7-2014

Digital Innocence

Joshua A.T. Fairfield
Washington & Lee University School of Law, fairfieldj@wlu.edu

Erik Luna
Washington and Lee University School of Law, lunae@wlu.edu

DIGITAL INNOCENCE

Joshua A.T. Fairfield† *& Erik Luna*††

Recent revelations have shown that almost all online activity and increasing amounts of offline activity are tracked using Big Data and data mining technologies. The ensuing debate has largely failed to consider an important consequence of mass surveillance: the obligation to provide access to information that might exonerate a criminal defendant. Although information technology can establish innocence—an ability that will only improve with technological advance—the fruits of mass surveillance have been used almost exclusively to convict. To address the imbalance and inform public dialogue, this Article develops the concept of "digital innocence" as a means of leveraging the tools of Big Data, data mining, ubiquitous consumer tracking, and digital forensics to prevent wrongful convictions and to provide hard proof of actual innocence for those already convicted.

† Professor of Law, Washington and Lee University School of Law.
†† Sydney and Frances Lewis Professor of Law, Washington and Lee University School of Law.

INTRODUCTION

The recent National Security Agency (NSA) data scandal has revealed what technologists have long suspected: every aspect of online life is tracked and recorded. The NSA maintains programs that cover "nearly everything a typical user does on the internet"[1] and collect "pretty much everything it can"[2]—e-mail and text messages, voice and video chats, photos and videos, file transfers, social networking information, Internet browsing histories and searches, and so on—rendering all of this data searchable by the government.[3] Pursuant to secret court orders, Americans' telephone and Internet metadata records are being proactively recorded, stored, parsed, and searched.[4] From the massive datasets derived from this data, it is possible to determine whom people talk to, where they are, what they are interested in, and even to predict what they might do next.[5] Outside of the NSA context, government monitoring has expanded through the use of third-party data and by the creation of state-run databases. Digital surveillance is increasing offline as well. For example, some police cars

---

1 Glenn Greenwald, *XKeyscore: NSA Tool Collects "Nearly Everything a User Does on the Internet,"* THE GUARDIAN (July 31, 2013, 8:56 AM), http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (quoting NSA materials on XKeyscore program) (internal quotation marks omitted).

2 James Ball, *NSA Collects Millions of Text Messages Daily in "Untargeted" Global Sweep*, THE GUARDIAN (Jan. 16, 2014, 1:55 PM), http://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep (quoting document on NSA's Dishfire program) (internal quotation marks omitted).

3 *See, e.g.*, *id.*; Greenwald, *supra* note 1; James Glanz, Jeff Larson & Andrew W. Lehren, *Spy Agencies Tap Data Streaming from Phone App*, N.Y. TIMES, Jan. 28, 2014, at A1; Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST, Oct. 15, 2013, at A1; Glenn Greenwald & Ewen MacAskill, *Revealed: How US Secretly Collects Private Data from AOL, Apple, Facebook, Google, Microsoft, Paltalk, Skype, Yahoo and Youtube*, THE GUARDIAN, June 7, 2013, at A1.

4 *See* Barton Gellman, *The Architecture: Four-Pronged U.S. Approach Relies Heavily on Data Behind Internet, Phone Communications*, WASH. POST, June 16, 2013, at A1 (Internet and telephony metadata); James Ball, *Verizon Court Order: Telephone Call Metadata and What It Can Show*, THE GUARDIAN (June 6, 2013, 10:12 PM), http://www.theguardian.com/world/2013/jun/06/phone-call-metadata-information-authorities (telephony metadata). "Metadata" can be defined as data about data. In the context of electronic communications, metadata is information about a communication—the addresses and identities of an e-mail sender and recipient, for instance, and the time, duration, and relevant numbers of a phone call—but it does not include the communication itself.

5 *See* Barton Gellman & Ashkan Soltani, *NSA Maps Targets by Their Phones*, WASH. POST, Dec. 5, 2013, at A1; James Risen & Laura Poitras, *N.S.A. Examines Social Networks of U.S. Citizens*, N.Y. TIMES, Sept. 29, 2013, at A1.

now use license plate readers to create a database of driver locations.[6] New overhead camera technology permits tracking of the location and activities of everyone in an entire city for hours.[7] In the Boston bombing investigation, street cameras, cellphone recordings, and even a municipal facial recognition system were employed in pursuit of the culprits.[8]

Largely due to the disclosures of Edward Snowden, the nation is now engaged in a wide-ranging discussion about the balance between national security and individual privacy. The responses include major reports,[9] several legal challenges,[10] numerous congressional hearings,[11] and a high-profile presidential address.[12] These contributions often point in different directions, sparking objections and further controversies.[13] There is disagreement not only about what should be done but also as to the factual predicates for decision making, including whether the NSA's programs have prevented acts of terrorism.[14]

---

6 *See You Are Being Tracked: How License Plate Readers Are Being Used to Record Americans' Movements*, AM. C.L. UNION, https://www.aclu.org/alpr (last visited Aug. 23, 2013).

7 *See* Craig Timberg, *High Above, an All-Seeing Eye Watches for Crime*, WASH. POST, Feb. 6, 2014, at A1.

8 *See* Mariel Myers, *Boston Bombings: How Facial Recognition Can Cut Investigation Time to Seconds*, CNET (Apr. 18, 2013, 5:56 PM), http://www.cnet.com/news/boston-bombings-how-facial-recognition-can-cut-investigation-time-to-seconds/.

9 *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (2014); PRESIDENT'S REVIEW GRP. ON INTELLIGENCE & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD (2013) [hereinafter PRG REPORT].

10 *See* Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013); ACLU v. Clapper, No. 13 Civ. 3994 (WHP), 2013 WL 6819708 (S.D.N.Y. Dec. 27, 2013).

11 *See, e.g.*, *Examining Recommendations to Reform FISA Authorities: Hearing Before the H. Comm. on the Judiciary*, 113th Cong. (2014); *Strengthening Privacy Rights and National Security: Oversight of FISA Surveillance Programs: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (2013).

12 *See* Barack Obama, U.S. President, Remarks by the President on Review of Signals Intelligence, Address at the Department of Justice (Jan. 17, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/remarks-president-review-signals-intelligence; *see also* Presidential Policy Directive 28: Signals Intelligence Activities, The White House (Jan. 17, 2014), *available at* http://www.whitehouse.gov/sites/default/files/docs/2014sigint_mem_ppd_rel.pdf (directive accompanying President Obama's remarks).

13 *Compare* PRG REPORT, *supra* note 9, at 24–27, 36, 86–94, 200–08 (proposing various changes to the Foreign Intelligence Surveillance Court (FISC)), *with* Letter from John D. Bates, Dir. of the Admin. Office of the U.S. Courts, to Dianne Feinstein, Chairman of the Senate Select Comm. on Intelligence (Jan. 13, 2014), *available at* http://www.feinstein.senate.gov/public/index.cfm/files/serve/?File_id=3bcc8fbc-d13c-4f95-8aa9-09887d6e90ed (criticizing proposals).

14 *Compare Klayman*, 957 F. Supp. 2d at 40–41 (noting the "utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics"), PETER BERGEN ET AL., NEW AM. FOUND., DO NSA'S BULK SURVEILLANCE PROGRAMS STOP TERRORISTS? 1–3 (2014) (rejecting government claims that mass surveillance has kept the United States safe from terrorism), *and* PRG REPORT, *supra* note 9, at 104 ("[T]he information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily

What is largely missing from the debate, however, is any discussion of the consequences of mass surveillance for the rights of those accused and convicted of crime.

In trying to bolster the argument for one controversial surveillance statute, a federal lawmaker cited a series of criminal cases as proof that the law was effective at thwarting terrorism.[15] As it turns out, the defendants in those cases had not been notified that the NSA's programs provided information in the underlying criminal investigations.[16] Later revelations showed that the government has been engaged in a long-term ruse in which law enforcement covers up the source of information provided by the intelligence community.[17] This strikes at the heart of the American criminal justice system and likely violates a number of constitutional provisions. But these practices also demonstrate a gross hypocrisy: the government is using digital surveillance to build its case for conviction while refusing to disclose that fact to the defendant, let alone providing him the content of the surveillance and access to the relevant databases. This is not just a matter of procedural fairness, however. The government's high-tech tools of incrimination—the use of "Big Data,"[18] data mining, ubiquitous consumer tracking, and digital forensics—can also provide hard proof of actual innocence for the wrongfully accused or convicted.

Consider the Occupy Wall Street protests, lauded by some for raising political awareness and doubts,[19] chided by others as the law-

---

have been obtained in a timely manner using conventional [methods]."), *with Clapper*, 2013 WL 6819708, at *25–26 (citing government's purported successes and stating that "[t]he effectiveness of bulk telephony metadata collection cannot be seriously disputed"), Michael Morell, *Correcting the Record on the NSA Review*, WASH. POST, Dec. 29, 2013, at A17 (former CIA Acting Director arguing that bulk surveillance "would likely have prevented 9/11" and "has the potential to prevent the next 9/11"), *and* Benjamin Wittes, *A Critique of the New America Foundation's Recent NSA Report*, LAWFARE (Jan. 23, 2014, 10:47 AM), http://www.lawfareblog.com/2014/01/a-critique-of-the-new-america-foundations-recent-nsa-report/ (criticizing report by BERGEN ET AL., *supra*).

15 158 CONG. REC. S8384 (daily ed. Dec. 27, 2012) (statement of Sen. Diane Feinstein); *see also* Ellen Nakashima, *NSA Surveillance Questioned in Plot Case*, WASH. POST, June 22, 2013, at A2 (quoting and discussing Sen. Diane Feinstein's comments concerning reauthorization of 50 U.S.C. § 1881a); *infra* notes 270–82 and accompanying text (discussing 50 U.S.C. § 1881a).

16 *See infra* notes 290–91 and accompanying text.

17 *See infra* notes 387–89 and accompanying text.

18 *See, e.g.*, JAMES MANYIKA ET AL., MCKINSEY GLOBAL INST., BIG DATA: THE NEXT FRONTIER FOR INNOVATION, COMPETITION, AND PRODUCTIVITY 1 (2011) ("'Big Data' refers to datasets whose size is beyond the ability of typical database software tools to capture, store, manage, and analyze. This . . . incorporates a moving definition of how big a dataset needs to be in order to be considered big data . . . . [A]s technology advances over time, the size of datasets that qualify as big data will also increase.").

19 *See, e.g.*, Rose Aguilar, *Occupy Has Raised Class Consciousness: Now What?*, TRUTHOUT (Feb. 13, 2012), http://truth-out.org/news/item/6628-occupy-has-raised-class-consciousness-now-what (stating that the Occupy movement has "raised awareness about the widen-

lessness of neo-ne'er-do-wells.[20] In the ensuing arrests of protesters in New York City and elsewhere, the account of events by law enforcement differed markedly from those of the protesters.[21] But some defendants had digital proof of their innocence.[22] Witnesses had recorded the protests, often on cellphone cameras, creating footage that might absolve or condemn in the eyes of the law.[23] When the recordings were made available through defense requests, most of the footage proved useless for those arrested. Yet a few recordings displayed the relevant events exactly as they occurred and, most importantly, offered proof of protestor innocence.[24] Inadvertently, Occupy Wall Street showcased the role of technology in preventing wrongful convictions.[25] Social network tools, mobile computing, and consumer recording offer the prospect of findable exculpatory evidence for those facing criminal trial and punishment.

Such stories are not part of the dueling narratives in America's current debate over pervasive government surveillance, which, depending on one's perspective, either leads to a dystopian panoptic society or prevents another 9/11. The choice is pitched as whether the information should be gathered, and, if so, when, where, and how much. A different question needs to be asked: Who will have access to the data? For the most part today, only the government and corporate entities gather and tap the stores of information about the populace. This creates a dangerous imbalance where only the most powerful public and private actors may draw upon data about the general population. Some experts have argued for the tables to be turned by increasing the capacity of individuals to find out information about

---

ing wealth gap, inequality, rising student debt, criminal activity on Wall Street, poverty and home foreclosures").

20 *See, e.g.*, Kate Zernike, *Wall St. Protest Isn't Like Ours, Tea Party Says*, N.Y. TIMES, Oct. 22, 2011, at A1 (discussing portrayal of Occupy protesters as, among other things, "messy, indolent, drug-addled," "unemployed, uneducated, and uninformed").

21 *See* Nick Pinto, *Jury Finds Occupy Wall Street Protester Innocent After Video Contradicts Police Testimony*, VILLAGE VOICE (Mar. 1, 2013, 2:53 AM), http://blogs.villagevoice.com/runninscared/2013/03/jury_finds_occu.php (noting discrepancies between law enforcement officials' account of an arrest and video evidence).

22 *Id.*

23 *Id.*

24 *See id.* (discussing how video evidence undercut police testimony and resulted in a not guilty verdict for protester); *see also* Nick Pinto, *In the First Occupy Wall Street Trial, Acquittal*, VILLAGE VOICE (Mar. 16, 2012, 9:29 AM), http://blogs.villagevoice.com/runninscared/2012/05/in_the_first_oc.php [hereinafter *Occupy Trial*] (discussing another case in which photographic evidence contradicted police testimony).

25 *See* Radley Balko, *Tech-Savvy Occupy Protesters Use Cellphone Video, Social Networking to Publicize Police Abuse*, HUFFINGTON POST (Oct. 29, 2011, 1:26 PM), http://www.huffingtonpost.com/2011/10/29/occupy-protesters-armed-with-technology_n_1063706.html ("In both [civil and] criminal proceedings . . . it's likely that any significant protest will have independent video . . . to ferret out what actually happened.").

their surveillance.[26] If the powerful are going to spy on us and collect data about our lives, shouldn't we know what information is being gathered and have access to the resulting databases?

This argument takes on a constitutional dimension when the information is wielded by law enforcement to accuse, convict, and punish. Modern surveillance technology can provide both inculpating and exculpating evidence. Electronic eavesdropping can catch the guilty red-handed, but it can also provide alibis for the wrongfully accused and convicted. With citizens' lives increasingly logged and tracked, online and off, the chance of finding evidence tending to prove innocence only increases. The breadth and depth of corporate and government surveillance seem to guarantee the existence of exonerating evidence, stored somewhere, proving the innocence of suspects and defendants. Assuming computer engineers can refine the tools necessary to find it, proof of innocence will be uncovered in some yet-to-be-determined number of cases. This Article calls for the development of a new concept—*digital innocence*—seeking to leverage the tools and content of Big Data to prevent wrongful convictions and provide hard proof of actual innocence for those already convicted.

