If a Tree Falls: Bulk Surveillance, the Exclusionary Rule, and the Firewall Loophole

Carrie Leonetti*

I. INTRODUCTION

The Supreme Court's current attenuation doctrine for the Fourth Amendment exclusionary rule has created a "firewall loophole" that police can use, even intentionally, to engage in illegal searches and seizures with immunity from suppression and most likely, without detection. Up until now, my scholarship on digital privacy has focused on constitutional issues relating to the "fit" between modern technology and traditional legal doctrines including bulk data-mining programs like the National Security Agency ("NSA")'s Prism program, taking the position that it is questionable whether they are unconstitutional under *Smith v. Maryland*.[1] This Article seeks to answer two different but related questions: first, assuming that bulk digital surveillance does violate the Fourth Amendment, does it necessarily follow that its fruits must be suppressed and second, if the Fourth Amendment does not require their suppression, what role might Congress play in doing so? In answering these questions, this Article makes a normative assumption, defended in my earlier Article, that pervasive-surveillance programs ("dragnets") like Prism are undesirable and should be deterred.[2]

II. SUPPRESSING "IDENTITY"

A. *Derivative Evidence*

The Fourth Amendment exclusionary rule applies not only to evidence derived directly from illegal investigation ("the primary illegality"), but also to secondary evidence (the "fruit of the poisonous tree"). Textbook examples of this

* Associate Professor, Wayne Morse Resident Scholar, University of Oregon School of Law. The author thanks Jenna Royce for her research assistance, Margaret Hallock, Rebecca Flynn, and the Morse Center for their support, Margie Paris, Leslie Harris, Liz Tippets, Michael Fakhri, Suzanne Rowe, Roberta Mann, and Stuart Chinn for their thoughtful insights, and especially Ofer Raban, for his enthusiastic criticism, which, as usual, did not convince me, but did sharpen my arguments.

[1] 442 U.S. 735 (1979). *See* Carrie Leonetti, *Bigfoot: Data Mining, the Digital Footprint, and the Constitutionalization of Inconvenience*, 15 J. HIGH TECH. L. 260 (2015).

[2] *See id*. at 270.

include using an illegal wiretap to obtain a search warrant[3] or inducing a confession by confronting a suspect with illegally obtained evidence.[4]

While ordinarily the exclusionary rule requires suppression of these secondary forms of evidence, the Government can defeat its application by proving that the causal connection between the primary illegality and the subsequent evidence is sufficiently attenuated.[5] This is a question of causation, the sufficiency of the nexus between the initial illegality and the evidence subsequently obtained.

Increasingly, the Supreme Court or at least a majority of it, has been uncomfortable with and even hostile to the suppression of secondary evidence, drawing the attenuation line ever closer to the illegal police conduct and requiring a greater causal nexus between the illegal investigation and its subsequent fruits, particularly through the development of the independent-source and inevitable-discovery doctrines.[6] In *Hudson v. Michigan*,[7] for example, the Court held that the exclusionary rule was inapplicable to "knock and announce" violations. Justice Scalia, writing for the majority, reached this conclusion in part because he deemed there to be no causal connection between the unlawful entry (without knocking and announcing) and the resulting evidence.[8] In doing so, he announced:

---

[3] *See, e.g.*, Carter v. State, 337 A.2d 415 (Md. 1975) (holding that information garnered through an illegal wiretap could not be used to issue a search warrant).

[4] *See, e.g.*, United States v. Timmann, 741 F.3d 1170 (11th Cir. 2013) (suppressing Timmann's telephonic admissions because they were the direct result of agents exploiting evidence obtained from an illegal search); United States v. Cotton, 722 F.3d 271, 272 (5th Cir. 2013) (suppressing Cotton's admissions "made immediately on the heels of the unlawful search and discovery of drugs"); United States v. $186,416.00 in U.S. Currency, 590 F.3d 942 (9th Cir. 2010) (suppressing a suspect's incriminating declaration of ownership of seized currency made in an application seeking its return because the seizure was the product of an illegal search); United States v. Davis, 323 F.3d 1163 (9th Cir. 2003) (suppressing Davis's admission that he possessed a shotgun as the fruit of the prior illegal search of his gym bag that led to the discovery of the gun); United States v. Nafzger, 965 F.2d 213 (7th Cir. 1992) (suppressing Nafzger's admission that he knew that a truck was stolen when it was made immediately after agents discovered the truck in an illegal search); United States v. Parker, 722 F.2d 179 (5th Cir. 1983) (suppressing Parker's statements five months after an illegal search because agents exploited the evidence illegally obtained in the search to induce it).

[5] *See* United States v. Ramirez, 523 U.S. 65, 72, n.3 (1998) (explaining that the exclusionary rule depended on a "sufficient causal relationship" between unlawful conduct and discovery of evidence); Wong Sun v. United States, 371 U.S. 471, 484–88 (1963) (defining attenuation as when evidence derived from a violation of the Fourth Amendment results from "means sufficiently distinguishable to be purged of the primary taint"); Nardone v. United States, 308 U.S. 338, 340–41 (1939) (holding that when discovery of secondary evidence occurs after the effect of the primary illegality became "attenuated," the causal chain has been broken).

[6] *See* Nix v. Williams, 467 U.S. 431 (1984) (adopting the independent-source and inevitable-discovery doctrines).

[7] 547 U.S. 586 (2006).

[8] *See id*. at 592.

> [E]xclusion may not be premised on the mere fact that a constitutional violation was a "but-for" cause of obtaining evidence. Our cases show that but-for causality is only a necessary, not a sufficient, condition for suppression. In this case, of course, the constitutional violation of an illegal manner of entry was not a but-for cause of obtaining the evidence. Whether that preliminary misstep had occurred or not, the police would have executed the warrant they had obtained, and would have discovered the gun and drugs inside the house.[9]

B. *Illegal Arrests*

There is a line of cases dealing with the consequences of illegal arrests that later give rise to criminal charges, which are independent of, but related to, the attenuation doctrine. If a suspect is arrested illegally (e.g., in the absence of probable cause) and searched incident to that arrest, the Fourth Amendment dictates that the fruits of that search be suppressed.[10] Similarly, if a suspect is arrested illegally and as a direct result of that arrest makes incriminating statements, the Fourth Amendment dictates that those statements be suppressed.[11] If however, the illegal arrest does not directly result in any incriminating evidence—if the police for example, arrest a defendant before they have probable cause to do so, but later develop probable cause without relying on any fruits of the initial arrest—the defendant cannot "suppress" the prosecution.[12]

The parameters of this doctrine are illustrated by a pair of cases: *Davis v. Mississippi*[13] and *United States v. Crews*.[14] In *Davis*, during a rape investigation,

---

[9] *Id.*

[10] *See, e.g.*, Davis v. Mississippi, 394 U.S. 721 (1969) (suppressing Davis's fingerprints, taken during his illegal arrest, which "matched" fingerprints at the crime scene); Kremen v. United States, 353 U.S. 346 (1957) (suppressing evidence seized after Kremen's illegal arrest).

[11] *See* Taylor v. Alabama, 457 U.S. 687 (1982); Brown v. Illinois, 422 U.S. 590 (1975).

