; it is expected that there will soon be a version that will allow forwarding to third parties.246 These are exactly the sort of capabilities that justified the third-party doctrine in the first place,247 thus Privnote’s legal advantage is unlikely to apply to Snapchat.

The irony of an outcome where Privnote messages receive greater constitutional protection than Snapchat’s is that Privnote seems much more likely to be used by wrongdoers than Snapchat. Snapchat involves people (mostly teens),248 who know each other well enough to be

---


240 Id.

241 Other websites, even those primarily used for anonymous sexual hookups, such as Grindr, which are surely 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, http://grindr.com/terms-of-service.


243 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/ (“it’s possible to pull Snapchat photos from Android phones simply by downloading data from the phone using forensic software and removing a “.NoMedia” file extension that was keeping the photos from being viewed on the device.”).

244 How Snaps are Stored and Deleted, supra note 242.


246 Ellie Zolfaghari, 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

247 The logic of the third party doctrine is that if you reveal information to a third party, they can betray you, and thus there is no difference 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.

248 Magid, supra note 239.
“friend” contacts, passing 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. 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 non-criminal private communications but it is inherently well suited to masking criminality,249 and far less convenient for back-and-forth conversation.

Unlike email 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 smalltime 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 police do not know where to look. But for more serious crime, subject to more thorough investigation, these programs offer less protection, as they can be made accessible to the government, and Snapchat has received warrants to look at unopened images.250 Thus 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 police to know where to look. Thus the police may be as well off having to develop probable cause and obtaining a warrant to search a criminal’s email than in having no warrant requirement but, as a result of even petty criminals turning to this kind of innovation, having to figure out which platform a criminal was using and trying to find the incriminating messages before they are destroyed.

So without a warrant requirement, the end result seems likely to be that programs like Snapchat, most likely to be used by non-criminals, will receive little protection; Privnote and its ilk that are inherently amenable to smalltime criminality will offer significant protection but be permeable; and serious criminals will use more complex innovations, such as Tor or email encryption, that will be far more costly but extremely hard to crack. The heightened fear of investigation due to the lack of warrant requirement will, then, 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 crime investigation as hard as the warrant requirement would.


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

249 However, there are legitimate uses 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, https://www.torproject.org/about/overview.

For instance, if the police profile individuals who wear red and white checked scarves because they are associated with approval of terrorist methods, then these searches can be easily avoided by switching apparel, albeit perhaps with free speech costs. Whereas if the government targets red cars for additional scrutiny because they believe these cars are more dangerous, drivers can only avoid such additional scrutiny to the extent that they can absorb the transaction costs of switching cars or painting their cars. And if the police 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. Thus if the public knows that government can and does access your email, your expectation of privacy in email is reduced by this revelation, 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), the NSA has been capturing, siphoning, storing and cross-referencing vast swathes of personal data, including collecting the call-detail records of all customers of the major telecommunications companies, and data mining billions of emails each day, analyzing them for patterns and connections. This metadata includes all “non-content” information of phone calls, including the numbers dialed, duration of calls, and the location information of cell phones. 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

---


252 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.

253 Spencer Ackerman, FISA Court Order that Allowed NSA Surveillance is Revealed for First Time, THE GUARDIAN (Nov. 19, 2013, 10:09 AM), available at http://www.theguardian.com/world/2013/nov/19/court-order-that-allowed-nsa-surveillance-is-revealed-for-first-time.

254 See e.g., Electronic Frontier Foundation, How the NSA’s Domestic Spying Program Works, https://www.eff.org/nsa-spying/how-it-works.


256 Id.
reasonable suspicion. 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. The core of the controversy of the NSA searches is that it alters the basic principle that the Fourth Amendment limits police investigation methods by requiring specificity and reliability of police 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 email communications makes switching to alternative means of communication dependent on some form of technology, such as those described 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 in the manner that Tor does with Internet communication, or by rerouting telephone calls over Wi-Fi and other channels to avoid any call log being created. 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 by ordinary citizens.

Second, the constitutionality of the NSA searches hinges on the same considerations described above in relation to privacy in email 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, coming to opposite conclusions. In the D.C. District Court, Judge Leon held that the NSA’s bulk collection of telephone metadata is likely unconstitutional. Judge Leon distinguished Smith v. Maryland by stating that it was no longer applicable to modern-day circumstances, where 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. The opinion struck many as incorrect because the added capabilities of cellular phones arguably should not matter because the metadata being collected by the NSA is the same that was collected 34 years ago in Smith. The Supreme Court has repeatedly said that achieving in a more efficient manner an outcome that was previously judicially approved does not render a state action

---

257 Under the Foreign Intelligence Surveillance Act 50 U.S.C. § 1861 (1978), 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 emails without a FISC approval or a warrant. Officer of the Inspector General, Working Draft Report ST-09-0002 8 (March 24, 2009), available at http://www.theguardian.com/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection
258 See supra Part I.A.
260 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, 22 WIRED 62, 66, (Feb. 2014).
262 Id. at 45-55.
unconstitutional. 263 In contrast, Judge Pauley of the Southern District of New York held that the program was constitutional under the controlling precedent of Smith. 264 So 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 email communications and their brethren are not protected from any state scrutiny: they will not just be subject to the relatively non-intrusive scanning of metadata, but to individualized content analysis.

Third, 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; that is true of all police investigations that are categorized as non-searches. While 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 police investigation is categorized as a non-search, Fourth Amendment protections do not apply at all. The NSA controversy is just a high-profile example of what the police have long been able to do in investigations not categorized as searches.

V. Conclusion

Throughout Fourth Amendment law, it is assumed that requiring the police to obtain a warrant for an investigation will do great harm to the ability of the police to solve crime and prosecute criminals. This Assumption exists in debates about the search/non-search distinction, possible exceptions to the warrant requirement, and about the warrant requirement itself. Yet it is often not true.

In some situations, the police 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 police detection, requiring the police to obtain a warrant will do little or no harm to police investigations in many cases. Reduced costs of police investigation will incentivize criminals to innovate more often. This increased innovation will often completely offset the gains that police receive by not having to obtain a warrant.

Other than differences in constitutional interpretation,265 the main argument made in favor of doing away with the warrant requirement is that it makes police work much more difficult.266 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 the police do not have to work as hard to investigate them. 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, the police will often realize no gain when an investigation is termed a non-

265 Amar, supra note 40, at 438.
search or otherwise not requiring a warrant. 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.