To be clear, the following is not an apologia for data gathering in service of national security or commercial interests. State and corporate invasions of individual privacy have clear and much-discussed costs for society.[27] And needless to say, the government's unprecedented level of secret, suspicionless monitoring of personal communication raises myriad legal, political, and philosophical issues. We think the practice is anathema to a liberal, open democracy and inconsistent with the framework and rights protections of the U.S. Constitution. The present argument is different, however, serving not as a paean to surveillance but as a kind of warning. If the government gathers information about its citizens, it cannot use that data solely to accuse and convict—or worse yet, hide the information or obfuscate its source—leaving the individual with no defense. Consistent with well-established rights of evidentiary access, the information must be made available to defendants to protect against wrongful convictions and to exonerate those who have already been convicted.

Indeed, far from supporting mass surveillance, the concept of digital innocence complicates government efforts to use surveillance data only to investigate and prosecute. The President's Review Group

---

26 *See, e.g.*, DAVID BRIN, THE TRANSPARENT SOCIETY 80–84 (1998) (discussing concept of "reciprocal transparency"); Steve Mann et al., *Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments*, 1 SURVEILLANCE & SOC'Y 331 (2003) (discussing concept of "sousveillance").

27 *See* Ron Wyden et al., Op-Ed., *End the N.S.A. Dragnet, Now*, N.Y. TIMES, Nov. 26, 2013, at A25 (three U.S. Senators discussing danger of mass surveillance).

on Intelligence and Communications Technology recommended that government should base its surveillance decisions on "a careful analysis of consequences, including both benefits and costs."[28] One important consequence of government surveillance is the legal requirement of reciprocal access to information, which carries a real cost for the law enforcement and intelligence communities. There is also a consequence and cost for commercial acquisition of people's data: any company that collects such data must be prepared to provide information that might help exonerate a criminal defendant.

This Article proceeds in five parts. Part I discusses the conceptual gap in the legal academic literature regarding digital innocence, while Part II provides an overview of the relevant technology. Part III then discusses the legal foundation for government exploitation of Big Data. Part IV considers defendants' right to access and use this information and the challenges they will face in trying to exercise this right. Finally, Part V describes how defendants can establish digital innocence, based on a measured analysis of case law and statutory authority.

I
The Concept of Digital Innocence

In 2005, San Francisco introduced cameras at hotspots throughout the city as a way of bringing down the overall crime rate. But the cameras were soon put to a different purpose. "[M]ore than just a crime-fighting tool," the cameras "have also become a tool exploited by defense lawyers who often seek footage from the cameras to exonerate falsely accused clients."[29] In one case, a man was cleared of a murder charge when footage showed him defending a disabled woman.[30] Public defenders are now trained to ask for the data, with a third of all requests for footage coming from defense attorneys.[31]

A similar phenomenon is unfolding around law enforcement recording, typically done by citizens filming police in action.[32] Mobile recording devices have become a check on abuse of power and, as was the case for some Occupy Wall Street protestors, a means of proving

28 PRG Report, *supra* note 9, at 16, 50; *see also id.* at 42, 50–51, 257–58 (recommending cost-benefit analysis and risk-management approaches).

29 Joshua Sabatini, *San Francisco's Crime Cameras Zoom in on the Innocent*, S.F. Examiner (July 8, 2011), http://www.sfexaminer.com/sanfrancisco/san-franciscos-crime-cameras-zoom-in-on-the-innocent/Content?oid=2177815.

30 *See id.*

31 *See id.*

32 *See* Balko, *supra* note 25.

one's innocence.[33] Elsewhere, dashboard-mounted video cameras have become indispensable for motorists who rely upon the captured images as a means to protect themselves against erroneous or crooked traffic enforcement.[34] At times, however, the government's own recordings have helped free the innocent. In a recent case, a New Jersey man charged with resisting arrest and assault was cleared after the defense requested and received a police dash-cam video, which both exonerated him and exposed wrongdoing by several officers.[35] "If we hadn't had the tapes in this case," defense counsel said, "an innocent man would be in jail today."[36]

These examples are merely the faintest ripple of a coming tide of digital evidence. An important report by the National Academy of Sciences (NAS) described the development of "an emerging forensic science discipline":

> The proliferation of computers and related devices over the past 30 years has led to significant changes in and the expansion of the types of criminal activities that generate digital evidence. Initially, computers were either the weapon or the object of the crime. . . . As computers became more popular, they became storage containers for evidence. . . . Finally, digital media have become witnesses to daily activities. . . . As a result, almost every crime could have digital evidence associated with it.[37]

Clearly, digital evidence can incriminate the guilty. But the NAS report—which documented the possibilities and perils of other forensic disciplines for the factually innocent[38]—failed to discuss the potential of digital evidence to exonerate the wrongfully accused and convicted.

Part of the problem is that the concept of digital innocence is under-theorized. We are aware of no academic article that discusses the use of Big Data to prove innocence. This is a marked and startling gap. The defense bar has begun to recognize that a client being on camera, or being recorded, or being geolocated, can be a good

---

33 *See* Joshua Holland, *How Video of Police Behaving Badly Made Occupy Wall Street a Global Phenomenon*, ALTERNET (Oct. 24, 2011), http://www.alternet.org/story/152856/how_video_of_police_behaving_badly_made_occupy_wall_street_a_global_phenomenon.

34 *See* Tom Balmforth, *Cops, Cars, and Videotape: Russians Embrace Dash-Cam Craze*, RADIO FREE EUR. (Nov. 24, 2012), http://www.rferl.org/content/dash-cams-russia-fighting-corruption-and-scams-car-crashes/24780355.html (describing how dashboard-mounted video cameras have become "an essential accoutrement for Russian motorists," who "use these dash cams as a tool to help fight their corner against Russia's notoriously corrupt traffic police").

35 Sarah Wallace, *Exclusive: Dashcam Video Clears NJ Man*, WABC-TV (Feb. 21, 2014), http://abclocal.go.com/wabc/story?section=news/investigators&id=9440401#.

36 *Id.* (quoting defense attorney Steven Brown).

37 NAT'L RESEARCH COUNCIL OF THE NAT'L ACADS., STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 179–80 (2009) [hereinafter NAS REPORT].

38 *See id.* at 4–5, 37, 42–48, 100.

thing.[39] The growth of data collection, connection, and parsing capabilities could transform Big Data technologies into an important tool for establishing innocence.

The extant relevant literatures fall into two rough categories. The first is the discussion of privacy and the Fourth Amendment, which to date has dominated the discussion of the intersection between surveillance technology and criminal defense. The idea of digital innocence has lagged behind for at least a couple of reasons.[40] The scholarship has spoken consistently to the invasion of individual rights and interests by Big Data data mining and mass-market consumer surveillance, often focusing on proposals to restrict government access to information as a means to protect privacy and vindicate Fourth Amendment interests.[41] The privacy conversation is vitally important, all the more so in light of recent revelations about massive government spying. But it has also created a blind spot of sorts to the exonerating potential of digital information.[42]

This shortcoming in the literature is understandable. To broach the topic of digital innocence in the age of Big Data, rights-minded scholars would have to confront yet another temptation in a Faustian bargain that already trades privacy and liberty for knowledge, convenience, and security.[43] Alternatively, scholars might have to assume arguendo that mass surveillance will continue despite powerful objections. As seen in our introductory caveat, we are deeply troubled by the massive and relentless tracking of people's interactions, particularly when done by the government. But we are also concerned that

---

39 *See* Bob Sullivan, *Lawyers Eye NSA Data as Treasure Trove for Evidence in Murder, Divorce Cases*, NBC NEWS (June 20, 2013), http://www.nbcnews.com/technology/lawyers-eye-nsa-data-treasure-trove-evidence-murder-divorce-cases-6C10398754?franchiseSlug=technolog.

40 *See* James S. Liebman et al., *The Evidence of Things Not Seen: Non-Matches as Evidence of Innocence*, 98 IOWA L. REV. 577, 619–22 (2013) (noting that the civil liberties issues with data mining have focused more on the use of such information to target specific individuals).

41 For a strain of this conversation, see Orin S. Kerr, *Congress, the Courts, and New Technologies: A Response to Professor Solove*, 74 FORDHAM L. REV. 779 (2005); Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) [hereinafter Kerr, *The Fourth Amendment*]; Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557 (2004); Daniel J. Solove, *The Coexistence of Privacy and Security: Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747 (2005). For an excellent, fairly recent summation of the debate and literature, see Joshua S. Levy, *Towards a Brighter Fourth Amendment: Privacy and Technological Change*, 16 VA. J.L. & TECH. 502 (2011).

42 *See, e.g.*, Marc J. Zwillinger & Christian S. Genetski, *Criminal Discovery of Internet Communications Under the Stored Communications Act: It's Not a Level Playing Field*, 97 J. CRIM. L. & CRIMINOLOGY 569, 571–72 (2007).

43 *Cf.* Robert Weisberg, *IVHS, Legal Privacy, and the Legacy of Dr. Faustus*, 11 SANTA CLARA COMPUTER & HIGH TECH. L.J. 75, 75–77 (1995) (discussing the Fourth Amendment tradeoff—privacy rights balanced against security concerns—in the context of Intelligent Vehicle Highway Systems).

the current debate has failed to take into consideration an important cost of mass surveillance: the non-derogable obligation to provide access to potentially exonerating information. By exploring the concept of digital innocence, this Article seeks to make clear that government and corporate entities will have to pay a price if they intend to (and are allowed to) monitor the entirety of people's lives.

The second scholarly category offers an analogous enterprise to the one we have undertaken here: the literature on the DNA revolution in wrongful convictions.[44] This scholarship is not concerned with the concept we have described as digital innocence and only hints at the possibility,[45] but it still serves as a good example of how technological advance can change the legal debate surrounding innocence, suggesting how our concept might fit into the overall scheme of the law. In fact, the path of DNA technology through legal institutions may serve as a trail for digital innocence.[46] Proof-of-innocence technologies exert a unique influence on the criminal justice system. Although prosecutors do not always respond well to wrongful conviction claims—especially those premised on human error, such as false confessions and mistaken witness identifications—hard scientific proof of innocence is more likely to move the government to drop charges or acquiesce to the release of an inmate.[47] The DNA technology literature therefore sets the stage for a discussion about the broader role of technology in establishing innocence.

The literature also provides insights on the application and pace of technological advance.[48] Evidence in criminal cases changes with technology,[49] as developments help finger the guilty but also have the power to exonerate the wrongfully accused or convicted. Typically, however, new technology is first used to convict and only years later, if ever, used to acquit.[50] Moreover, lags in the exoneration of defend-

---

44 For prominent works in this area, see BRANDON L. GARRETT, CONVICTING THE INNOCENT: WHERE CRIMINAL PROSECUTIONS GO WRONG (2011); BARRY SCHECK ET AL., ACTUAL INNOCENCE: FIVE DAYS TO EXECUTION AND OTHER DISPATCHES FROM THE WRONGLY CONVICTED (2000); Samuel R. Gross et al., *Exonerations in the United States: 1989 Through 2003*, 95 J. CRIM. L. & CRIMINOLOGY 523 (2005); Richard A. Leo & Jon B. Gould, *Studying Wrongful Convictions: Learning from Social Science*, 7 OHIO ST. J. CRIM. L. 7 (2009).

45 *Cf.* Julie A. Singer et al., *The Impact of DNA and Other Technology on the Criminal Justice System: Improvements and Complications*, 17 ALB. L.J. SCI. & TECH. 87, 118–20 (2007) (considering the idea that non–DNA technology might provide strong evidence of innocence).

46 *See* Jules Epstein, *"Genetic Surveillance"—the Bogeyman Response to Familial DNA Investigations*, 2009 U. ILL. J.L. TECH. & POL'Y 141, 141–42 (2009).

47 *See, e.g.*, Jeffrey Rosen, *Wrongly Accused*, N.Y. TIMES, Sept. 16, 2007, § 7, at 6.

48 *See, e.g.*, Robert P. Mosteller, *Evidence History, the New Trace Evidence, and Rumblings in the Future of Proof*, 3 OHIO ST. J. CRIM. L. 523, 535–36 (2006).

49 *See, e.g.*, Emily Green, *Forensic Advances Raise New Questions About Old Convictions*, NAT'L PUB. RADIO (Mar. 20, 2013, 12:44 PM), http://www.npr.org/2013/03/20/174842256/forensic-advances-raise-new-questions-about-old-convictions.

50 *Id.*

ants are often characterized by issues of storage, followed by improvements in the testing technology.[51] Along these lines, DNA analysis initially was the province of prosecutors but over time became essential to claims of actual innocence.[52] If a wrongfully convicted defendant was lucky, biological evidence of the real perpetrator was properly stored, sometimes for years, until the capacity and technology were developed to test the evidence.[53]

As suggested by the language quoted from the NAS report, data science and Big Data technologies have been overwhelmingly used to convict.[54] Prosecutors often gather cookie data,[55] search terms,[56] web-surfing history,[57] and cell-site location information as part of their case against the accused.[58] But in the future, this data need not accrue exclusively to the benefit of prosecutors.[59] As search algorithms get better and private citizens obtain access to data-mining tools and technologies, defense counsel might have a significantly greater ability to prove actual innocence by finding some specific video from a local camera, for instance, or by cross-referencing geolocation information from a cellphone, thereby showing that the defendant was not at a given place at a given time.[60] The question is whether the massive amounts of data gathered about every American citizen will result in a similar or even greater potential to exonerate the innocent.

We predict it will. Commercial[61] and government actors gather enormous amounts of data about every element of people's daily lives.[62] An individual's real-world location is shown by his cellphone geolocation information.[63] Each person's text messages and e-mails

---

51 *See, e.g.*, Kevin Johnson, *Storage of DNA Evidence Key to Exonerations*, USA TODAY (Mar. 28, 2011), http://usatoday30.usatoday.com/news/nation/2011-03-28-crimelab28_ST_N.htm.