[12] *See* Payton v. New York, 445 U.S. 573 (1980) (holding that Payton's indictment need not be dismissed even though his arrest violated the Fourth Amendment); United States v. Crews, 445 U.S. 463 (1980) (holding that the illegality of Crews's arrest did not require suppression of evidence untainted by police misconduct); Frisbie v. Collins, 342 U.S. 519 (1952); *see also* Ker v. Illinois, 119 U.S. 436 (1886) (holding that Ker could not challenge his conviction on the ground that he was illegally extradited from Peru for trial). The only exception to this general rule is that a court can dismiss a prosecution under the Due Process Clause, if the Government engages in conduct so outrageous that it "shocks the conscience." *See, e.g.*, United States v. Marshank, 777 F. Supp. 1507 (N.D. Cal. 1991) (dismissing narcotics charges because the Government collaborated with Marshank's attorney during his investigation and prosecution); *cf.* Rochin v. California, 342 U.S. 165 (1952) (holding that forcibly pumping Rochin's stomach to obtain morphine capsules for trial evidence so offended prevailing notions of fairness that it invalidated his conviction).

[13] 394 U.S. 721 (1969) (holding that fingerprints taken during Davis's illegal detention had to be suppressed).

[14] 445 U.S. 463 (1980) (holding that a complaining witness's in-court identification of Crews did not have to be suppressed as the fruit of his unlawful arrest).

the police conducted an illegal dragnet of young black men, taking their fingerprints for comparison to one left at the crime scene. Davis's fingerprint, taken during his illegal arrest, matched the crime-scene print. When he moved to suppress his fingerprint as the fruit of his unlawful seizure, the Supreme Court agreed.

In *Crews*, during an investigation of a string of robbery-assaults in women's restrooms, Crews was arrested without probable cause, photographed, and released. The police showed his arrest photo to a victim and she identified him as her assailant. Prior to trial, the court suppressed the pretrial identification of Crews, but denied Crews's motion to dismiss and permitted the victim to identify him at trial. The Supreme Court affirmed, holding that the in-court identification did not have to be suppressed because it was sufficiently attenuated from the illegal arrest and pretrial identification. The Court also held that the denial of the motion to dismiss was proper because Crews's identity was not the "fruit" of his unlawful arrest.

A narrow reading of Crews suggests that the Court simply misunderstood the cognitive science surrounding eyewitness identification—i.e., that a subsequent identification can never be "independent" of a prior tainted one.[15] A broader reading of Crews however, suggests the beginning of a doctrinal exception to the fruit-of-the-poisonous tree doctrine for evidence of "identity."

This doctrine governing the remedy (or lack thereof) for illegal arrests from which no trial evidence is derived arises in the context of the prompt-presentment requirement—or, more precisely, in the context of violations of the requirement. For example, in *Gerstein v. Pugh*,[16] in which the Court held that the Fourth Amendment required that defendants arrested without a warrant or grand-jury indictment were entitled to a "prompt" judicial determination of probable cause, the Court reiterated that "illegal arrest or detention does not void a subsequent conviction."[17] Fifteen years later, in *Riverside Co. v. McLaughlin*,[18] the Court defined "prompt," adopting a presumptive forty-eight-hour rule.[19] One practical effect of *Pugh* and *McLaughlin* has been that, while, doctrinally, probable cause is required prior to arrest, as a practical matter, it is not necessary that the State have probable cause until approximately forty-eight hours after arrest—i.e., that the police can "build" probable cause in the forty-eight hour period between a warrantless arrest and presentment of the suspect without consequence, because

---

[15] *See* Kathryn Segovia, *et al.*, *Virtual Human Identification Line-ups*, *in* CRANIOFACIAL IDENTIFICATION 101 (Caroline Wilkinson et al. eds., 2012) (discussing accuracy concerns with eyewitness-identification procedures).

[16] 420 U.S. 103 (1975) (holding unconstitutional procedures under which suspects arrested without a warrant could remain in custody for thirty days or more without a judicial determination of probable cause).

[17] *Id*. at 119.

[18] 500 U.S. 44 (1991).

[19] *See id*. at 56.

the premature arrest does not result in a dismissal, only suppression of evidence obtained as a result of the period of delay. Typically, this evidence caused is limited to two classes: (1) the defendant's confession, if there is one and if it occurred during the period of unreasonable delay;[20] and (2) evidence relating to the defendant's "identity," which generally means fingerprints (and resulting criminal-history information, if any).

C. *Identification of Suspects*

One result of the expansion of the concept of attenuation, in conjunction with these cases holding that dismissal is not the consequence of illegal arrest, has emerged in the context of illegal arrests that result in the identification of suspects, the constitutional consequences of which have befuddled judges ever since the Supreme Court penned the following sentence in *I.N.S. v. Lopez-Mendoza*:[21] "The 'body' or identity of a defendant . . . in a criminal . . . proceeding is never itself suppressible as a fruit of an unlawful arrest, even if it is conceded that an unlawful arrest, search, or interrogation occurred."[22] *Lopez* involved two Mexican citizens caught up in putatively illegal arrests by the Immigration and Naturalization Service ("INS"). During their arrests, they admitted to being undocumented. The INS used their admissions in their subsequent deportation hearings, over their objections. On appeal, the Court reached two holdings. The primary one was that the Fourth Amendment exclusionary rule did not apply in civil deportation hearings. The secondary one was somewhat more cryptic. The Court held that the illegality of the arrests was irrelevant to the subsequent deportation hearings. It is in the context of this second holding that the Court penned the cryptic sentence above.

Post-*Lopez*, the question arises: what if an illegal arrest leads to the discovery of a suspect's fingerprints, which then leads to the discovery of other evidence—for example, the suspect's immigration file or criminal history—to be used at trial? A narrow reading of the second holding of *Lopez* would be consistent with earlier cases like *Payton v. New York*[23] and *Crews*, standing merely for the uncontroversial proposition that the illegality of an arrest does not deprive a court of jurisdiction over a subsequent criminal charge, and would not bar suppression of this evidence. Relying on a broader reading of *Lopez* however, some federal circuits refuse to suppress the discovery not only of a defendant's "identity," but

---

[20] *See* 18 U.S.C. § 3501(c) (1968) (providing that a confession made while a defendant is "under arrest or other detention in the custody of any law-enforcement officer or law-enforcement agency, shall not be inadmissible solely because of delay in bringing such person before [a judicial officer]" if it was made voluntarily and "within six hours" following arrest).

[21] 468 U.S. 1032 (1984).

[22] *Id*. at 1039.

[23] 445 U.S. 573 (1980).

also of evidence related to it, usually fingerprints, even when it is the "fruit" of the illegal arrest.[24]

For example, in *United States v. Navarro-Diaz*,[25] Navarro was illegally arrested during a drug bust and provided a fake identity card. The search conducted incident to his arrest turned up his real identity card. When the police confronted Navarro with the real card, he admitted that it was his and that the name and date of birth were accurate. Navarro's real name and birthdate led agents to his immigration file, and the Government charged him with returning to the United States illegally after a previous deportation.[26] Navarro moved to suppress the evidence of his "identity" as fruits of his illegal detention. On appeal, the Sixth Circuit upheld the denial of his motion because "identity cannot be suppressed" under *Lopez*.[27]

The Ninth Circuit reached a similar result in *United States v. Del Toro Gudino*.[28] Del Toro was stopped illegally and gave agents a fake name and date of birth. When they confronted him with the fact that they could not find an immigration file associated with the identity that he had given, he admitted to being undocumented. The fingerprints and photograph taken during his arrest led agents to his immigration file, which showed that he had previously been removed from the United States. When the Government charged him with illegally returning after that prior removal, he moved to suppress his fingerprints, photograph, and statements about his "identity" as fruits of his illegal arrest. On appeal, the Ninth Circuit affirmed the denial of his motion to suppress, reasoning that under *Lopez*, when an illegal arrest led only to the disclosure of a defendant's "identity," evidence of that identity could not be suppressed.[29]

Other circuits have limited the holding in *Lopez* to challenges to a court's jurisdiction over a defendant, rather than more broadly prohibiting the suppression

---

[24] *See* United States v. Navarro-Diaz, 420 F.3d 581, 588 (6th Cir. 2005) (interpreting *Lopez* as barring suppression of evidence of Navarro's "identity" stemming from his illegal arrest); United States v. Bowley, 435 F.3d 426, 430–31 (3d Cir. 2006) (same); United States v. Roque-Villanueva, 175 F.3d 345, 346 (5th Cir. 1999) (same).

[25] 420 F.3d 581.

[26] *See* 8 U.S.C. § 1326 (1947) (criminalizing an alien's being "found in" the United States subsequent to a prior "removal").

[27] *Navarro-Diaz*, 420 F.3d at 588.

[28] 376 F.3d 997 (9th Cir. 2004).

[29] *See id*. at 1000–01.

of derivative evidence of identity.[30] Not to be outdone, the Ninth Circuit has issued reported opinions subscribing to both sides of the debate.[31]

Even in the circuits that read *Lopez* narrowly and suppress fingerprints and documentary evidence discovered as a result of illegal arrests, suppression of the derivative evidence would not prevent the Government from obtaining this evidence from an independent source by fingerprinting the defendant again, assuming that it had probable cause to do so without the suppressed evidence. This would simply be the application of *Crews* to fingerprints and/or the answer to the question not addressed in *Davis* (whether Mississippi could have refingerprinted him if it had probable cause, independent of the prior arrest). Even if the Government lacked probable cause for new prints, it could follow a defendant out of the courtroom and conduct the considerable surveillance available to it without probable cause, reasonable suspicion, or a warrant. The combination of *Whren v. United States*[32] and *Atwater v. City of Lago Vista*,[33] standing alone, almost guarantees that police can fingerprint any suspect if they want to. They just need to wait until their suspect rolls a stop sign or fails to signal a lane change.

III. THE FIREWALL DILEMMA:

A. *Thought Experiment*

These suppression-of-"identity" cases typically arise in the context of immigration prosecutions, but there is nothing doctrinally cabining them there. When placed in the context of national security and bulk high-tech surveillance, they give rise to an interesting thought experiment.

---

[30] *See* United States v. Olivares-Rangel, 458 F.3d 1104 (10th Cir. 2006) (holding that *Lopez* did not bar suppression of Olivares-Rangel's "identity" stemming from his illegal arrest); United States v. Guevara-Martinez, 262 F.3d 751, 754 (8th Cir. 2001) (upholding suppression of Guevara-Martinez's fingerprints, obtained after his illegal arrest and interpreting *Lopez* to refer only to jurisdictional challenges).

[31] *Compare Del Toro Gudino*, 376 F.3d at 1001 ("[W]ho a defendant is cannot be excluded, regardless of the nature of the violation leading to his identity."), *and* United States v. Orozco-Rico, 589 F.2d 433, 435 (9th Cir. 1978) ("[T]here is no sanction to be applied when an illegal arrest only leads to discovery of the man's identity and that merely leads to the official file or other independent evidence." (quoting Hoonsilapa v. INS, 575F.2d 735, 738 (9th Cir. 1978))), *with* United States v. Manzo-Jurado, 457 F.3d 928, 940 (9th Cir. 2006) (holding that neither the "insuppressible nature of identity evidence" nor the inevitable-discovery doctrine justified the admission of identity documents obtained during Manzo's suspicionless stop); United States v. Garcia-Beltran, 389 F.3d 864, 867–68 (9th Cir. 2004) (holding that *Lopez* did not bar suppression of evidence of Garcia-Beltran's "identity" stemming from his illegal arrest).

[32] 517 U.S. 806 (1996) (upholding pretextual traffic stops as long as officers could articulate probable cause for some offense).

[33] 532 U.S. 318 (2001) (holding that the Fourth Amendment did not prohibit warrantless arrests for any offense, no matter how minor).

First, imagine that an agency like the NSA is engaging in patently unconstitutional surveillance: in addition to tracking the metadata of Americans' telephone and e-mail communications, monitoring their Internet usage (check-ins, geo-tagged photographs, tweets, and movie-viewing histories on Google, Facebook, Twitter, YouTube, and Netflix), and collecting and analyzing commercial and governmental data (travel records, credit card transactions, insurance information, passenger manifests, voter registration rolls, and tax data), it is also listening to the contents of all phone conversations,[34] reading the full text of all e-mails[35] and text messages, and monitoring lawyers and journalists, all without individualized suspicion or court authorization (search warrants, FISC orders), in violation of the Fourth Amendment.

Second, imagine that the NSA does not share either the course or the results of its surveillance with the Federal Bureau of Investigation ("FBI"). Instead, a "firewall" is built between the two agencies. When the NSA illegally intercepts and analyzes information, concluding that an individual is participating or about to participate in a serious crime, the only piece of information that it shares over the firewall is the suspect's name. "Pssst, you should check out Carrie Leonetti." (Please don't.)

Third, imagine that the FBI takes only the name of the suspect generated by the NSA and begins legal surveillance of that person, which, under the Court's current jurisprudence, could be quite extensive even without probable cause or a search warrant. The FBI attaches a pen register to the suspect's phone(s),[36] collects metadata from electronic communications,[37] "pings" the suspect's phone[38] or obtains tower location information from his/her cell company,[39] follows the suspect on public roads[40] or from the air[41] observing everything that s/he does in

---

[34] *See* Katz v. United States, 389 U.S. 347 (1967) (reversing Katz's conviction for transmitting wagering information over the telephone because the police obtained the evidence to convict him by electronically eavesdropping without a warrant, on the pay phone that he used).

[35] *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (holding that the Fourth Amendment applied to e-mails sent through commercial internet service providers).

[36] *See* Smith v. Maryland, 442 U.S. 735, 743–46 (1979) (holding that Smith lacked a reasonable expectation of privacy in the phone numbers that he dialed from his home telephone).

[37] *See* Leonetti, *supra* note 1.

[38] *See* United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012) (holding that "pinging" Skinner's cell phone did not infringe on his reasonable expectation of privacy in his location).

[39] While police frequently obtain phone location data from telecommunication companies without a warrant and occasionally use cell-phone "scanners" to search phone data surreptitiously during traffic stops, the few lower courts to weigh in have been divided over the constitutionality of the practices. *Compare In re* Application of U.S. for an Order Directing a Provider of Elec. Commc'n Serv. to Disclose Records, 620 F.3d 304 (3d Cir. 2010) (holding that the Government did not need a warrant to require a cellular service provider to produce customer location history), *with* State v. Earls, 70 A.3d 630, 631 (N.J. 2013) (holding that the New Jersey Constitution required the police to get a warrant before obtaining cell-location information).

"plain view," seizes the suspect's garbage after it is left out for collection,[42] picks up "abandoned" DNA, fingerprints, etc.,[43] goes to the suspect's home and performs a "knock and talk," asking the suspect questions, observing at least the entryway of the suspect's home, and asking the suspect to consent to searches,[44] engages in a noncustodial interrogation of the suspect.[45] Based on these legal warrantless forms of investigation, the FBI develops probable cause "independent" of the NSA's illegal surveillance, which then provides the justification for warrants to search premises and seize evidence, for biological evidence,[46] wiretaps,[47] and thermal imaging of the suspect's home[48] or for arrest and custodial interrogation, all of which gives rise to the probable cause required to prosecute (and the proof beyond a reasonable doubt to convict) the suspect.

---

[40] *See* United States v. Knotts, 460 U.S. 276, 281 (1983) (holding that a person "traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."). Justice Alito explained the distinction between live surveillance and GPS tracking during the oral arguments in *United States v. Jones*. *See* Transcript of Oral Argument at 10, United States v. Jones, 132 S. Ct. 945 (2012) (No. 10-1259), 2011 WL 5360051, at *10.