52 *See* Randy James, *A Brief History of DNA Testing*, TIME (June 19, 2009), http://content.time.com/time/nation/article/0,8599,1905706,00.html.

53 *See id.*

54 *See* Damiano Beltrami, *I'm Innocent. Just Check My Status on Facebook.*, N.Y. TIMES, Nov. 12, 2009, at A27.

55 *See* Zwillinger & Genetski, *supra* note 42, at 571 & n.7.

56 *See, e.g.*, Kerr, *The Fourth Amendment*, *supra* note 41, at 829 & nn.161–62; Joseph Goldstein & Marc Lacy, *Man Charged in Tucson Shootings Had Researched Assassins, Official Says*, N.Y. TIMES, Jan. 27, 2011, at A16.

57 *See, e.g.*, Goldstein & Lacy, *supra* note 56; *see also* Beltrami, *supra* note 54.

58 *See* Mark Hansen, *Prosecutors' Use of Mobile Phone Tracking to Spot a Defendant Is "Junk Science," Critics Say*, A.B.A. J., June 2013, at 15.

59 *See* Sabatini, *supra* note 29.

60 *See id.*

61 *See* Ashlee Vance, *Facebook's Is Bigger Than Yours*, BUS. WK. (Aug. 23, 2012), http://www.businessweek.com/articles/2012-08-23/facebooks-is-bigger-than-yours.

62 *See* Glenn Greenwald, *US Orders Phone Firm to Hand Over Data on Millions of Calls*, THE GUARDIAN, June 6, 2013, at A1.

63 *See* Mathew J. Schwartz, *7 Facts About Geolocation Privacy*, INFO. WK. (Aug. 20, 2012, 12:13 PM), http://www.informationweek.com/security/risk-management/7-facts-about-geolocation-privacy/d/d-id/1105877?.

are stored, parsed, and keyword-searched, with his buying habits, online and offline, systematically incorporated into comprehensive databases.[64] People are also subject to increasing amounts of public surveillance.[65] Cameras on street corners, cameras on ATMs, cameras from shop windows, and cameras carried by citizens provide a wealth of photographic and audio evidence that might bear on a criminal case.[66] Most importantly, all of this information is being stored,[67] awaiting more useful access to the data.[68]

Although the DNA technology literature is replete with discussions of how innovation makes more accurate determinations possible,[69] the advances took time and generated multiple interpretations. New technology almost always contains the seeds of disparate meanings, as proposed advances vie with traditional methodologies for pride of place in trials and post-conviction proceedings.[70] This underscores the importance of discovery and access to databases so that the technology can be evaluated.[71] Government databases are often either secret or closed,[72] despite the fact that the contents and algorithms of these databases can be critical to criminal defense efforts. The ongoing NSA scandal is scandalous not only because of the information being gathered but also because of government efforts to conceal the source of information used by law enforcement.[73] As will be discussed below, if databases are used for criminal investigations and prosecutions, then defendants must be given access to them.[74] In this sense, the DNA technology literature points toward, but does not resolve, an issue that will be crucial for those seeking to use information technology to exonerate.

Certainly, the DNA revolution has placed a spotlight on the entire criminal justice system. Generations of defense lawyers struggled to free inmates who they believed to be innocent, but the available

---

64 *See* Jennifer Valentino-Devries & Jeremy Singer-Vine, *They Know What You're Shopping For*, WALL ST. J., Dec. 8, 2012, at C1.

65 *See* Keith Proctor, *The Great Surveillance Boom*, FORTUNE (Apr. 26, 2013, 4:56 PM), http://management.fortune.cnn.com/2013/04/26/video-surveillance-boston-bombings/.

66 *See id.*

67 *See* Andy Greenberg, *NSA's New Data Center and Supercomputer Aim to Crack World's Strongest Encryption*, FORBES (Mar. 16, 2012, 4:23 PM), http://www.forbes.com/sites/andygreenberg/2012/03/16/nsas-new-data-center-and-ultra-fast-supercomputer-aim-to-crack-worlds-strongest-crypto/.

68 *See* Steve Lohr, *Sizing Up Big Data*, N.Y. TIMES, June 20, 2013, at F1.

69 *See, e.g.*, Sarah M. Ruby, *Checking the Math: Government Secrecy and DNA Databases*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 257, 258–59 (2010).

70 *See generally* Note, *Confronting the New Challenges of Scientific Evidence*, 108 HARV. L. REV. 1481, 1557–82 (1995) (describing "DNA Evidence and the Criminal Defense").

71 *See* Ken Strutin, *Databases, E-Discovery and Criminal Law*, 15 RICH. J.L. & TECH. 6, 27–28 (2008).

72 *See* Ruby, *supra* note 69, at 263–64.

73 *See id.* at 270.

74 *See infra* Part IV.A.

means to upend convictions were limited to recantations by witnesses and confessions by the actual perpetrators. Even in the rare cases where such evidence surfaced, defense claims were often procedurally barred.[75]

> In what seems like a flash, DNA tests performed during the last decade of the [twentieth] century not only have freed sixty-four individuals but have exposed a system of law that has been far too complacent about its fairness and accuracy. . . .
> Now the fabric of false guilt is laid bare, and the same vivid threads bind . . . . Sometimes eyewitnesses make mistakes. Snitches tell lies. Confessions are coerced or fabricated. Racism trumps the truth. Lab tests are rigged. Defense lawyers sleep. Prosecutors lie.[76]

DNA-based exonerations have challenged long-held assumptions about the trustworthiness of particular forms of evidence, while opening the door to a reevaluation of the priorities of criminal justice by, for instance, eroding support for the trend toward finality at all costs. To date, however, DNA technology has freed only several hundred innocent inmates.[77] Their stories are invaluable and their releases are historic, but DNA alone cannot realign the legal process to better serve "'the twofold aim [of criminal justice] . . . that guilt shall not escape or innocence suffer.'"[78] In all likelihood, the vast majority of wrongful conviction cases will have no biological evidence subject to legally dispositive DNA testing.[79] One estimate places the wrongful conviction rate in the United States at between 0.5% and 1%, which would mean that 2000 to 4000 innocent defendants are imprisoned each year.[80]

The single discipline of DNA technology cannot serve as the comprehensive source of information needed to meaningfully reduce the incidence of wrongful convictions. The coming wave of Big Data information technologies has the potential to provide hard proof of actual innocence in many of the non-DNA cases. In fact, data-mining

---

75 *See* Karen Christian, Note, *"And the DNA Shall Set You Free": Issues Surrounding Post-conviction DNA Evidence and the Pursuit of Innocence*, 62 OHIO ST. L.J. 1195, 1209–10 (2001).

76 SCHECK ET AL., *supra* note 44, at xv.

77 *See, e.g.*, *DNA Exonerations Nationwide*, INNOCENCE PROJECT, http://www.innocenceproject.org/Content/DNA_Exonerations_Nationwide.php (last visited Mar. 25, 2014) (noting that there have been 314 post-conviction DNA exonerations in the United States).

78 United States v. Nixon, 418 U.S. 683, 709 (1974) (quoting Berger v. United States, 295 U.S. 78, 88 (1935)) (alteration in original).

79 *See, e.g.*, NAS REPORT, *supra* note 37, at 41 ("DNA evidence comprises only about 10 percent of case work and is not always relevant to a particular case. Even if DNA evidence is available, it will assist in solving a crime only if it supports an evidential hypothesis that makes guilt or innocence more likely." (citation omitted)).

80 *See* Marvin Zalman, *Qualitatively Estimating the Incidence of Wrongful Convictions*, 48 CRIM. L. BULL. 221, 230 (2012); *see also* D. Michael Risinger, *Innocents Convicted: An Empirically Justified Factual Wrongful Conviction Rate*, 97 J. CRIM. L. & CRIMINOLOGY 761, 785–88 (2007) (generalizing the factual error rate for capital rape-murders to other crimes).

technology could have an even greater backward-reaching impact on the criminal justice system. Mindboggling amounts of data are being gathered and stored, although defendants currently lack the capacity to access the contents or to isolate factors that might demonstrate their innocence.[81] The discrepancy between the present collection of large amounts of data, and the now budding industry of analyzing and drawing connections from and between that data, means that there are now people in prison who will be exonerated when the data-mining tools become good enough to locate and aggregate proof of their innocence.

The DNA revolution and concomitant actual innocence movement provide glimpses of the future for digital innocence. Among other things, dozens of innocence projects have opened around the country; national conferences are held on wrongful conviction every year; professional training on the sources and prevention of wrongful convictions is widely available to defense attorneys and other criminal justice actors; and every state has enacted post-conviction DNA testing statutes often accompanied by provisions for the preservation of biological evidence. One could imagine similar efforts focused on Big Data technologies, such as the creation of a "Digital Innocence Project," which could provide legal representation in cases of actual innocence; curate online communities and develop open source resources; educate defense lawyers, prosecutors, and judges; and positively shape the law by, for instance, seeking the expansion of DNA-specific statutes to include evidence gleaned from data science.

What is needed now is more fundamental: an understanding of Big Data and mass government surveillance, and an evaluation of the legal consequences for the actually innocent. Before there were DNA-based innocence projects and specialized statutory regimes, forward-thinking advocates had to obtain a basic comprehension of DNA technology and then deploy it within the then-existing legal framework to exonerate the wrongfully convicted. To date, the literature hints that information technology could play a part in actual innocence claims, but it does not address information technology directly. Existing scholarship suggests that the focus of law can only be turned toward exoneration if the wrongfully convicted can provide hard scientific proof of innocence, but it does not focus on Big Data techniques for doing so. Some commentators point toward a future in which actual innocence embraces more than DNA technology, yet no one has engaged information technology. The following seeks to fill that gap.

---

81 *See* John Rhoton, *Getting a Grip on Storage Growth*, ZDNET (Apr. 29, 2013), http://www.zdnet.com/getting-a-grip-on-storage-growth-7000014158/.

II
The Technology of Digital Surveillance

In early June 2013, the *Guardian* and the *Washington Post* broke stories on broad data surveillance programs conducted by the FBI and the NSA.[82] The *Guardian* revealed that Verizon was the target of a secret order requiring it to turn over all phone call records gathered for a ninety-day period.[83] Other sources verified that such orders were routinely renewed in a process that had been ongoing for years.[84] The result of the order was public confirmation that the government was collecting all "telephony metadata"—transactional information such as the originating and terminating telephone numbers and the time and duration of a call—regardless of who made the call, who received the call, or where the call was made or received.[85] This was the first evidence in the United States of total detail recording of American citizens. The order was not backward looking, in that it did not involve the production of records that already existed or were related to a specific case. Rather, the order required a telecommunications provider to turn over all future records that would be generated. Because the records did not yet exist at the time of the order, there could be no possible way in which the collection was constrained by suspicion of wrongdoing.

The *Washington Post* exposé on the PRISM program followed, describing how the NSA received access to social networking data.[86] It remains unclear whether this access was "streamlined"—that is, data was made immediately available upon the NSA's request in a dedicated sandbox-server environment accessible by the government—or "direct," in the sense that the NSA had direct access to the Silicon Valley companies' own servers.[87] Apple, Facebook, Google, and other technology companies claimed in unison that the NSA was not permitted direct access to their servers, but none addressed the question of

---

82 *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, Wash. Post, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (last updated June 7, 2013, 10:51 AM); Greenwald, *supra* note 62.

83 *See* Greenwald, *supra* note 62; *infra* notes 242–48, 261–68 and accompanying text (discussing section 215 of the Patriot Act, *see infra* note 230).

84 *See, e.g.*, Kimberly Dozier & Stephen Braun, *Secret Court Scolded NSA over Surveillance in 2011, Declassified Documents Reveal*, NBC News (Aug. 22, 2013, 5:00 AM), http://www.nbcnews.com/news/us-news/secret-court-scolded-nsa-over-surveillance-in-2011-declassified-documents-reveal-v20131077.

85 *See* Greenwald, *supra* note 62.

86 *See* Gellman & Poitras, *supra* note 82.

87 *Id.*

streamlined access.[88] This collective silence is telling since streamlined, indirect access may approach effective direct access. As discussed later, all of this is permitted by aggressive stances on statutory and constitutional interpretation.[89]

In the end, it may not matter whether and how much Silicon Valley companies have been complicit in mass surveillance. Not content with front-door entry, the NSA has accessed Big Data firms' unencrypted data through a backdoor tap on the fiber-optic cables between server farms.[90] Moreover, the NSA secretly cracked or circumvented much of the world's encryption technology, and it has embarked on a program of coaxing Internet companies to hand over their master encryption keys.[91] This Part provides an overview of the technology that allows mass surveillance to happen, while the next Part discusses the ostensible legal grounds for the government to engage in dragnet digital surveillance. Again, our goal is not to justify the resulting accumulation and examination of data but instead to provide the basis for defense access and use of this information.

A. Growth of Databases

The most significant characteristic of databases relevant to digital innocence is the rate of storage increase.[92] Growth in storage capacity means the data that might exonerate a defendant is stored but not necessarily parsed.[93] That data might reside in a telecommunication provider's cell-site location information, or in the photographs of a user-generated content website, or in e-mail, or text messages.[94] The odds of storing a piece of exonerating evidence must grow at least linearly as a function of the increase in storage capacity (i.e., storing more of what is already being stored) and as a function of the increase in types of information stored (i.e., storing additional kinds of infor-

88 *See* Kevin Poulsen, *Zuckerberg, Page: NSA Has No "Direct Access" to Facebook or Google Servers*, WIRED (June 7, 2013, 7:40 PM), http://www.wired.com/threatlevel/2013/06/prism-google-facebook/.

89 *See infra* Part III.

90 *See* Nicole Perlroth & John Markoff, *A Peephole for the N.S.A.*, N.Y. TIMES, Nov. 26, 2013, at B1; Craig Timberg et al., *Microsoft Moves to Boost Security*, WASH. POST, Nov. 27, 2013, at A1.

91 James Ball et al., *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN WKLY. (Sept. 5, 2013), http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security/.

92 *See* John Foley, *As Big Data Explodes, Are You Ready for Yottabytes?*, FORBES (June 21, 2013, 10:23 AM), http://www.forbes.com/sites/oracle/2013/06/21/as-big-data-explodes-are-you-ready-for-yottabytes/ (discussing growing data demands by the U.S. Department of Defense and business).

93 *See* Rhoton, *supra* note 81 (arguing that businesses have incentive to store data which they may not even know how to analyze yet).

94 *See* Foley, *supra* note 92 (discussing how "burgeoning databases" force organizations to "rethink their IT infrastructures").

mation). Actually, there is reason to believe that the ability to prove innocence digitally will increase more than linearly. Bigger databases allow algorithms to make more connections,[95] and more connections yield the ability to monetize more data, which in turn creates even bigger databases.[96]

Storage has now reached the point where the product of ubiquitous surveillance can be stored on a semi-permanent basis, as datacenters have gotten bigger and better at a seemingly ever-increasing rate.[97] The PRISM program and like government surveillance require massive data storage. "Full-take" systems, such as the United Kingdom's TEMPORA program, also require enormous storage because they ingest everything passing through a given conduit. Moreover, Congress is once again considering the Cyber Intelligence Sharing and Protection Act (CISPA), which would permit sharing of intelligence information with corporations, and vice versa, supposedly to combat cyber-threats.[98] This form of deep data mining can only function, however, if sufficient storage is available to save the data pending use.

Unsurprisingly, there are reports of large datacenters constructed with precisely this sort of data mining in mind. Termed the largest in the country, the NSA's mammoth facility in Bluffdale, Utah, is intended to store and parse data captured from worldwide electronic communications.[99] When completed, the Bluffdale Center will be five times the size of the U.S. Capitol.[100] According to reports, the project was ready for operation in September 2013. The information to be parsed includes "complete contents of private e-mails, cellphone calls, and Google searches, as well as all sorts of personal data trails—parking receipts, travel itineraries, bookstore purchases"—and much more.[101]

---

95 *See* Greenberg, *supra* note 67 ("Using what will likely be the world's fastest supercomputer and the world's largest data storage and analysis facility, the NSA plans to comb unimaginably voluminous troves of messages for patterns they could use to crack AES . . . .").

96 *See* Rhoton, *supra* note 81 (stored data need to be backed up, maintained, and "replicated and reused for different purposes").

97 *See* Mark Hachman, *Big Getting Bigger, Uptime Data Center Survey Finds*, SLASHDOT (Apr. 25, 2013), http://slashdot.org/topic/datacenter/big-getting-bigger-uptime-data-center-survey-finds/ ("[T]he conclusion of preliminary data collection by the Uptime Institute . . . found that the largest data centers are receiving the largest budget increases.").

98 *See* H.R. 3523, 112th Cong. (2d Sess. 2012) (proposed law allowing technology and manufacturing companies to share data with the U.S. government); *see also* Jeff Nesbit, *CISPA Rolls Along*, U.S. NEWS & WORLD REP. (May 6, 2013), http://www.usnews.com/news/blogs/at-the-edge/2013/05/06/cispa-rolls-along.

99 *See* Greenberg, *supra* note 67.

100 James Bamford, *The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)*, WIRED (Mar. 15, 2012, 7:24 PM), http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.

101 *Id.*

Some context is useful to appreciate the scale of the Bluffdale Center. From 1986 to 2007, worldwide computing capacity increased at a rate of 58% per year.[102] While the bulk of information storage remained analog until the year 2000, a dramatic shift occurred over the next seven years, with digital storage accounting for well over 90% of worldwide information storage. By contrast, all information stored on paper decreased from 0.33% of the worldwide total in 1986 to 0.007% in 2007.[103] It is also helpful to understand the sheer quantity of information stored, using the following metric.

1,000 megabytes = 1 gigabyte (10^9)
1,000 gigabytes = 1 terabyte (10^{12})
1,000 terabytes = 1 petabyte (10^{15})
1,000 petabytes = 1 exabyte (10^{18})
1,000 exabytes = 1 zettabyte (10^{21})
1,000 zettabytes = 1 yottabyte (10^{24})

Typically, the capacity of a hard drive in a personal computer (PC) is measured in gigabytes, where 1 "gig" holds several hundred thousand pages of text. According to a study published in *Science*, "[t]he total amount of information [in the world] grew from 2.6 optimally compressed exabytes in 1986 to 15.8 in 1993, over 54.5 in 2000, and to 295 optimally compressed exabytes in 2007."[104] The Bluffdale Center will store yottabytes of data, that is, thousands of times the amount of all human data existing in 2007.[105] Yet the government's data-storage capacity lags far behind the ability, and motivation, of the combined private sector. Facebook and Google are in the midst of enormous datacenter construction projects.[106] Google is building its new datacenters in Finland, where the cold weather permits the servers to lose heat more efficiently.[107]

The revolution in storage capacity is the result of larger and better datacenters, as well as improvements in storage technology, more efficient data management algorithms, and the explosion of cheap,

---

102 Martin Hilbert & Priscila López, *The World's Technological Capacity to Store, Communicate, and Compute Information*, 332 SCIENCE 60, 63–64 (2011).

103 *Id.* at 62.

104 *Id.*; *see* Jon Stewart, *Global Data Storage Calculated at 295 Exabytes*, BBC NEWS (Feb. 11, 2011, 6:25 AM), http://www.bbc.co.uk/news/technology-12419672 (noting that 295 exabytes "is the equivalent of 1.2 billion average hard drives").

105 *See* Greenberg, *supra* note 67.

106 *See* Stacey Higginbotham, *Data Center Rivals Facebook and Google Pump $700M in New Construction into Iowa*, GIGAOM (Apr. 23, 2013, 1:09 PM), http://gigaom.com/2013/04/23/data-center-rivals-facebook-and-google-pump-700m-in-new-construction-into-iowa/ (discussing Facebook's $300 million investment and Google's $400 million investment in additional data centers in Iowa).

107 Katie Fehrenbacher, *Cool Finnish Weather the New Hotness for Data Centers*, GIGAOM (Sept. 12, 2011), http://gigaom.com/2011/09/12/cool-finnish-weather-the-new-hotness-for-green-data-centers/.

often portable storage in the hands of consumers.[108] Gone is the necessary connection of data to a given location. Data can be shifted smoothly from virtual server to virtual server.[109] The movement and allocation of data as needed permits efficiencies in data processing and produces maximum accessibility. In addition, bandwidth has undergone a worldwide increase in throughput, making accessing data remotely as or more efficient than accessing it locally.[110]

The result of this cluster of technologies is termed "the cloud," in somewhat passé technological parlance.[111] This phrase is meant to convey the idea that data can be remotely stored, processed, and accessed in a way that outcompetes local processing or storage.[112] The result has been a transformation of computing away from the PC paradigm.[113] Cloud computing has facilitated the rise of tablets and smartphones, which focus on smooth presentation of information that is parsed and stored remotely.[114] In a sense, this is less a revolution than a swing of the pendulum. When transfer costs are higher than processing costs, local processors and storage become more important. When transfer costs are lower than processing costs, however, remote storage and processing dominate.

An example drawn from contemporary technology literature may further clarify the scope of these changes in storage capacity. "Hadoop" is an open-source platform for data storage.[115] A single one of Facebook's Hadoop clusters was reported to include 4,000 machines with over 100 petabytes of data.[116] (For comparison, 1 petabyte

---

108 *See* Quentin Hardy, *Big Data Done Cheap*, N.Y. TIMES (Mar. 4, 2013, 8:00 AM), http://bits.blogs.nytimes.com/2013/03/04/big-data-done-cheap/? (discussing development of data storage cards that can make ordinary servers, costing thousands of dollars, perform activities currently done on multimillion-dollar racks of computers).

109 *See* Chris Poelker, *Will Cloud Computing Kill the Storage Area Network?*, COMPUTER WORLD (Dec. 11, 2012, 6:00 AM), http://blogs.computerworld.com/data-storage/21360/will-private-cloud-kill-storage-area-network (discussing the availability of cloud storage).

110 *Cf.* Jon Brodkin, *Bandwidth Explosion: As Internet Use Soars, Can Bottlenecks Be Averted?*, ARS TECHNICA (May 1, 2012, 12:40 PM), http://arstechnica.com/business/2012/05/bandwidth-explosion-as-internet-use-soars-can-bottlenecks-be-averted/.

111 *See* Brian Braiker, *Understanding "Cloud Computing,"* NEWSWEEK, June 20, 2008, http://www.newsweek.com/technology-understanding-cloud-computing-90829.

112 *See id.*

113 *See* Joshua Gruenspecht, *"Reasonable" Grand Jury Subpoenas: Asking for Information in the Age of Big Data*, 24 HARV. J.L. & TECH. 543, 548 (2011) (discussing how the increase in data storage has "practically eliminated the requirement that users clean out their email inboxes and Internet browsing history periodically in order to free up storage"); Ben Worthen et al., *H-P Explores Quitting Computers as Profits Slide*, WALL ST. J., Aug. 19, 2011, at A1 (discussing H-P's decision—in the face of declining revenue—to shutdown its tablet and smartphone operations, and considerations to abandon efforts to sell computers).

114 *See* Worthen et al., *supra* note 113.

115 *See* Katherine R. Lewis, *What the Heck Is Hadoop?*, FCW (Mar. 25, 2013), http://fcw.com/articles/2013/03/25/what-is-hadoop.aspx.

116 Cade Metz, *Meet the Data Brains Behind the Rise of Facebook*, WIRED (Feb. 4, 2013, 6:30 AM), http://www.wired.com/wiredenterprise/2013/02/facebook-data-team/.

was said to be the equivalent of 250 billion pages of text.)[117] The Hadoop clusters permit storage of activities of Facebook's approximately one billion users.[118] More importantly, the Hadoop platform permits clusters to expand to capture more data as it becomes available.[119] As a result, there are very few functional limits to the amount of data that may be kept even if there is no immediate use for the information. This feature makes the technology particularly attractive to companies such as Facebook, which must parse amounts of data that continuously expand past the ability of any single datacenter to handle.[120]

Facebook's new Hadoop-based system came out in February 2013. Coincidentally or not, the system is called "Prism"—the same name used by the NSA for the system implemented by Silicon Valley companies to provide the agency smooth access to social media data. According to the technology press, Facebook's Prism permitted a qualitative shift in how the information can be processed and parsed.[121] Each research team can have faster access to the entire distributed dataset as the system determines the data necessary for a specific task and then copies that data to a specific datacenter.

The examples of the cross-datacenter Hadoop cluster and the Facebook Prism system underscore several points necessary for our conception of digital innocence. Technology companies in general, and social media companies in particular, are dedicated to collecting and preserving data about human relationships on an unprecedented scale. Not only is the amount of this information increasing nonlinearly, but the ability to parse this information is also moving closer to real time. Many of these systems are open source or freely licensable, meaning that as soon as one company develops the capacity to expand significantly its data-storage and parsing capabilities, other companies can follow suit at lower costs.[122]

With increases in data storage, data flexibility, and data-processing efficiency come new tools that use the data to produce meaningful results for the prosecution or defense. One possible example is the new RIOT (rapid information overlay technology) system modeled by the security firm Raytheon.[123] RIOT gathers geolocation data from a

---

117 Vance, *supra* note 61.

118 *See id.*

119 *Id.*

120 *See* Metz, *supra* note 116.

121 *See id.*

122 *See* Cade Metz, *Spark: Open Source Superstar Rewrites Future of Big Data*, WIRED (June 19, 2013, 6:30 AM), http://www.wired.com/wiredenterprise/2013/06/yahoo-amazon-amplab-spark/all/ (discussing Spark, an open-source data crunching platform 100 times faster than Hadoop).

123 Alex Fitzpatrick, *Security Firm Can Use Social Media to Track People's Movements*, MASHABLE (Feb. 11, 2013), http://mashable.com/2013/02/11/social-media-tracking/.

range of social media platforms to provide an in-depth picture of the ongoing life of the target.[124] For instance, the system identified that a test subject used the gym every Monday at 6:00 AM.[125] Obviously, this would be an extremely useful fact for anyone who was interested in finding the subject or in gaining access to his laptop.[126]

These examples highlight ongoing increases in the ability to store and parse data. But they are not offered as the latest development—nor could they be, given the pace of invention. Rather, the point is that this increase in the ability to store data now, coupled with the increase in the ability to leverage data already stored, can yield proof of innocence in criminal cases. Social media has been critical to some prosecutions.[127] We predict that it could be central to future trial and post-conviction exoneration efforts, as the increasingly sophisticated tools currently used in the commercial technology sector come into widespread use by legal advocates.[128] This will occur over the ever-larger databases made possible by increases in data-storage capacity and flexibility.

B. Increase in Types of Information

There has also been a shift in the sorts of information stored and collected. Specifically, the past several years have seen significant increases in at least three types of data that could bear on the question of digital innocence: comprehensive browser-tracking information, geolocation and mobile location information, and social network mapping data. The first, comprehensive browser tracking, represents a change in quantity and quality of data recording. Nearly everything citizens do online is tracked and logged by advertisers,[129] which now employ more data about users' online behavior than ever before. A prime example is Google, which not only tracks user behavior over its own services (e.g., YouTube, Gmail, and the Google flagship search engine) but also behavior on any site that carries Google advertising. Because this represents a very high percentage of the active commer-

---

124 *Id.*

125 Ryan Gallagher, *Defence Giant Builds "Google for Spies" to Track Social Networking Users*, THE GUARDIAN, Feb. 10, 2013, at A1.

126 *See id.*

127 *See* Justin P. Murphy & Adrian Fontecilla, *Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues*, 19 RICH. J.L. & TECH. 1, 23–24 (2013) (discussing cases in which MySpace and Facebook accounts contained significant evidence used by prosecution).

128 *See* MANYIKA ET AL., *supra* note 18, at 2.