[41] *See* California v. Ciraolo, 476 U.S. 207, 213–15 (1986) (holding that Ciraolo's backyard marijuana garden was in plain view when officers spotted it from a helicopter 1,000 feet overhead); Dow Chem. Co. v. United States, 476 U.S. 227, 240 (1986) (holding that enhanced visual surveillance via aerial photographs from navigable airspace was not a search).

[42] *See* California v. Greenwood, 486 U.S. 35, 40 (1988) (holding that Greenwood had no reasonable expectation of privacy in the trash left at her curb for city collection).

[43] *See* Maryland v. King, 133 S. Ct. 1958 (2013) (upholding the constitutionality of warrantless DNA collection upon arrest for violent felonies); People v. Thomas, 200 Cal. App. 4th 338 (Dist. Ct. App. 2d. 2011) (holding that Thomas abandoned any privacy interest in his DNA when he failed to wipe his saliva off of a breath-test device); People v. Gallego, 190 Cal. App. 4th 388, 396 (Dist. Ct. App. 3d. 2010) (The "cigarette butt, like the trash bags in *Greenwood*, was left in a place 'particularly suited for public inspection.' Defendant thus abandoned the cigarette butt in a public place, and therefore had no reasonable expectation of privacy concerning the DNA testing of it to identify him as a suspect."); Williamson v. State, 413 Md. 521 (Ct. App. 2010) (holding that the Fourth Amendment did not apply to the warrantless collection of DNA from a cup that Williamson abandoned on the floor of his holding cell); State v. Athan, 158 P.3d 27, 37 (Wash. 2007) ("Police may surreptitiously follow a suspect to collect DNA, fingerprints, footprints, or other possibly incriminating evidence, without violating that suspect's privacy.").

[44] *See* Washington v. Chrisman, 455 U.S. 1 (1982) (holding that an officer lawfully in a student's room could seize marijuana seeds and a pipe in plain view).

[45] *See* Florida v. Bostick, 501 U.S. 429 (1991) (holding that encounters in which a reasonable person would feel free to disregard the police and go about his/her business were consensual and did not need reasonable suspicion).

[46] *See* Skinner v. Railway Labor Execs' Ass'n, 489 U.S. 602 (1989) (holding that the Fourth Amendment applied to breath and urine tests); Schmerber v. California, 384 U.S. 757, 770 (1966) (holding that the Fourth Amendment applied to "searches involving intrusions beyond the body's surface").

[47] *See* 18 U.S.C. § 2510, (2010) (prohibiting the interception, disclosure, and use as evidence of oral, wire, and electronic communications without a court order)*;* 18 U.S.C. § 3121 (2010) (prohibiting the use of pen-register or trap-and-trace devices without a court order).

[48] *See* Kyllo v. United States, 533 U.S. 27, 40 (2001) (holding that thermal imaging into a home was a search, even though it did not involve a "physical intrusion").

IV. INADEQUACY OF THE FOURTH AMENDMENT EXCLUSIONARY REMEDY

Finally, imagine that the suspect, now defendant, moves to suppress the evidence that the FBI has amassed on the ground that it was derived from the NSA's earlier illegal surveillance. Under *Lopez* and *Payton*, the motion would be denied, and the denial would be affirmed on appeal. In the terminology of current exclusionary-rule jurisprudence, the causal chain between the primary illegality (the NSA's secret surveillance) and the derivative evidence (from the FBI's legal investigation) would be sufficiently "attenuated," even though the FBI would never have focused on the suspect without the name from the NSA.

The problem is not that the Fourth Amendment would not prohibit the NSA's illegal surveillance; the problem is that the exclusionary rule, as the Court understands it, would not be an adequate remedy for it. Even though the Court's recent decisions in *United States v. Jones*[49] (GPS tracking), *Florida v. Jardines*[50] (dog sniffs), and *Riley v. California*[51] (cellular data) are promising in terms of its willingness to expand Fourth Amendment protections along with expansions of high-tech surveillance capabilities, those cases do not change the exclusionary-rule calculus. As long as none of the evidence gathered by the NSA is used against the defendant at trial (which is unnecessary once the FBI's "independent" legal investigation generates its own evidence), the defendant has no remedy, at least in the criminal case, for the violation.[52]

In fact, the NSA's illegal surveillance in the hypothetical scenario would likely go undetected, except perhaps for a nagging question about why the FBI began to focus on the defendant in the first instance, a question that frequently goes unanswered even in criminal cases in which the investigation begins legally (e.g., because of information from a confidential informant). In federal court, there are two primary sources of defense discovery: Rule 16 of the Federal Rules of Criminal Procedure and Due Process. In national-security cases, the Foreign Intelligence Surveillance Act ("FISA")[53] also grants the defendant the right to disclosure of certain electronic surveillance.

Rule 16 requires the Government to disclose the defendant's statements, criminal record, and certain objects that it intends to introduce at trial.[54] Since the

---

[49] 132 S. Ct. 945 (2012) (holding that installing a GPS device on Jones's vehicle and monitoring its public movements without a valid warrant constituted a search).

[50] 133 S. Ct. 1409, 1413 (2013).

[51] 134 S. Ct. 2473 (2014) (holding that a valid search incident to arrest did not extend to a suspect's phone data).

[52] *See* Sibron v. New York, 392 U.S. 40 (1968) (refusing to permit Sibron to raise a facial challenge to the constitutionality of New York's stop-and-frisk law).

[53] 50 U.S.C. § 1801 (1978).

[54] *See* FED. R. CRIM. P. 16 (a).

results of the secret NSA spying in the hypothetical scenario are, by definition, secret and unintended for use at trial, Rule 16 would confer no right of disclosure.

Brady v. Maryland and its progeny require the Government to disclose evidence that may be favorable to the defense,[55] including evidence in the possession of investigating law-enforcement agencies.[56] Evidence is "favorable" if it tends to demonstrate innocence, mitigate sentence, or undercut the credibility of prosecution witnesses (e.g., evidence that a witness received or expected consideration in exchange for testimony or was dishonest on a prior occasion).[57] Returning to the hypothetical scenario, it is hard to imagine how anything that the illegal NSA investigation revealed would meet these definitions. On the contrary, the results of the secret, illegal investigation would likely be more damning to the defendant. Evidence may also be favorable if it tends to support a pretrial motion, such as a motion to suppress the fruits of an illegal search. Because there is no exclusionary remedy for illegal investigations that do not result in trial evidence (but rather merely result in the identification of a suspect) the defendant would not be entitled to disclosure of the illegal investigation on this ground, either.[58]

Recent national-security cases exemplify these discovery obstacles. In *United States v. Moalin*,[59] the Government charged Moalin with providing material support to terrorists and related offenses.[60] Moalin moved to suppress wiretap evidence obtained pursuant to a warrant.[61] The motion challenged the Government's use of electronic surveillance pursuant to Title I of FISA[62] and the FISA Amendments Act.[63] Moalin requested that his attorney, who possessed the appropriate security clearances, be granted access to the FISA warrant applications

---

[55] *See* Brady v. Maryland, 373 U.S. 83, 87 (1963) ("[S]uppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.").

[56] *See* Youngblood v. West Virginia, 547 U.S. 867, 869–70 (2006) (explaining that *Brady* applies to any evidence known to police investigators, even if the prosecutor is not aware of the existence of the evidence, because prosecutors have a duty to discover any favorable evidence known to others acting on their behalf); Kyles v. Whitley, 514 U.S. 419, 437 (1995) (explaining that prosecutors have a duty to learn of any favorable evidence known to others acting on their behalf in the case, including the police).