129 *See* Valentino-Devries & Singer-Vine, *supra* note 64 (noting that of "roughly 70 popular websites that request a login . . . more than a quarter of the time, the sites passed along a user's real name, email address or other personal details, such as username, to third-party companies").

cial Internet,[130] Google knows the comprehensive online habits of a huge proportion of citizens.[131] But Google is not the only tracker. Most popular webpages transmit to multiple tracking entities.[132] These entities, and the advertisers to whom they sell the data, use comprehensive browser-tracking information for targeted behavioral advertising—that is, advertisements based on the user's past browsing and purchasing habits.[133] This information can be as useful to prosecutors as it is to advertisers. Comprehensive browser-tracking data, as well as e-mail account-use data, search data, and other information gathered through comprehensive consumer surveillance, are routinely sought and obtained by state or federal prosecutors, usually without resort to a warrant.[134]

Another important category is geolocation data, which stems from the fact that most mobile devices now offer global positioning system (GPS) capability and nearly all such devices must speak to one or more cell towers.[135] This cell-site location information (CSLI) or GPS information is of significant value to online services and advertisers because it permits narrower tailoring of advertisements based on the real-world location of the client, while also providing a window into the offline, real-world habits and economic behavior of the cellphone owner.[136] The resulting CSLI or GPS information is of interest to law enforcement as well, since it can establish the real-world location of a cellphone and, at least presumably, the presence of the owner.[137]

For exactly the same reason, suspects and defendants may be interested in CSLI and cellphone GPS data as a means to establish the

---

130 *See* Robert Epstein, *Google's Gotcha*, U.S. NEWS & WORLD REP. (May 10, 2013), http://www.usnews.com/opinion/articles/2013/05/10/15-ways-google-monitors-you.

131 *See id.*

132 *See* Ellen Messmer, *Study: 86% of Top Websites Expose Visitors to Third-Party Tracking Cookies*, NETWORK WORLD (June 28, 2012, 12:47 PM), http://www.networkworld.com/news/2012/062812-tracking-cookies-260544.html.

133 *See id.*

134 *See* Ryan Gallagher, *Microsoft Finally Releases Info About Law Enforcement Shooting on Skype, Other User Data*, SLATE (Mar. 21, 2013, 2:38 PM), http://www.slate.com/blogs/future_tense/2013/03/21/microsoft_transparency_report_details_law_enforcement_requests_for_skype.html?wpisrc=obinsite ("The report reveals that in 2012, Microsoft and Skype received a total of 75,378 law enforcement requests . . . .").

135 *See* Ellen Nakashima, *"Tower Dumps" Give Police Masses of Cellphone Data*, WASH. POST, Dec. 9, 2013, at A1.

136 *See* Anton Troianovski, *Phone Firms Sell Data on Customers*, WALL ST. J., May 22, 2013, at B1.

137 *See* Hansen, *supra* note 58; *see also* Andrew E. Kramer, *Ukraine's Opposition Says Government Stirs Violence*, N.Y. TIMES, Jan. 22, 2014, at A6 (protesters received threatening text message from ersatz government cellphone tower).

location of a range of actors important to a criminal case.[138] An individual's own cell-site location information may provide an alibi straight off,[139] perhaps resulting in no charges being brought at the outset of a case. But CSLI might also be useful in later exoneration cases. Among other things, it can establish the presence or absence of witnesses. This information might identify witnesses who could support a defense, for instance, or it might demonstrate that a prosecution witness was not in a place or position to observe matters within the scope of his or her testimony.

A user's own CSLI may be obtained from an Internet service provider (ISP), but information about other users is difficult to get through a traditional subpoena to an ISP.[140] There are other options, however, based on developments such as the rise of geolocation services that share information between consumers.[141] A range of computer software applications (i.e., "apps") exists to tell consumers where their friends are in real time.[142] This information can then be retrieved by anyone in the social group. Other geolocation information is simply embedded in files and can be read by anyone who knows where to look.[143] A good example is uploaded photographs, which may have time and geolocation information embedded in the uploaded file, often without the knowledge of an amateur photographer.[144] Pictures that place a defendant in a specific place at a specific time may be key to his exoneration.

A third category of information, social media, has played an increasing role in investigations and prosecutions. According to a LexisNexis survey of law enforcement personnel, four out of five respondents use social networking sites to aid investigations.[145] The

---

138 *See Cell Phone Tower Records Can Be Crucial in Court Cases*, GAZETTE.NET (Nov. 14, 2012), http://www.gazette.net/article/20121114/NEWS/711149556/cell-phone-tower-records%20-can-be-crucial-in-court-cases&template=gazette.

139 *See* Michael Brick, *Cellphone Records Help to Clear a Murder Suspect*, N.Y. TIMES, Aug. 24, 2007, at B3 ("A man was cleared of murder charges yesterday after offering cellular telephone records [containing his location] as alibi evidence.").

140 *See infra* Part V.A.2.

141 *See, e.g.*, Adam Popescu, *3 Must-Have Geolocation Apps*, MASHABLE (May 8, 2013), http://mashable.com/2013/05/08/top-geolocation-apps-you-need/.

142 *See* John D. Sutter, *What's Next for "Check-in" Apps?*, CNN (Aug. 27, 2010, 10:44 AM), http://www.cnn.com/2010/TECH/innovation/08/27/checkin.apps/index.html.

143 *See* Mathew J. Schwartz, *7 Facts About Geolocation Privacy*, INFO. WK. (Aug. 20, 2012, 12:13 PM), http://www.informationweek.com/security/risk-management/7-facts-about-geolocation-privacy/d/d-id/1105877? ("While smartphone users may realize that their devices have the capability to track their whereabouts, what they may not know is that other devices, such as new cameras, also have the capability to know their location and add location information to a photograph . . . ." (internal quotation marks omitted)).

144 *See id.*

145 *See* LEXISNEXIS, LAW ENFORCEMENT PERSONNEL USE OF SOCIAL MEDIA IN INVESTIGATIONS: SUMMARY OF FINDINGS 1, http://images.solutions.lexisnexis.com/Web/LexisNexis/Infographic-Social-Media-Use-in-Law-Enforcement.pdf.

value of social media data comes from its availability, its specificity when tied to Internet protocol (IP) logs or geolocation information, and the fact that it maps the social networks that often serve as the broader social contexts for alleged criminal wrongdoing.

By enhancing pre-digital media, it is also possible to data mine the past.[146] Although analog recordings of video and sound have supported convictions for years, the tapes are often blurry or the sounds unclear and therefore subject to challenge. The situation has changed with the marriage of digital technology with sophisticated search algorithms.[147] This technology may help reveal more information from background noise on analog-taped telephone calls or other recordings than was ascertainable at the time of trial. Likewise, state-of-the-art graphics programs can resolve blurred features on pre-digital tapes, which then might show that the wrong person was convicted.[148]

These new types of information could play an ever-larger part in defense and post-conviction exoneration efforts.[149] Obtaining access to data will be an impediment in such efforts,[150] although presumably the hurdle will be at its lowest for broadly shared social media.[151] Information from social media is often publicly posted, publicly stored, and even publicly searchable for a limited time. It may not be permanently stored outside of the virtual wall of the social network itself, however, and semi-closed ecosystems like Facebook can be hard to research. But tweets and blogs are often stored by wayback machines

---

146 *See, e.g.*, Maurice Possley, *Roberto Cuevas*, NAT'L REGISTRY OF EXONERATIONS, https://www.law.umich.edu/special/exoneration/Pages/casedetail.aspx?caseid=3928 ("[The defendant's] appellate attorney informed the district attorney's office that another enhanced version of the video recording had been made using state of the art technology that allowed for the creation of still photographs. The attorney contended the new photographs showed that [the defendant] was not involved.").

147 *See* Jeremy Brown, *Pan, Tilt, Zoom: Regulating the Use of Video Surveillance of Public Places*, 23 BERKELEY TECH. L.J. 755, 762 (2008) ("The technological constraints that prevented misuse of analog surveillance cameras—grainy images, limited storage capacity, and difficult duplication—no longer impede video surveillance."); *cf.* Ric Simmons, *Technology-Enhanced Surveillance by Law Enforcement Officials*, 60 N.Y.U. ANN. SURV. AM. L. 711, 712 (2005) ("These surveillance tools . . . do not provide extraordinarily intrusive information . . . .").

148 For example, Brian Avery was convicted in 1994 of armed robbery based in part on surveillance videos. Years later, digital enhancement techniques showed that the person in the videotape was three inches shorter than Avery. *See* State v. Avery, 807 N.W.2d 638, 654 (Wis. Ct. App. 2011) (granting a new trial on the basis of the new evidence), *rev'd*, 826 N.W.2d 60, 76–77 (Wis. 2013) (ruling new trial not warranted).

149 *See* Robert D. Richards, *Compulsory Process in Cyberspace: Rethinking Privacy in the Social Networking Age*, 36 HARV. J.L. & PUB. POL'Y 519, 523 (2013).

150 *See, e.g.*, Ethan Bronner, *Lawyers, Saying DNA Cleared Inmate, Pursue Access to Data*, N.Y. TIMES, Jan. 4, 2013, at A1.

151 *See* Gruenspecht, *supra* note 113, at 544 ("The advent of mass digital storage, however, has significantly increased the chances that records of any given document exist and is increasingly unifying the locations in which those records can be found.").

or Internet archives,[152] and in some cases, Google itself keeps a record of an archived page.[153] This quasi-public data could be an important source of exculpatory evidence as access and search tools grow in strength.

C. Aggregation and Cross-Referencing of Databases

At first, digital innocence may be proved by single "smoking gun" pieces of evidence culled from now-colossal datasets. But just as guilt is often established by piecing together different pieces of data into a convincing pattern, innocence might be demonstrated in a similar fashion by linked data and pattern analysis. The more linked data the system can access, the more patterns that may emerge, even from unlikely concatenations of data points. This methodology is most advanced in advertising. As mentioned, advertisers have access to large commercial databases, providing information they sell to one another in a semi-closed ecosystem. Access to this ecosystem is either through deals for entire databases or by access to databases that draw on these stores. The databases are increasingly linked, permitting an advertiser to target potential customers based not just on their physical proximity to the seller's location, their web-surfing pattern, their credit card purchasing history, or their recent life events (e.g., births, funerals, and vacations), but rather on a combination of all this information.[154]

Connected databases yield insights that individual databases do not. Knowing where someone is in real space may augment information about his browsing history, while knowing a user's social network can supplement information about his purchasing history.[155] Advertisers routinely target those consumers who are thought leaders, whose purchasing decisions affect others in their social network, by cross-referencing knowledge of purchasing history with social network information. This permits advertisers to optimize advertising efforts by focusing customer services and perks on influential members of a network.[156] The same type of cross-linking is a common feature of law enforcement's use of data. Police start by examining text messages, cellphone connections, and social networks. The connection of com-

---

152 *See, e.g.*, *About the Internet Archive*, INTERNET ARCHIVE, http://archive.org/about/ (last visited June 28, 2013).

153 *See Google Cached Pages: What Are Cached Pages?*, GOOGLE GUIDE, http://www.googleguide.com/cached_pages.html (last visited Jan. 16, 2014).

154 *See* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1957 (2013).

155 *See* Ashkan Soltani et al., *NSA Using Online "Cookies" to Find Targets*, WASH. POST, Dec. 11, 2013, at A1.

156 This practice became so widespread that rules governing sponsored advertising were expanded to include bloggers who received gifts from a company whose products they reviewed. *See* Tim Arango, *Soon, Bloggers Must Give Full Disclosure*, N.Y. TIMES, Oct. 6, 2009, at B3.

munication history (i.e., text, voice, and Internet) with geolocation data and social network mapping can be a heady technique.[157]

The question is whether defense or later exoneration efforts can also benefit from data aggregation and cross-linking. As always, access constraints are a problem, but the barrier is decreasing over time. Already many of these databases can be accessed by anyone with a limited liability company and a credit card. For example, a privacy advocate purchased for $5 the personal details of one million Facebook users, from a seller who allegedly employed Facebook apps to gather the information.[158] Facebook's embarrassment was not at the fact of data sales, which are one of its core offerings, but at the publicity concerning the ease with which anyone with a few dollars can buy and sell large amounts of user data.[159]

The impact of cross-linking and aggregation is strengthened by the advent of a new generation of wearable computing technology that increasingly links online data with data about the real world. Cellphones report real-space location and correlate it with browsing history,[160] with cellphone apps providing rich information to both app developers and government actors.[161] Now consider technology like Google Glass, which permits a user to record and upload a constant stream of information about the people and places around her.[162] It is hard to overstate the potential impact on criminal justice from millions of citizens wearing this technology, particularly since Google is aware of the location and status of each person who wears one of its products.[163] Imagine the possibilities for both government

---

157 *See, e.g.*, Memorandum in Support of Motion for Full Discovery Regarding the Facts and Circumstances Underlying Surveillance at 16–17, 21–25, 31, 49, United States v. Mohamud, 941 F. Supp. 2d 1303 (D. Or. 2013) (No. 3:10-cr-00475-KI) [hereinafter Mohamud Motion] (describing various techniques used by law enforcement).

158 *See* Ben Weitzenkorn, *Details of 1 Million Facebook Users Sold for $5*, NBC NEWS (Oct. 26, 2012, 4:36 PM), http://www.nbcnews.com/technology/details-1-million-facebook-users-sold-5-1C6714691.

159 *See* Bogomil Shopov, *Mixed Feelings After My Conversation with Facebook.(updated)*, A GROWTH HACKER BLOG, http://talkweb.eu/mixed-feelings-after-my-conversation-with-facebook/ (last visited Mar. 25, 2014).

160 *See* Charles Arthur, *iPhone Keeps Record of Everywhere You Go*, THE GUARDIAN (Apr. 20, 2011), http://www.theguardian.com/technology/2011/apr/20/iphone-tracking-prompts-privacy-fears; Greg Kumparak, *AT&T Considers Selling Your Browsing History, Location, and More to Advertisers. Here's How to Opt Out*, TECHCRUNCH (July 5, 2013), http://techcrunch.com/2013/07/05/att-considers-selling-your-browsing-history-location-and-more-to-advertisers-heres-how-to-opt-out/.

161 *See* James Glanz et al., *Spy Agencies Tap Data Streaming from Phone Apps*, N.Y. TIMES, Jan. 28, 2014, at A1.

162 *Google Glass—What It Does*, GOOGLE, http://www.google.com/glass/start/what-it-does/ (last visited Aug. 25, 2013).