[57] *See* United States v. Bagley, 473 U.S. 667 (1985); Giglio v. United States, 405 U.S. 150 (1972) (clarifying that "favorable" evidence included evidence that tended to impeach prosecution witnesses).

[58] *See* Moore v. Illinois, 408 U.S. 786, 795 (1972) ("We know of no constitutional requirement that the prosecution make a complete and detailed accounting to the defense of all police investigatory work on a case.").

[59] No. 10cr4246 JM., 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013) (holding that the NSA's warrantless collection of international "telephony metadata" was legal because Moalin lacked a reasonable expectation of privacy in it).

[60] *See id*. at *1.

[61] *See id*.

[62] 50 U.S.C. § 1806 (1978).

[63] 50 U.S.C. § 1881 (2008).

and pertinent orders of the Foreign Intelligence Surveillance Court [FISC], arguing that the electronic surveillance was obtained in violation of FISA and the First and Fourth Amendments and seeking disclosure pursuant to *Brady* and Rule 16.[64] In the alternative, Moalin requested that the court perform an *in camera* review of the documents, pursuant to the Classified Information Procedures Act.[65] The Court rejected Moalin's discovery request and denied his motion to suppress because it found that he did not have a colorable Fourth Amendment challenge to the surveillance that would render disclosure favorable to the defense.[66]

In *United States v. Mohamud*, the Portland "Christmas Tree Bomber" was convicted of attempting to use a weapon of mass destruction.[67] At Mohamud's initial appearance, the Government provided notice that it intended to use evidence obtained under FISA.[68] Prior to trial, Mohamud moved to suppress information seized from his computer and cell phone.[69] He also moved for disclosure of the details of the FISA searches.[70] Almost a year after Mohamud's trial, the Government filed a Supplemental FISA Notification, notifying Mohamud:

> "This supplemental notice is being filed as a result of the government's determination that information obtained or derived from Title I FISA collection [domestic electronic surveillance] may, in particular cases, also be "derived from" prior Title VII FISA collection [foreign intelligence gathering]. . . . [T]he United States hereby provides notice . . . that the government has offered into evidence or otherwise used or disclosed in proceedings, including at trial, in the above-captioned matter information derived from acquisition of foreign intelligence information . . . ."[71]

In other words, Mohamud's communications with foreign intelligence targets abroad had been incidentally intercepted during the NSA's surveillance of them, the discovery of those communications made Mohamud the subject of domestic surveillance through analysis of his telephone metadata, and the metadata collection (in conjunction with the foreign communications) led to the FBI sting operation, which produced the evidence used at trial.

---

[64] *See Moalin*, 2013 WL 6079518, at *1.

[65] 18 U.S.C. app. §§ 3, 4 (1980). *See Moalin*, 2013 WL 6079518, at *2.

[66] *See Moalin*, 2013 WL 6079518, at *9.

[67] *See* United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *1 (D. Or. June 24, 2014).

[68] *See id*.

[69] *See* United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2012 WL 5208173, at *1 (D. Or. Oct. 22, 2012).

[70] *See* United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2012 WL 4594746 (D. Or. Oct. 2, 2012).

[71] *Mohamud*, 2014 WL 2866749, at *1.

When Mohamud, who had not yet been sentenced, received the supplemental notification, he challenged the constitutionality of the foreign intelligence gathering (the incidental collection of his communications during the surveillance of foreign targets) and what he presumed to have been (but was not disclosed as) his telephone-metadata collection under the Patriot Act,[72] from which the other evidence against him had been "derived," and requested discovery relating to the surveillance.[73] The court denied Mohamud's motion for discovery, as well as his motion to suppress the FISA evidence and its "fruits,"[74] reasoning: "[S]urveillance is not evidence—it produces evidence."[75]

In *United States v. Daoud*,[76] the Government charged Daoud with attempting to use a weapon of mass destruction and related offenses.[77] The indictment arose out of an FBI investigation after Daoud joined an e-mail conversation with two undercover FBI agents and discussed using explosives while engaging in "violent jihad," which led the agents to obtain surveillance warrants.[78] Daoud ultimately attempted to detonate a fake bomb, given to him by undercover agents, in downtown Chicago.[79]

Prior to trial, the Government notified Daoud that it intended to present evidence derived from electronic surveillance conducted under FISA.[80] Daoud moved for disclosure of the classified materials submitted in support of the government's FISA warrant applications to his attorneys, who held appropriate security clearances, in order to support a motion for a hearing under *Franks v. Delaware*,[81] to suppress the evidence obtained in violation of FISA.[82] The court granted the motion after an *in camera* review of the materials. On appeal, the Seventh Circuit reversed the order, holding that Daoud was not entitled to the FISA application to make his preliminary showing that it contained false statements by the agents who prepared it and holding, on the merits of the motion to suppress, that the investigation did not violate FISA.[83] Judge Rovner, in dissent, noted the somewhat perverse implications of this ruling:

---

[72] 50 U.S.C. § 1861 (2001).

[73] *See Mohamud*, 2014 WL 2866749, at *2, *14.

[74] *Id*. at *2.

[75] *Id*. at *6.

[76] 755 F.3d 479 (7th Cir. 2014).

[77] *See id*. at 480.

[78] *Id*.

[79] *See id*.

[80] *See id*.

[81] 438 U.S. 154, 155–56 (1978) (holding that Franks could challenge a search conducted pursuant to a warrant if it was procured by a knowing or reckless falsehood).

[82] *See Daoud*, 755 F.3d at 480–82.

[83] *See id*. at 484.

> "[N]otwithstanding the presumed applicability of *Franks* to the FISA framework, defendants in FISA cases face an obvious and virtually insurmountable obstacle in the requirement that they make a substantial preliminary showing of deliberate or reckless material falsehoods or omissions in the FISA application without having access to the application itself."[84]

V. AN EFFECTIVE REMEDY

A. *Congress to the Rescue?*

There are several ways that the Court could close the firewall loophole, if it were so inclined. One way would be to *tighten the attenuation doctrine*, replacing its proximate causation with but-for causation. The hypothetical consequence would be recognition of a direct and unbreakable line between the NSA's "discovery" of a suspect and the Government's prosecution of the same defendant,[85] but it is hard to imagine how the Court could cabin this change in the exclusionary rule solely in the firewall situation. A more sweeping doctrinal reform to the exclusionary rule, one not limited to the NSA hypothetical, seems unlikely in light of the Court's hostility to the concept of "tainted" evidence.[86]

Another possibility would be for the Court to carve out an exception to the attenuation and independent-source doctrines for digital or bulk surveillance, but these distinctions would also be doctrinally problematic. It is difficult to imagine a principled distinction between evidence derived from somewhat distant electronic surveillance and evidence derived from other forms of attenuated illegal investigations vis a vis the application of the exclusionary remedy. With regard to the bulk nature of the hypothetical surveillance, the Court has already rejected arguments that other forms of bulk surveillance (the "knock and talk"[87] random urine testing[88] roadblocks,[89] border searches,[90] searches in correctional facilities,[91]

---

[84] *Id*. at 490 (Rovner, J., dissenting).

[85] Re made a somewhat similar proposal advocating suppression based on due process. *See* Richard M. Re, *The Due Process Exclusionary Rule*, 127 HARV. L. REV. 1885 (2014).

[86] *See, e.g.*, Herring v. United States, 555 U.S. 135, 141 (2009) (asserting that the exclusionary rule imposed too high a price upon truth seeking); United States v. Calandra, 414 U.S. 338, 349–50 (1974) (describing the exclusionary rule's costs).