163 *See* Julia Angwin & Jennifer Valentino-Devries, *Apple, Google Collect User Data*, WALL ST. J. (Apr. 22, 2011), http://online.wsj.com/news/articles/SB10001424052748703983704576277101723453610.

intrusion and proof of innocence if a simple query to Google would reveal all wearers of Glass within 300 meters of the location of an incident, along with an indication as to whether those people were recording at the time of the event. The tools are simply too good for law enforcement to pass up willingly. The issue is whether the law will allow government to exploit this data source and, if so, whether the information and related tools will be available to defendants in the quest to prove their innocence.

III
The Law of Digital Surveillance

Given the technological basis for digital innocence—as a function of the growth in database size, the wealth of new types of information stored, and the increase in the ability to connect more data points to new types of information—this Part addresses the legal foundation for the current state of government surveillance, including how the government got access to Big Data. This implicates elements of standard Fourth Amendment doctrine as well as the shadowy regime of government surveillance in service of national security. The jurisprudence helps frame a discussion of the legal basis for and impediments to defense access to proof of digital innocence.

A. Surveillance and the Fourth Amendment

The government's authority to conduct digital surveillance and draw upon the fruits of Big Data traces back to relatively low-tech eavesdropping and wiretapping. For decades, these practices were legally uncontroversial based on the theory that listening devices without an accompanying physical trespass did not violate the Fourth Amendment.[164] Even when the Supreme Court held that federal legislation precluded the introduction at trial of conversations overheard on wiretaps by law enforcement,[165] the Justice Department took the position that it was still permissible to conduct warrantless electronic surveillance to gather intelligence for national security purposes.[166]

In 1967, the Court's decision in *Katz v. United States*[167] rejected the prevailing doctrine that had allowed warrantless wiretapping but now "ignore[s] the vital role that the public telephone has come to play in private communication."[168] In the ensuing decades, the *Katz*

164 *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 465–66 (1928).

165 *See* Nardone v. United States, 308 U.S. 338, 339 (1939); Nardone v. United States, 302 U.S. 379, 380–85 (1937).

166 *See, e.g.*, Herbert Brownell, Jr., *The Public Security and Wire Tapping*, 39 Cornell L.Q. 195, 197–200 (1954); Richard G. Donnelly, *Comments and Caveats on the Wire Tapping Controversy*, 63 Yale L.J. 799, 799–801 (1954).

167 389 U.S. 347 (1967).

168 *Id.* at 352.

test for when state action implicates the Fourth Amendment would be interpreted as requiring an expectation of privacy that "society is prepared to recognize as 'reasonable.'"[169] Somewhat ironically, the case that safeguarded conversations by telephone, one of the seminal breakthroughs in modern communications, did not provide much protection against subsequent advances of technology. More often than not, the Supreme Court has held that a given investigative technique does not violate a reasonable expectation of privacy and therefore does not trigger the Fourth Amendment at all.[170]

Two features of this jurisprudence are especially important for electronic surveillance: (1) data about data (i.e., metadata) may be considered deficient of any content that might engender a privacy expectation,[171] and (2) data may lose the protection afforded by a reasonable expectation of privacy once the information is provided to third parties.[172] Thus, the government may eavesdrop on otherwise private conversations in residences transmitted by wired informants,[173] obtain records detailing an individual's otherwise private financial information,[174] and install pen registers on home phone numbers to determine whom someone is calling.[175] In the latter

---

169 *Id.* at 361 (Harlan, J., concurring); *see also* Erik Luna, *The Katz Jury*, 41 U.C. DAVIS L. REV. 839, 842–43 (2008) (discussing the basis and evolution of the *Katz* standard).

170 *See, e.g.*, Illinois v. Caballes, 543 U.S. 405, 407–10 (2005) (use of a narcotics-detection dog during a lawful traffic stop); Florida v. Riley, 488 U.S. 445, 450–52 (1989) (observations of a private greenhouse from a helicopter 400 feet away); California v. Greenwood, 486 U.S. 35, 39–44 (1988) (warrantless search and seizure of garbage left on the street for collection); United States v. Dunn, 480 U.S. 294, 300–03 (1987) (investigation, without physically entering, of a barn outside the curtilage of a private house); California v. Ciraolo, 476 U.S. 207, 212–15 (1986) (observations of a private backyard from a private airplane); Dow Chem. Co. v. United States, 476 U.S. 227, 234–39 (1986) (aerial photography taken from public navigable airspace); Oliver v. United States, 466 U.S. 170, 176–77 (1984) (government intrusion on open fields); United States v. Jacobsen, 466 U.S. 109, 118–26 (1984) (DEA agents' warrantless search and seizure of a package after the owner's privacy interest was compromised); United States v. Place, 462 U.S. 696, 700–07 (1983) (subjecting personal luggage to a "canine sniff").

171 *See* Smith v. Maryland, 442 U.S. 735, 741–43 (1979).

172 *See* United States v. Miller, 425 U.S. 435, 442–44 (1976).

173 *See* United States v. White, 401 U.S. 745, 746–54 (1971).

174 *See* United States v. Payner, 447 U.S. 727, 741–42 (1980) (loan guarantee); *Miller*, 425 U.S. at 440–45 (copies of checks and deposit slips retained by bank); Couch v. United States, 409 U.S. 322, 335–36 (1973) (financial records given to accountant).

175 *See Smith*, 442 U.S. at 741–46. As defined by statute, a pen register "records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3) (2012). By contrast, a trap and trace device "captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4). Neither pen registers nor trap and trace devices are supposed to include the contents of communications. Although *Smith* only concerned pen registers, its logic has been applied to trap and trace devices as well. *See, e.g.*, United States v. Hallmark, 911 F.2d 399, 402 (10th Cir. 1990) (citing *Smith* for the proposition that "[t]he installation and use of a pen register and trap and trace device is

instance, the Supreme Court's decision in *Smith v. Maryland* held that, by conveying numerical information to a phone company, an individual "assumed the risk" this information would be provided to government agents.[176] Given that Big Data is the aggregation of data about data, and that all data online is handed off to ISPs in some form or another, the foregoing principles have been (over)extended to place the entire Internet outside of meaningful constitutional protections, thereby allowing massive, suspicionless, and even prospective data gathering by government.

The advance of technology itself has also been problematic. At times, the Supreme Court seems to sense that reasonable expectations can be corroded by a conclusory determination that a new technology affords no privacy. In fact, a few post-*Katz* decisions have found the Fourth Amendment applicable to high-tech surveillance. In *Kyllo v. United States*, the Court examined the use of a thermal imager to scan for heat emanating from a home, a technique that allowed officers to infer a suspect was growing marijuana inside.[177] "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without [a physical intrusion] constitutes a search," the *Kyllo* Court concluded, "at least where (as here) the technology in question is not in general public use."[178] To hold otherwise "would leave the homeowner at the mercy of advancing technology."[179]

This insight continues to be strongly tested, however, since Big Data technology allows the government not only to peer into the home but also to track individuals everywhere they go. Based on a pair of electronic-beeper cases from the 1980s, law enforcement had been permitted to deploy tracking devices without a warrant so long as the information concerned public movements.[180] Nonetheless, the Supreme Court did warn that "dragnet-type law enforcement practices" might raise "different constitutional principles,"[181] a proviso that would linger for nearly three decades.

In a 2012 case, *United States v. Jones*,[182] law enforcement had attached a GPS tracking device to the defendant's vehicle for the pur-

---

not a 'search' requiring a warrant pursuant to the Fourth Amendment"); S. Bell Tel. & Tel. Co. v. Hamm, 409 S.E.2d 775, 780 (S.C. 1991) ("In light of the holding in *Smith*, we cannot hold that the telephone number of the equipment from which a call has been placed is entitled to more privacy than the telephone numbers called by someone.").

176 *Smith*, 442 U.S. at 744–45.

177 533 U.S. 27, 29–30 (2001).

178 *Id.* at 34.

179 *Id.* at 35.

180 *See* United States v. Karo, 468 U.S. 705 (1984); United States v. Knotts, 460 U.S. 276 (1983).

181 *Knotts*, 460 U.S. at 284.

182 132 S. Ct. 945 (2012).

pose of following his public movements over the course of four weeks.[183] The Supreme Court concluded that the installation and use of the device constituted a search, although not based on the reasoning in *Katz*. According to Justice Antonin Scalia, "the *Katz* reasonable-expectation-of-privacy test . . . *added to*, not *substituted for*, the common-law trespassory test."[184] Here, the Fourth Amendment was triggered by the government's physical occupation of private property—that is, the placement of the device on the defendant's car—for the purpose of obtaining information.

In an important concurrence,[185] Justice Sonia Sotomayor agreed that the government had unconstitutionally usurped private property in order to conduct surveillance of the defendant. But she expressed concern that the government could obtain the same information "by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones," which could provide "a wealth of detail about [an individual's] familial, political, professional, religious, and sexual associations."[186] The data could be stored and efficiently mined by government in covert processes that evade the non-legal checks on abusive tactics—namely, limited resources and popular criticism—with the prevailing blanket third-party exception allowing Big Data surveillance to avoid constitutional scrutiny.

For this reason, Justice Sotomayor suggested that it might be necessary to reevaluate the proposition that people have no reasonable expectation of privacy in information voluntarily disclosed to third parties.[187]

> This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks. People disclose the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers. . . . I for one doubt that people would accept without complaint the warrantless disclo-

---

183 "By means of signals from multiple satellites, the device established the vehicle's location within 50 to 100 feet, and communicated that location by cellular phone to a Government computer." *Id.* at 948.

184 *Id.* at 952.

185 Justice Sotomayor provided the critical fifth vote in support of Justice Scalia's trespassory test for Fourth Amendment protection where "the Government obtains information by physically intruding on a constitutionally protected area." *Id.* at 954 (Sotomayor, J., concurring) (quoting majority opinion). But she also agreed with a four-member concurrence that, "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" *Id.* at 955 (quoting Justice Samuel Alito's concurrence).

186 *Id.* at 955.

187 *Id.* at 957 (citing Smith v. Maryland, 442 U.S. 735, 742 (1979); United States v. Miller, 425 U.S. 435, 443 (1976)).

> sure to the Government of a list of every Web site they had visited in the last week, or month, or year. But whatever the societal expectations, they can attain constitutionally protected status only if our Fourth Amendment jurisprudence ceases to treat secrecy as a prerequisite for privacy.[188]

The opinion underscores the potential danger of a third-party exception in the age of Big Data technology, although the actual state of affairs has already gone beyond the world Justice Sotomayor describes. She expressed concern about a state of affairs in which *any* record for *any* person could be disclosed to the government, retrospectively. But as discussed below,[189] the third-party exception has been expanded to require disclosure of *every* record regarding *every* person, prospectively.[190]

B. Surveillance and FISA

As *Katz* noted, the warrant requirement is "subject only to a few specifically established and well-delineated exceptions."[191] The opinion explicitly reserved the question of "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security."[192] Congress responded to the Supreme Court's jurisprudence by enacting Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[193] Among other things, Title III generally prohibits electronic eavesdropping but authorizes law enforcement to obtain a court order to engage in such surveillance as a last resort—in particular, when there is probable cause to believe that an individual has committed, is committing, or is about to commit certain serious crimes and that the wiretap will intercept communications regarding those crimes.[194] Consistent with *Katz*'s reservation, Title III disclaimed any pretense of limiting the President's power to protect the United States against hostile powers and to ensure the secrecy of U.S. national security information.[195]

---

188 *Id.*

189 *See infra* Part III.C.

190 *See infra* Part III.C.

191 Katz v. United States, 389 U.S. 347, 357 (1967).

192 *Id.* at 358 n.23; *see also id.* at 363–64 (White, J., concurring) (noting that the decision did not address national security cases).

193 Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified as amended at 18 U.S.C. §§ 2510–2522 (2012)). Congress was reacting not only to *Katz* but also to *Berger v. New York*, 388 U.S. 41 (1967), which had struck down a state eavesdropping statute.

194 Title III wiretaps involve a detailed application process and are subject to limitations on duration and scope, including procedures that minimize the capture of innocent communications. *See* 18 U.S.C. § 2518(3) (2012).

195 18 U.S.C. § 2511(3) (1970), *repealed by* Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 201(c), 92 Stat. 1783, 1797.

In its review of Title III in *United States v. U.S. District Court* (*Keith*), the Supreme Court held that warrantless domestic wiretapping was unconstitutional even when done for national security purposes.[196] The *Keith* Court did acknowledge that the focus of intelligence surveillance "may be less precise than that directed against more conventional types of crime."[197] Moreover, different standards "may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens."[198] Although the Court denied that it was attempting "to guide the congressional judgment" in this area, it offered some direction for subsequent legislation, in which a showing of probable cause could be different than in traditional criminal investigations, the time and reporting requirements may be less strict, and, "in sensitive cases," applications for prior judicial authorization might be made to "a specially designated court."[199]

Around the same time, media exposés and congressional investigations revealed a troubling history of executive branch abuses for the sake of national security.[200] Much of this came to light in the mid-1970s through the reports of the so-called "Church Committee," a U.S. Senate committee tasked with scrutinizing the exploits of American intelligence agencies.[201] The Church Committee found that "[i]ntelligence agencies pursued a 'vacuum cleaner' approach to in-

196 407 U.S. 297, 308–22 (1972).

197 *Id.* at 322.

198 *Id.* at 322–23. Subsequent to *Keith*, some lower court decisions concluded that there was a constitutional exception for surveillance undertaken for foreign intelligence or national security purposes. *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 913–15 (4th Cir. 1980) (finding a foreign intelligence exception to the Fourth Amendment). *But see, e.g.*, Zweibon v. Mitchell, 516 F.2d 594, 651, 654 (D.C. Cir. 1975) (expressing doubt that such an exception should be created).

199 *Keith*, 407 U.S. at 323.

200 Going back as far as the 1930s, "intelligence excesses, at home and abroad, have been found in every administration," many of which collaborated with intelligence agencies in "substantial wrongdoing." SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, S. REP. NO. 94-755, at v, viii, 9–10 (1976) [hereinafter CHURCH COMMITTEE BOOK II]; *see also* Christopher Pyle, *CONUS Intelligence: The Army Watches Civilian Politics*, WASH. MONTHLY, Jan. 1970, at 4 (revealing U.S. military's domestic spying program).