[87] *See* Kentucky v. King, 131 S. Ct. 1849, 1862 (2011) (holding that "knock and talks" were not searches because police were not doing "more than any private citizen might do").

[88] *See* Bd. of Educ. v. Earls 536 U.S. 822 (2002) (holding that drug testing students who participated in extracurricular activities did not violate the Fourth Amendment because it was designed to prevent drug use); Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 665 (1995) (upholding random urinalysis for student athletes because it was undertaken to protect children); Nat'l Treasury Emps. v. Von Raab, 489 U.S. 656 (1989) (upholding random drug testing of customs officers because the purpose was to ensure their fitness to handle firearms and interdict drugs).

and DNA databases[92]) are unconstitutional, let alone warrant special application of the exclusionary rule. On the contrary, in these cases, the existence of "special needs" and a "programmatic purpose" (rather than individualized suspicion) made them more, rather than less, palatable to the Court.[93]

A third option would be for the Court to carve out separate treatment for intentional violations of the Fourth Amendment and refuse to apply the attenuation doctrine to them, but doing so would be inconsistent with the Court's prior cases holding that the subjective intent of the police does not render an otherwise valid search or seizure unreasonable.[94] Conversely, however, the Court has ruled, in a variety of contexts, that the subjective intent of the police can render a warrantless search reasonable or the exclusionary rule inapplicable.[95] In other words, while

---

[89] *See* Michigan Dept. of State Police v. Sitz, 496 U.S. 444 (1990) (upholding drunk-driving checkpoints); United States v. Martinez-Fuerte, 428 U.S. 543 (1976) (upholding automobile checkpoints for illegal immigrants and contraband).

[90] *See* United States v. Flores-Montano, 541 U.S. 149 (2004) (holding that disassembly of a car's gas tank at the border did not require individualized suspicion); United States v. Montoya de Hernandez, 473 U.S. 531 (1985) (upholding routine searches and seizures at the border without probable cause or a warrant to collect duties and prevent introduction of contraband); United States v. Ramsey, 431 U.S. 606 (1977) (recognizing the "border search" exception to the Fourth Amendment).

[91] *See* Florence v. Bd. of Chosen Freeholders, 132 S. Ct. 1510 (2012) (holding that invasive strip searches of misdemeanor pretrial detainees without probable cause did not violate the Fourth Amendment because the purpose was to detect and deter possession of contraband in jail).

[92] *See* Maryland v. King, 133 S. Ct. 1958, 1972 (2013) (holding that collecting and searching DNA profiles in a database was not a search).

[93] *Cf.* Ferguson v. City of Charleston, 532 U.S. 67 (2001) (holding that a hospital's policy of testing pregnant patients' for drugs violated the Fourth Amendment because its purpose was to obtain evidence of cocaine use and report it to police).

[94] *See, e.g.*, Whren v. United States, 517 U.S. 806, 807 (holding that officers' motives, "*whatever* the subjective intent," were not relevant to a determination of probable cause or reasonableness); Horton v. California, 496 U.S. 128 (1990) (declining to require that the discovery of incriminating evidence by police be inadvertent in order for the plain-view exception to the warrant requirement to apply). *But see* City of Indianapolis v. Edmond, 531 U.S. 32 (2000) (holding that the city's warrantless drug interdiction checkpoints violated the Fourth Amendment in part because their purpose was crime control).

[95] *See, e.g.*, Davis v. United States, 131 S. Ct. 2419 (2011) (holding that the exclusionary rule did not apply to searches conducted in reasonable good-faith reliance on binding precedent subsequently overruled); Herring v. United States, 555 U.S. 135 (2009) (holding that the exclusionary rule did not apply to evidence obtained as the result of a negligent but unintentional bookkeeping error by the police); Arizona v. Evans, 514 U.S. 1 (1995) (holding that evidence seized in violation of Fourth Amendment as result of clerical errors of court employees fell within the good-faith exception to exclusionary rule); Maryland v. Buie, 494 U.S. 325 (1990) (holding that the Fourth Amendment permitted officers to conduct a warrantless protective sweep of a home during an arrest as long as it was conducted with the good-faith non-investigative purpose of ensuring officer safety); Colorado v. Bertine, 479 U.S. 367 (1987) (holding that warrantless inventory searches of automobiles administered in good faith satisfied the Fourth Amendment); United States v. Leon, 468 U.S. 897 (1984) (recognizing the "good-faith exception" to the Fourth Amendment exclusionary rule and holding that the rule did not apply to evidence obtained by officers in good-faith reliance on a search warrant later found to be invalid); South Dakota v. Opperman, 428 U.S. 364 (1976) (holding that the

good faith often inures to the benefit of a search, seizure, or subsequent use of derivative evidence, bad faith rarely inures to their detriment.

The only remaining remedy therefore, is a legislative one, targeted not at the attenuation doctrine in its entirety, but rather at a subset—the illegal surveillance of suspects that results in no direct evidence at trial. Unlike the Supreme Court, which must be wary of the future implications of its precedents,[96] Congress is free to adopt a statutory remedy irrelevant of doctrinal or intellectual consistency with the remainder of the Court's jurisprudence. Through a legislative remedy, Congress could decide the appropriate limits on bulk surveillance as a matter of policy, rather than relying on the courts, through constitutional analysis, to do so. Congress has the power, in this context: first, to adopt an exclusionary remedy for intentionally illegal investigations (or even high-tech bulk surveillance in its entirety) that does not require proximate cause between the illegality and evidence derived from it but instead has a temporal or but-for nexus or a subject-matter trigger; and, second, to enact a statutory discovery mechanism requiring the Government to reveal the results of any investigation that led to the defendant becoming a suspect, irrelevant of whether it intends to use those results at trial or whether they are favorable to the defense.

There has been a longstanding debate among jurisprudence scholars and political scientists about the relative effectiveness and appropriateness of courts versus legislatures in furthering social and political change.[97] In the context of

---

warrantless inventory search of Opperman's impounded automobile was not an "unreasonable" search in violation of the Fourth Amendment as long as the officers conducted it in the good-faith absence of an investigatory motive).

[96] *See* Planned Parenthood v. Casey, 505 U.S. 833, 864 (1992) ("[A] decision to overrule should rest on some special reason over and above the belief that a prior case was wrongly decided."); Vasquez v. Hillery, 417 U.S. 254, 268 (1986) (explaining the importance of adhering to precedent); *see also* Hilton v. South Carolina Public Railways Comm'n, 502 U.S. 197, 202 (1991) (explaining that the obligation to precedent has special force when it has given rise to settled expectations).

[97] The original protagonist in the debate was Gerald Rosenberg. *See* GERALD N. ROSENBERG, THE HOLLOW HOPE: CAN COURTS BRING ABOUT SOCIAL CHANGE? (2nd ed.1991) (arguing that the nature of constitutional rights is limited, courts are fundamentally conservative, and they lack tools to enforce decisions that are out of step with social mores); Gerald N. Rosenberg, *Hollow Hopes and Other Aspirations: A Reply to Feeley and McCann*, 17 L. & SOC. INQUIRY 761, 776 (1992); *see also* Robert A. Dahl, *Decision-Making in A Democracy: The Supreme Court as a National Policy-Maker*, 50 EMORY L. J. 563, 578 (2001) ("[I]t would appear on political grounds, somewhat unrealistic to suppose that a Court whose members are recruited in the fashion of Supreme Court Justices would long hold to norms of Right or Justice substantially at odds with the rest of the political elite."); Mark A. Graber, *Resolving Political Questions into Judicial Questions: Tocqueville's Thesis Revisited*, 21 CONST. COMMENTARY 485 (2004) (describing the limited ability of courts to resolve political issues through constitutional adjudication); Jeremy Waldron, *The Core of the Case Against Judicial Review*, 115 YALE L.J. 1346, 1376–86 (2006) (arguing that there are "important outcome-related defects in the way [that] courts approach rights"). Other scholars have taken the opposite position. *See, e.g.*, JEFFREY ROSEN, THE MOST DEMOCRATIC BRANCH: HOW THE COURTS SERVE AMERICA (2006); *see also* GEORGE I. LOVELL, LEGISLATIVE DEFERRALS: STATUTORY AMBIGUITY, JUDICIAL POWER, AND AMERICAN DEMOCRACY (2003) (arguing that courts step into the breach intentionally left to them by

high-tech surveillance, however, a legislative solution is not unprecedented. The two actions proposed in this Article (a statutory exclusionary remedy for illegal dragnets and a discovery mechanism) are analogous to prior actions that Congress has taken with respect to wiretapping and FISA.

In 1934, Congress acted to reign in wiretapping excesses, spurred largely by Prohibition and organized-crime investigations, with a limited federal statute.[98] After the Supreme Court failed to adopt a more sweeping constitutional remedy in Berger v. New York,[99] Congress crafted the Wiretap Act, a more comprehensive statutory scheme regulating wiretapping.[100] In 1968, Congress enacted the Electronic Communications Privacy Act ("ECPA"),[101] updating and reorganizing the Wiretap Act, because of concerns with new technologies.[102]

In 1975, Congress organized the Senate Select Committee to Study Governmental Operations With Respect to Intelligence Activities (the "Church Committee") to investigate Government intelligence gathering.[103] The Church Committee concluded that the Executive Branch had engaged in widespread surveillance of citizens and that Congress needed to reign in foreign intelligence gathering.[104] As a result, in 1978, Congress enacted FISA, requiring the Government to obtain court orders from the FISC for certain foreign intelligence activities.[105]

While typically the political branches of government have been more hostile to constitutional rights protecting criminal defendants than the judiciary,[106] high-

---

legislatures' vague statutory enactments); RAN HIRSCHL, TOWARD JURISTOCRACY: THE ORIGINS AND CONSEQUENCES OF THE NEW CONSTITUTIONALISM (2004) (advocating judicial constitutional interpretation to resolve difficult policy issues).

[98] *See* Communications Act of 1934, ch. 652, 48 Stat. 1064 (current version at 47 U.S.C § 605 (1996)) (excluding wiretap evidence from federal criminal trials).

[99] 388 U.S. 41 (1967) (reviewing New York's wiretap statute, N.Y. Code Crim. Proc. § 813-a, and holding it to be unconstitutional on narrow grounds).

[100] *See* Title III § 802 of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-315, 82 Stat. 197 (current version at 18 U.S.C. §§ 2510-20 (2013)).

[101] Pub. L. 99-508, 100 Stat. 1848 (1986) (codified as amended in scattered sections of 18 U.S.C.).

[102] *See* Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1557–58 (2004).

[103] *See* ACLU v. Clapper, 785 F.3d 787, 793 (2d Cir. 2015).

[104] *See id*.

[105] *See* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801 (1978)).

[106] *See* KATHERINE BECKETT, MAKING CRIME PAY: LAW AND ORDER IN CONTEMPORARY AMERICAN POLITICS (1997); ELLIOTT CURRIE, CRIME AND PUNISHMENT IN AMERICA 6–7 (2013) (describing the tendency of policymakers to fixate on increasing punishment as their sole criminal-justice remedy); STUART A. SCHEINGOLD, THE POLITICS OF LAW AND ORDER: STREET CRIME AND PUBLIC POLICY 71 (Malcolm M. Feeley et al. eds.,1984) (describing how politics drive punitive political discourse and policies); William Lyons & Stuart Scheingold, *The Politics of Crime and*

tech bulk surveillance seems to be one area in which Congress has demonstrated sufficient recent outrage, interest, and willingness to support privacy protections. Ric Simmons has described this "rise of Congress" in ensuring privacy against encroachment by new surveillance technologies.[107]

In 2012, the Senate Judiciary Committee passed the ECPA Amendments Act, which would have strengthened privacy protections for e-mail communications by amending the ECPA to require a warrant based on probable cause to access electronic communications, like text messages, e-mails, and other private documents in individual electronic accounts.[108] More recently, a bipartisan group of Senators proposed the USA Freedom Act[109] in response to Edward Snowden's disclosures in June 2013 about the NSA's bulk-surveillance programs.[110] The Act would prohibit bulk collection of Americans' communications without a court order and permit telecommunications companies to report publicly their participation in surveillance programs. The Act was intended to rein in dragnet data collection, increase Congressional oversight of the FISC, permit third parties to release information regarding FISA requests, and create an independent constitutional advocate to argue before the FISC.[111] In May 2014, the House passed the Act.[112] Similar legislation was introduced in the Senate in August,[113] and was narrowly defeated in November, with fifty-eight votes in favor.[114]

These bills would restrict some of the bulk surveillance that may be permitted by the Fourth Amendment, but they do not create an exclusionary rule for their violation nor do they otherwise address the question that this Article raises: what if

---

Punishment, 1 CRIM. JUST. 103, 114 (2000) (describing the punitive nature of the "malign neglect" politics of crime control); Linda S. Mullenix, *Hope Over Experience: Mandatory Informal Discovery and the Politics of Rulemaking*, 69 N.C. L. REV. 795, 843–57 (1991) (questioning the ability of legislatures appropriately to promulgate procedural-justice rules); Michael Tonry & David P. Harrington, *Strategic Approaches to Crime Prevention*, *in* BUILDING A SAFER SOCIETY: STRATEGIC APPROACHES TO CRIME PREVENTION (Michael Tonry & David S. Harrington, eds. 1995); *see also* Robert Sampson & Dawn Jeglum Bartusch, *Legal Cynicism and (Subcultural?) Tolerance of Deviance: The Neighborhood Context of Racial Differences*, 32 L. & SOC'Y REV., 777 (1998) (describing how social policies drive increasingly intense surveillance).

[107] Ric Simmons, *The New Reality of Search Analysis: Four Trends Created by New Surveillance Technologies*, 81 MISS. L. J. 991, 995–99 (2012).

[108] *See* Charlie Savage, *Panel Approves a Bill to Safeguard E-Mail*, N.Y. TIMES Nov. 30, 2012, at B7.

[109] *See* H.R. 3361, 113th Cong. § 1 (2013) (expanding the definition of "tangible things" in FISA Section 215 to include "call detail records," restricting the interception of Americans' communications with foreign targets, and reforming FISC and the use of National Security Letters).

[110] *See* Charlie Savage & Jeremy W. Peters, *Bill to Restrict N.S.A. Data Collection Blocked in Vote by Senate Republicans*, N.Y. TIMES, November 19, 2014, at A1.

[111] *See* H.R. 3361 113th Cong. § 1 (2013).

[112] *See* Jennifer Granick & Christopher Sprigman, *The Criminal N.S.A.*, N.Y. TIMES June 27, 2013, http://nytimes.com/2013/06/28/opinion/the-criminal-nsa.html.

[113] *See* S.B. 2685 113th Cong. (2013).