201 Officially titled the "Select Committee to Study Governmental Operations with Respect to Intelligence Activities," the Church Committee issued a series of reports accompanied by volumes of documents and hearings. *See, e.g.*, SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES ("CHURCH COMMITTEE"), http://www.intelligence.senate.gov/churchcommittee.html (last visited Mar. 24, 2014) (providing much of the materials). Several other bodies also investigated allegations of surveillance abuses. *See, e.g.*, RICHARD A. BEST, JR., CONG. RESEARCH SERV., RL32500, PROPOSALS FOR INTELLIGENCE REORGANIZATION, 1949–2004, at 19–25 (2004) (describing investigations).

telligence collection—drawing in all available information about groups and individuals, including their lawful political activity and details of their personal lives."[202] As a result, "[t]oo many people have been spied upon by too many Government agencies and [too] much information has been collected," with secret surveillance often undertaken against citizens who "posed no threat of violence or illegal acts on behalf of a hostile foreign power."[203] The Committee's chair and namesake, Senator Frank Church, offered these prophetic words:

> In the need to develop a capacity to know what potential enemies are doing, the United States government has perfected a technological capability that enables us to monitor the messages that go through the air. . . . Now that is necessary and important to the United States as we look abroad at enemies or potential enemies. We must know, at the same time, that capability at any time could be turned around on the American people, and no American would have any privacy left such is the capability to monitor everything—telephone conversations, telegrams, it doesn't matter. There would be no place to hide.[204]

A few years later, Congress enacted the Foreign Intelligence Surveillance Act (FISA)[205] "in large measure [as] a response to the revelations that warrantless electronic surveillance in the name of national security has been seriously abused."[206] FISA was intended "to provide legislative authorization and regulation for all electronic surveillance conducted within the United States for foreign intelligence purposes."[207] Relying upon the framework offered in *Keith*,[208] the 1978 law created the Foreign Intelligence Surveillance Court (FISC), a special spy court that meets in secret proceedings and is empowered to issue ex parte orders authorizing electronic surveillance to gather foreign intelligence.[209] The denial of an order is subject to review by a

---

202 CHURCH COMMITTEE BOOK II, *supra* note 200, at 165, 178. For instance, the NSA obtained copies of almost all telegrams to or from the United States, involving the private communications of millions of U.S. citizens, in what was at that time "the largest governmental interception program affecting Americans ever undertaken." SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK III, S. REP. NO. 94-755, at 765 (1976).

203 CHURCH COMMITTEE BOOK II, *supra* note 200, at 5.

204 *Meet the Press* (NBC television broadcast Aug. 17, 1975) (comments of Sen. Church), *available at* http://www.youtube.com/watch?v=9DjJKYYb5-4.

205 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801–1885c (2006 & Supp. V 2011)).

206 S. REP. NO. 95-604, at 7 (1977).

207 S. REP. NO. 95-701, at 9 (1978).

208 *See id.* at 11, 15–16 (discussing *Keith*).

209 *See* 50 U.S.C. § 1803(a), (c) (2006 & Supp. V 2011). A subsequent amendment extended that authority to issuing court orders to conduct physical searches for foreign intelligence purposes. *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No.

special appellate tribunal, the Foreign Intelligence Surveillance Court of Review (FISCR).[210]

In theory, a court order is required for foreign intelligence surveillance whenever there is a substantial likelihood that the eavesdropping will acquire communications involving a "United States person,"[211] which means an American citizen, an alien lawfully admitted for permanent U.S. residence, an association composed of a substantial number of American citizens and lawful aliens, or an American corporation.[212] To issue an order for electronic surveillance, a FISC judge must find "probable cause" to believe that the target of the surveillance is a foreign power or its agent,[213] which includes not only foreign governments and factions, but also individuals and groups engaged in international terrorism and even "a foreign-based political organization, not substantially composed of United States persons."[214] In addition, the FISC judge must sign off on proposed minimization procedures, which are "specific procedures . . . that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[215] The judge is tasked with some clerical work as well, ensuring that the application contains the necessary certifications and statements

---

103-359, § 807, 108 Stat. 3423, 3443 (1994) (codified at 50 U.S.C. §§ 1821–1824 (2006 & Supp. V 2011)).

210 *See* 50 U.S.C. § 1803(b). If the FISCR upholds the denial of an order, the U.S. Supreme Court may hear the case by writ of certiorari. The FISCR is composed of three judges. The FISC is composed of eleven judges drawn from at least seven of the twelve judicial circuits. At least three of the FISC judges must reside within twenty miles of the District of Columbia. The Chief Justice of the U.S. Supreme Court designates district court judges to serve on the FISC, as well as appellate or district court judges to serve on the FISCR. *See id.* § 1803(a)(1), (b). The judges on both courts serve seven-year, staggered terms, and they may only serve once on either the FISC or FISCR. *See id.* § 1803(d).

211 *See id.* § 1802(a)(1)(B). *But see infra* notes 281–82 and accompanying text (discussing inevitable interception of communications by U.S. persons).

212 50 U.S.C. § 1801(i) (2006 & Supp. V 2011).

213 *Id.* § 1805(a)(2) (2006 & Supp. V 2011). This is different from probable cause in the traditional sense, that is, reasonable grounds to believe that a crime has been or is about to be committed, and evidence of that crime will be obtained by the proposed search. *See, e.g.*, Brinegar v. United States, 338 U.S. 160, 175–76 (1949) (providing classic formulation of probable cause). Nonetheless, the courts found that FISA's "requirements provide an appropriate balance between the individual's interest in privacy and the government's need to obtain foreign intelligence information, and that FISA does not violate the probable cause requirement of the Fourth Amendment." United States v. Duggan, 743 F.2d 59, 74 (2d Cir. 1984).

214 50 U.S.C. § 1801(a)–(b). Subject to certain requirements, the Attorney General may authorize foreign intelligence surveillance in an emergency situation without a court order. *See id.* § 1805(e).

215 *Id.* § 1801(h)(1); *see, e.g.*, *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 617–18 (Foreign Intelligence Surveillance Ct. 2002) (describing some of the minimization procedures).

regarding the proposed surveillance.[216] Unlike wiretaps under Title III,[217] however, the target of a FISA order does not have to be notified of the surveillance.

The statutory scheme would undergo just a few modifications during the first two decades of its existence. In 1998, Congress amended the law to allow FISC judges to issue orders authorizing the use of pen registers and trap and trace devices for facilities used by foreign agents or those engaged in international terrorism or clandestine intelligence activities.[218] The amendment also allowed for orders requiring the production of some business records (e.g., car rental, hotel, and storage facility records),[219] upon a showing by the government that "there are specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[220] Nonetheless, the basic approach of FISA remained the same through the turn of the millennium. Among other things, this scheme fostered a split among government agencies and their activities along two axes: law enforcement versus intelligence gathering and domestic surveillance versus foreign surveillance.

As originally enacted, FISA required the government to demonstrate that "the purpose of the surveillance is to obtain foreign intelligence information."[221] Federal court opinions interpreted this provision as insisting that the *primary* purpose of FISA surveillance be the collection of foreign intelligence information and not the investi-

---

216 50 U.S.C. § 1805(a)(4). The Attorney General must approve each application "based upon his finding that it satisfies the criteria and requirements" of FISA. *Id.* § 1804(a) (2006 & Supp. V 2011). Among other things, the application must include a certification by the National Security Advisor (or another high-ranking official designated by the President) that the information sought is foreign intelligence information, that the purpose of the surveillance is to gather such information, and that this information cannot reasonably be obtained by normal investigative techniques. *Id.* § 1804(a)(6). The term "[f]oreign intelligence information" means information relating to "the ability of the United States to protect against" hostile actions of a foreign power or agent of a foreign power, including actual or potential attacks, clandestine intelligence activities, sabotage, and international terrorism. *Id.* § 1801(e). When the target is a United States person, the FISC judge must determine that the certifications are not clearly erroneous based on the statements provided. *Id.* § 1805(a)(4). A similar process applies to applications for FISA orders to conduct physical searches. *Id.* § 1824.

217 *See id.* § 1803(c) (2006 & Supp. V 2011).

218 *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105-272, § 601, 112 Stat. 2396, 2404 (1998) (codified as amended at 50 U.S.C. §§ 1841–1846 (2006 & Supp. V 2011)).

219 *See id.*

220 50 U.S.C. § 1862(b)(2)(B) (2000).

221 *See* 18 U.S.C. § 2516(8)(d) (2012) (requiring that the target be notified of the surveillance within ninety days of the wiretap's termination).

gation of criminal activity.[222] To comply with this standard, the Justice Department erected a "wall" between criminal investigations and foreign intelligence surveillance. Although the exact timing of its creation remains "shrouded in historical mist," the wall came to be understood as restricting the ability of law enforcement agents and intelligence officials to share information.[223] The wall complemented the separation between domestic and foreign surveillance, with statutory law and executive orders divvying up responsibilities between the FBI, CIA, and military intelligence agencies such as the NSA.[224] Ostensibly urging "full and free exchange of information,"[225] the legal and practical arrangement perpetuated a "foreign-domestic divide" that at times discouraged cooperation and information sharing among agencies.[226]

Both the wall and the foreign-domestic divide could be seen as protecting civil liberties and preventing the type of abuses uncovered by the Church Committee. But in the wake of the attacks of September 11, 2001, these constraints (or at least the perception thereof)[227] were among the culprits fingered for missed opportunities to foil the terrorist plot. Apparently, "handoffs of information were lost across the divide separating the foreign and domestic agencies of government,"[228] and "beliefs about what the wall required" inhibited the flow of information about the conspiracy and prevented the participation

---

222 *See* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1076 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Duggan, 743 F.2d 59, 77–78 (2d Cir. 1984).

223 *In re* Sealed Case, 310 F.3d 717, 727–28 (Foreign Intelligence Surveillance Ct. Rev. 2002). *See generally* Diane C. Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437 (2006).

224 Since its establishment, the CIA was tasked with collecting intelligence outside of the United States but was given "no police, subpoena, or law enforcement powers or internal security functions." National Security Act of 1947, § 102(d), Pub. L. No. 80-253 (codified at 50 U.S.C. § 3036). In turn, the FBI was responsible for domestic surveillance, including gathering foreign intelligence within the United States. Various agencies within the Department of Defense were concerned with military-related intelligence both at home and abroad; for instance, the NSA collected and processed signals intelligence, a term that includes all forms of communication using the electromagnetic spectrum. In December 1981, President Reagan formalized the division by issuing an executive order that, among other things, barred the CIA and military intelligence agencies from engaging in domestic electronic surveillance unless coordinated with the FBI. *See* Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

225 Exec. Order No. 12,333, pt. 1.1, 46 Fed. Reg. 59,941 (Dec. 4, 1981).

226 *See, e.g.*, NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT, at xvi, 80, 263–65, 353–57, 399–406, 409 (2004) [hereinafter 9/11 COMMISSION REPORT] (describing and critiquing the foreign-domestic divide).

227 *See, e.g.*, *Sealed Case*, 310 F.3d at 723–27 (concluding that "primary purpose" requirement was not mandated by FISA itself); 9/11 COMMISSION REPORT, *supra* note 224, at 78–80, 270–72 (describing misinterpretation of wall requirements).

228 9/11 COMMISSION REPORT, *supra* note 226, at 353.

of criminal investigators in a search for two of the hijackers.[229] Six weeks after 9/11, Congress enacted the USA PATRIOT Act (Patriot Act)[230]—a wide-ranging compendium of provisions, many of which had been proposed and debated in previous years but were repackaged after the attacks as tools to prevent terrorism.[231]

The legislation tore down the wall by amending FISA to state that acquisition of foreign intelligence information need only be *a significant* purpose, rather than the *primary* purpose, of the surveillance.[232] In addition, the Patriot Act explicitly permits information sharing among law enforcement and intelligence gathering offices.[233] Indeed, one provision and a subsequent directive seemed to demand the expeditious flow of information between law enforcement and intelligence agencies.[234] Several cases—including the first ever appeal to the FISCR—upheld the change to FISA's search and surveillance provisions.[235] A short-lived district court decision, however, expressed the concerns of many who opposed the makeover: "Now, for the first time in our Nation's history, the government can conduct surveillance to gather evidence for use in a criminal case without a traditional warrant," thereby "allowing the Executive Branch to bypass the Fourth Amendment."[236]

---

229 OFFICE OF THE INSPECTOR GEN., U.S. DEP'T OF JUSTICE, A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS 21–22 (2004).

230 *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (Patriot Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S. Code).

231 *See, e.g.*, *Administration's Draft Anti-Terrorism Act of 2001: Hearing Before the H. Comm. on the Judiciary*, 107th Cong. 57–59 (2001) (comments of Rep. Bob Barr).

232 *See* Patriot Act § 218 (codified at 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B) (2006 & Supp. V 2011)).

233 One provision allows the disclosure of foreign intelligence and counterintelligence information uncovered during the course of criminal investigations—including information obtained by grand juries and Title III surveillance—to "any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official." *Id.* § 203 (codified at FED. R. CRIM. P. 6(e)(3) and 18 U.S.C. § 2517(6) (2012)). Another provision permits federal officials conducting foreign intelligence surveillance to consult with law enforcement officers to coordinate efforts to investigate or protect against actual or potential attacks, sabotage, international terrorism, and clandestine intelligence activities by foreign powers or their agents. *Id.* § 504 (codified at 50 U.S.C. §§ 1806(k), 1825(k) (2006 & Supp. V 2011)).

234 *See id.* § 905 (codified at 50 U.S.C. § 403-5b(a)(1) (2006 & Supp. V 2011)); Memorandum from John Ashcroft, U.S. Att'y Gen., to FBI Director et al., Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI (Mar. 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html.

235 *See, e.g.*, *In re* Sealed Cases, 310 F.3d 717, 736–46 (Foreign Intelligence Surveillance Ct. Rev. 2002) (upholding amendments); United States v. Abu-Jihaad, 630 F.3d 102, 120 (2d Cir. 2010) (collecting cases).