[114] *See* Savage & Peters, *supra* note 110,.

the NSA does it anyway? The question that remains for legislation, therefore, is how to close the firewall loophole. In the context of patently illegal surveillance and the attenuation doctrine, the greater need is for a remedy rather than recognition of the right in the first instance, a legislative exclusionary rule for all evidence derived, directly or indirectly, from illegal surveillance, irrelevant of the constitutional concepts of taint and attenuation. The key is to exclude the results of illegal surveillance, even when those results are merely the identification of a suspect for subsequent investigation. This exclusionary rule must ask whether, but for the primary illegality (the NSA's illegal spying), the derivative evidence would have been found (the FBI would have focused on the defendant), in contrast to the constitutional exclusionary rule whose effectiveness against derivative evidence of identity founders against the proximate cause requirement.[115] This rule could be limited and unwanted consequences prevented if, unlike Fourth Amendment doctrine,[116] it also took into consideration the intentionality of illegal surveillance: the but-for test for causation kicks in when an agency engages in surveillance that it knows, or should know, is illegal.

B. *Deterrence*

Of course, determining the effectiveness of any "remedy" first depends upon the definition of "success." In the context of an exclusionary remedy, the Court generally recognizes deterring illegal police conduct as the only valid justification.[117] Assuming that deterring the NSA from engaging in flagrantly illegal surveillance is the goal of the statutory exclusionary remedy, then this proposal would be effective only if excluding subsequently derived evidence provided enough disincentive for the NSA to terminate the illegal surveillance. If the NSA does not care whether the indirect fruits of its illegal surveillance can be used in court, if it is not relying on judicial process to deal with the suspects that it reveals (if instead the NSA is intending, for example, to subject the suspects identified to extra-judicial procedures), then a stronger, statutory exclusionary rule will not prevent the illegal conduct.

It seems likely that a wide-scale program of illegal surveillance would generate a large list of domestic suspects, too large for the NSA to seize and detain. It is unlikely that a surreptitiously seized phone or e-mail conversation would say, "I am looking to blow up a federal building. How much and what kind

---

[115] *See* Roger S. Ruffin, *Out on a Limb of the Poisonous Tree: The Tainted Witness*, 15 U.C.L.A. L. REV. 32 (1967) (explaining how giving *Miranda* warnings to an accused or another witness relates to the attenuation of some prior police misconduct).

[116] *See, e.g.*, Whren v. United States, 517 U.S. 806 (discussed *supra* text accompanying note 94).

[117] *See* United States v. Leon, 468 U.S. 897, 916 (1984) ("[T]he exclusionary rule is designed to deter police misconduct . . . ."); United States v. Calandra, 414 U.S. 338, 347 ("[T]he rule's prime purpose is to deter future unlawful police conduct . . . ."); Herring v. United States, 555 U.S. 135, 140–41 (2009); Hudson v. Michigan, 547 U.S. 586, 591, 599.

of explosives will I need?" As wiretapping other types of illicit conduct has shown, individuals contemplating acts of illegality cloak their plans behind code words and veiled language.[118] As a practical matter, therefore, the NSA would need the subsequent, legal investigation, at least in most cases, to winnow its suspects from plausible to likely guilty. Even today, not all investigation can be done from a computer. If nothing else, the difference between the number of anti-terrorism field agents that the FBI and the NSA can deploy domestically would seem to necessitate the involvement of the second, post-firewall agency.

In addition, the selection of the NSA in the thought experiment is hypothetical (at least, the author hopes so). The more salient point is that, under current attenuation doctrine, any two law-enforcement agencies, or even two divisions within one agency, could engage in the two-step investigation, as long as they were sufficiently separated by a firewall. In other words, the FBI (or a local police department) could launch some bureaucratically titled "Non-Evidentiary Investigation Unit" within itself and, as long as all that unit shared with the team investigating criminal charges was the suspect's name, the subsequent investigation by the "court unit" would be an independent source for the evidence at trial. So, the firewall-loophole problem is not dependent on the involvement of a foreign-intelligence agency like the NSA that may not care about conventional prosecution.

Finally, even preventive-detention procedures, like those that the Court has historically approved, require Congressional authorization[119] and some level of individualized proof of guilt.[120] Assuming that the Congressional intent behind a legislative remedy for illegal surveillance that does not result in trial evidence is to deter the illegal surveillance in the first instance, Congress could enact an exclusionary rule that governed extrajudicial determinations, as well.

As I previously explained:

---

[118] *See, e.g.*, United States v. Dukagjini, 326 F.3d 45, 52 (2d. Cir. 2003) (describing the interception of traffickers' "opaque" coded conversations); United States v. Delpit, 94 F.3d 1134 (8th Cir. 1996) (describing wiretapped jargon and code words); United States v. Castiello, 915 F.2d 1, 3 (1st Cir. 1990) (describing "drug world jargon"); United States v. Theodoropoulos, 866 F.2d 587 (3d. Cir. 1989) (describing wiretapped drug jargon).

[119] *See* Non Detention Act, 18 U.S.C. § 4001 (1948) (expressly foreclosing detention of Americans without statutory authorization); *Ex Parte* Merryman, 17 F. Cas. 144 (C.C.D. Md. 1861) (holding that only Congress could suspend *habeas corpus*); *cf.* Boumediene v. Bush, 553 U.S. 723 (2008) (holding that the Military Commissions Act of 2006, codified at 28 U.S.C. § 2241(e), which precluded federal-court jurisdiction over petitions for habeas corpus by "enemy combatants," was an unconstitutional suspension of habeas corpus). *But cf.* Johnson v. Eisentrager, 339 U.S. 763 (1950) (denying German combatants tried by a military tribunal the constitutional right to *habeas corpus*); Hirota v. MacArthur, 338 U.S. 197 (1948) (holding that federal courts lacked jurisdiction over habeas-corpus petitions filed by Japanese citizens convicted in American military tribunals).

[120] *See* Hamdan v. Rumsfeld, 548 U.S. 557 (2006) (holding that trying Hamdan by military tribunal violated the Geneva Convention); Hamdi v. Rumsfeld, 542 U.S. 507 (2004) (holding that the preventive detention of Americans without review of the factual basis for detention in a neutral forum was unconstitutional).

> "The police have always been able to surveil *anyone* and collect evidence that they have abandoned or left in plain view. . . . Because of resource constraints, however, they would only surveil people against whom they had some individualized suspicion in the first instance—people who were already suspects. The police of the past were never able to surveil *everyone*. But today, they both can and do surveil people prior to suspicion as a way of looking for suspects."[121]

Because of the firewall loophole created by the attenuation doctrine and the "identity" cases, as long as surveillance that identifies a suspect is not employed at trial, there is no consequence, even if it was blatantly illegal.

VII. CONCLUSION

While Americans are often willing to trade freedom and privacy for security, in the case of the mass surveillance revealed by Snowden, they have shown interest in, and expressed outrage over, the programs.[122] The convergence of the two phenomena identified in this Article—the unwillingness of the Court to adopt a stricter attenuation doctrine and the popular resistance to high-tech bulk surveillance—may create an opportunity for Congress to take the lead in protecting privacy, rather than relying upon constitutional adjudication by the courts.

---

[121] *See* Leonetti, *supra* note 1, at 295.

[122] *See* Jennifer Agiesta & Nancy Benac, *Poll: OK to Trade Some Freedoms to Fight Terrorism*, THE ASSOCIATED PRESS-NORC CENTER FOR PUBLIC AFFAIRS RESEARCH, Sept. 7, 2011, http://www.apnorc.org/news-media/Pages/News+Media/poll-ok-to-trade-some-freedoms-to-fight-terrorism.aspx. Richard A, Clarke et al., *Protecting Citizens*, *and Their Privacy*, N.Y. TIMES Dec. 20, 2013, http://www.nytimes.com/2013/12/20/opinion/protecting-citizens-and-their-privacy.html; *What is Valued More: Freedom or Security?*, THE JOURNAL GAZETTE (Fort Wayne, Ind.), Sept. 7, 2011, at 1A.