236 Mayfield v. United States, 504 F. Supp. 2d 1023, 1036–37 (D. Or. 2007), *rev'd on other grounds*, 599 F.3d 964 (9th Cir. 2010).

As for pen registers and trap and trace devices[237]—which sometimes work in combination and are referred to as PR/TT devices—the Patriot Act dispensed with the previous requirement that a targeted facility be used by foreign agents or by individuals involved in international terrorism or clandestine intelligence activities. Instead, the government needs only show that the information sought is foreign intelligence not regarding a U.S. person or that it is "relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities."[238] While a PR/TT order used to be limited to the jurisdiction of the issuing court, now a single order can be executed nationwide.[239] The scope of such orders was also expanded to include the collection of metadata for electronic communications (e.g., e-mail).[240] In hindsight, the absence of individualized suspicion, elimination of jurisdictional limitations, and inclusion of electronic communications made the PR/TT provision a potential vehicle for mass surveillance. But at the time, these changes were depicted as merely streamlining the process and updating the law consistent with technological changes.[241]

Another provision of the Patriot Act, section 215, permits the FBI Director or his designee to request production of "any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[242] Dubbed the "library section" because of concerns that a library might be required to give up records about its patrons,[243] section 215 was challenged in court as violating search-and-seizure doctrine as well as speech and associational rights.[244] In 2006, Congress amended the provision to address

---

237 *See supra* note 175 (defining both terms).

238 Patriot Act § 214, 50 U.S.C. § 1842(a)(1), (c)(2) (requiring only a nexus with "an ongoing investigation to protect against international terrorism or clandestine intelligence activities").

239 *See id.* § 216 (codified at 18 U.S.C. §§ 3121(b)(1)(C), 3127(2)).

240 *See id.* (codified at 18 U.S.C. §§ 3121, 3123).

241 *See* CHARLES DOYLE, CONG. RESEARCH SERV., RL31200, TERRORISM: SECTION BY SECTION ANALYSIS OF THE USA PATRIOT ACT 10–13 (2001) (describing investigations).

242 *See* Patriot Act § 215, 50 U.S.C. § 1861 (2006 & Supp. V 2011). The Patriot Act also expanded the scope of "national security letters" (NSL), which are roughly analogous to administrative subpoenas by allowing federal law enforcement to gather records from third parties without court authorization. *See id.* § 505 (codified at 12 U.S.C. § 3414(a)(5)(A), 15 U.S.C. § 1681u, 18 U.S.C. § 2709(b)); *see also* CHARLES DOYLE, CONG. RESEARCH SERV., R41619, NATIONAL SECURITY LETTERS: PROPOSALS IN THE 112TH CONGRESS 2–11 (2011) (providing background and problems of NSLs).

243 *See, e.g.*, *The PATRIOT Act*, AM. LIBRARY ASSOC., http://www.ala.org/advocacy/advleg/federallegislation/theusapatriotact (last visited Feb. 15, 2014).

244 *See* Muslim Cmty. Ass'n v. Ashcroft, 459 F. Supp. 2d 592 (E.D. Mich. 2006).

some of these concerns.[245] Among other things, the government was now required to provide "reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation,"[246] with the tangible things limited to those items otherwise obtainable by subpoena or court order.[247] The changes to section 215 were sufficient to persuade litigants to drop their lawsuit.[248] What many failed to foresee was that this provision, ostensibly geared toward the collection of a narrow range of preexisting business records, might be interpreted to justify government snooping on a far larger scale.

C. Mass Surveillance

In October 2001, President Bush secretly authorized the NSA to conduct warrantless eavesdropping on international communications and to engage in bulk collection of metadata on telephone and Internet communications.[249] In 2004, in response to a near revolt by high-ranking Justice Department and FBI officials,[250] the bulk collection of Internet metadata was transitioned from a warrantless program to one requiring FISC authorization.

To achieve this feat, the government made the remarkable claim that FISA's pen register/trap and trace (PR/TT) provisions could be used to collect the metadata for e-mail communications by millions of

---

245 *See* USA PATRIOT Improvement Reauthorization Act of 2005, Pub. L. No. 109-177, § 106, 120 Stat. 192 (2006).

246 *See* 50 U.S.C. § 1861(b)(2)(A). The items sought would be presumptively relevant to an investigation if the government shows that they pertain to a foreign power or its agents. *See id.*

247 *See id.* § 1861(a)(3), (g). High-level FBI approval is also required for book sales records, book customer lists, firearms sales records, tax return records, educational records, and medical records. *See id.* § 1861(a)(3). In addition, the amendments demanded the adoption of minimization procedures for the retention and dissemination of information; required approval at the national level of the FBI when demanding records that raise certain constitutional sensitivities, including information from libraries; and allowed recipients to disclose the order to an attorney for purposes of legal advice and to seek judicial review of an order in the FISC. *See id.* § 1861(c)(2)(D), (d)(1), (f). Although the production order may be challenged immediately, the recipient must wait a year before seeking review of a nondisclosure order. *See id.* § 1861(f)(2)(A)(i). Moreover, a FISC judge must treat a high-level certification, made in good faith, as conclusive "that disclosure may endanger the national security of the United States or interfere with diplomatic relations." *Id.* § 1861(f)(2)(C)(ii).

248 *See Citing Improvements to Law, ACLU Withdraws Section 215 Case but Vows to Fight Individual Orders*, AM. C.L. UNION (Oct. 27, 2006), http://www.aclu.org/national-security/citing-improvements-law-aclu-withdraws-section-215-case-vows-fight-individual-orde (last visited Feb. 15, 2014).

249 *DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001*, IC ON THE RECORD (Dec. 21, 2013) [hereinafter *DNI Announces*], http://icontherecord.tumblr.com/post/70683717031/dni-announces-the-declassification-of-the.

250 *See, e.g.*, OFFICES OF THE INSPECTORS GEN., U.S. DEP'T OF DEFENSE ET AL., UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 21–27 (2009) [hereinafter OIG Report] (describing incidents); Gellman, *supra* note 4 (same).

people—and, remarkably, the FISC accepted the argument, despite acknowledging that the "raw volume of the proposed collection is enormous" and this "novel use of statutory authorities" allows "a much broader type of collection" than any previous application.[251] Nonetheless, the court found that the collection of metadata did not implicate the Fourth Amendment,[252] relying upon the aforementioned third-party exception[253] and, in particular, the Supreme Court's 1979 decision in *Smith v. Maryland*.[254] Along the way, the FISC adopted an extraordinarily broad interpretation of the statutory requirement that any information sought be "relevant to an ongoing investigation."[255]

Neither the initial warrantless bulk collection of Internet metadata nor the rebranding of the program as a FISC-approved program would be disclosed until 2013.[256] But beginning in late 2005, news articles revealed that the government was intercepting international communications and gathering telephony metadata in bulk, all without a warrant or court order.[257] The Bush Administration's attempts to assuage public anxiety[258] and to blunt legal criticisms were not completely successful,[259] and as a result, the government began

---

251 Opinion and Order at 1–2, 23, 39, 58, [*redacted*], No. PR/TT [*redacted*] (Foreign Intelligence Surveillance Ct. [*redacted*]) [hereinafter Kollar-Kotelly Opinion], *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

252 *See id.* at 58–66.

253 *See supra* Part III.A.

254 442 U.S. 735 (1979); Kollar-Kotelly Opinion, *supra* note 251, at 59–62.

255 50 U.S.C. § 1842(a)(1),(c)(2) (2006 & Supp. V 2011); *see* Kollar-Kotelly Opinion, *supra* note 251, at 48–49. The court ignored obvious signs that the PR/TT scheme was aimed at "the micro scale, not the macro scale." Orin Kerr, *Problems with the FISC's Newly-Declassified Opinion on Bulk Collection of Internet Metadata*, LAWFARE (Nov. 19, 2013, 2:35 AM), http://www.lawfareblog.com/2013/11/problems-with-the-fiscs-newly-declassified-opinion-on-bulk-collection-of-internet-metadata/. It also failed to appreciate the critical differences between the Internet transactional data at issue in the NSA program and the type of phone call data involved in *Smith*. Julian Sanchez, *Are Internet Backbone Pen Registers Constitutional?*, JUST SECURITY (Sept. 23, 2013, 7:55 PM), http://justsecurity.org/2013/09/23/internet-backbone-pen-registers-constitutional/.

256 *See supra* note 4 and accompanying text.

257 *See* Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA TODAY, May 11, 2006, at A1 (phone call records); James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1 (eavesdropping).

258 *See, e.g.*, GEORGE W. BUSH, REMARKS ON THE TERRORIST SURVEILLANCE PROGRAM (2006); 1 PUBLIC PAPERS OF THE PRESIDENTS OF THE UNITED STATES: GEORGE W. BUSH 917 (2006) ("We're not mining or trolling through the personal lives of millions of innocent Americans. Our efforts are focused on links to al Qaida and their known affiliates.").

259 *Compare* U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006), *available at* http://www.justice.gov/opa/whitepaperonnsalegalauthorities.pdf (Justice Department whitepaper providing some of the underlying reasoning for the NSA's activities), *and* Letter from William E. Moschella, Assistant Att'y Gen., to Pat Roberts, Chairman, Senate Select Comm. on Intelligence et al. (Dec. 22, 2005), *available at* http://www.justice.gov/ag/readingroom/surveillance6.pdf (similar arguments offered in letter from Assistant Attorney General), *with* Letter from Curtis A. Bradley et al., to Congressional Leadership (Feb. 2, 2006), *reprinted at* 81 IND. L.J. 1415 (2006) (critiquing Justice Department white paper),

exploring means of obtaining FISC authorization for these programs too.[260]

In May 2006, the government invoked Patriot Act section 215 as the vehicle for the NSA's bulk collection of phone call records.[261] Once again, the court approved the government's application for mass surveillance, although the order was not accompanied by any sort of legal reasoning.[262] Apparently,[263] it was only after the program was revealed in 2013 that the FISC issued an opinion attempting to justify the collection of "a very large volume of each [telephone] company's call detail records or telephony metadata."[264] Among other things, the court drew upon the earlier PR/TT opinion's assessment of the standard of proof, finding relevance to be a broad concept that "amounts to a relatively low standard."[265] The court also claimed that the FISC's standing interpretation of section 215 was bolstered by the doctrine of legislative reenactment[266] because Congress reauthorized section 215 only after the House and Senate Intelligence Committees had received a report on the government's bulk collection programs describing the nature and scope of the FISC's approval.[267] As for the program's constitutionality, the NSA's program was "squarely con-

---

and Letter from Curtis A. Bradley et al., to Congressional Leadership (Jan. 9, 2006), *reprinted at* 81 IND. L.J. 1364 (2006) (critiquing Moschella letter).

260 *See DNI Announces*, *supra* note 249 (noting the transitioning of both programs to the FISC).

261 *See* Memorandum of Law in Support of Application for Certain Tangible Things for Investigations to Protect Against International Terrorism, *In re* FBI for an Order Requiring the Production of Tangible Things from [*redacted*], No. BR 06-05, at 2 (Foreign Intelligence Surveillance Ct. May 23, 2006), *available at* https://www.eff.org/document/br-06-05-memo-law.

262 *See* Order, *In re* FBI for an Order Requiring the Production of Tangible Things from [*redacted*], No. BR 06-05, at 2 (Foreign Intelligence Surveillance Ct. May 24, 2006), *available at* http://www.dni.gov/files/documents/section/pub_May%2024%202006%20Order%20from%20FISC.pdf.

263 *See, e.g.*, Ellen Nakashima, *FISA Court Releases Ruling Upholding Phone Program*, WASH. POST, Sept. 18, 2013, at A4 (quoting ACLU's Jameel Jaffer, who described the opinion as "a document that appears to have been cobbled together over the last few weeks in an effort to justify a decision that was made seven years ago").

264 *In re* FBI for an Order Requiring Production of Tangible Things from [*redacted*], No. BR 13-109, 2013 WL 5741573, at *1 (Foreign Intelligence Surveillance Ct. Aug. 29, 2013) [hereinafter Eagan Opinion].

265 *Id.* at *6.

266 Also known as legislative ratification, the doctrine presumes the legislature appreciates and adopts a judicial or administrative interpretation of a statute that lawmakers subsequently reenact without change. *See* Forest Grove Sch. Dist. v. T.A., 557 U.S. 230, 239–40 (2009); Lorillard v. Pons, 434 U.S. 575, 580 (1978).

267 *See* Eagan Opinion, *supra* note 264, at *8–9 (discussing legislative reenactment in the context of section 215); PATRIOT Sunsets Extension Act of 2011, Pub. L. No. 112-14, 125 Stat. 216 (codified in scattered sections of 50 U.S.C.) (reauthorizing section 215).

trolled" by *Smith*, which "compels the conclusion that there is no Fourth Amendment impediment to the collection."[268]

Like the FISC's PR/TT opinion, the section 215 opinion would not come to light until 2013.[269] By contrast, the transition of the NSA's eavesdropping program was overt[270] and eventually addressed

---

268 *Id.* at *2–3. Like the PR/TT opinion, the FISC's section 215 opinion leaves much to be desired. "Congress intended [section 215] to allow the intelligence communities to access targeted information for specific investigations," said Representative Jim Sensenbrenner, one of the sponsors of the Patriot Act. "How can every call that every American makes or receives be relevant to a specific investigation?" Jim Sensenbrenner, *This Abuse of the Patriot Act Must End*, THE GUARDIAN (June 9, 2013, 7:00 AM), http://www.theguardian.com/commentisfree/2013/jun/09/abuse-patriot-act-must-end. He later wrote in a letter to Attorney General Eric Holder, "The administration's interpretation to allow for bulk collection is at odds with Congressional intent and with both the plain and legal meanings of 'relevance.'" Letter from F. James Sensenbrenner Jr., Rep., to Eric Holder, U.S. Att'y Gen. (Sept. 6, 2013), *available at* http://sensenbrenner.house.gov/uploadedfiles/sensenbrenner_letter_to_attorney_general_eric_holder.pdf. As for reliance on the doctrine of legislative reenactment, Sensenbrenner and other members of Congress have said they were not briefed on the expansive interpretation of section 215. *See, e.g.*, Jim Sensenbrenner, *How Obama Has Abused the Patriot Act*, L.A. TIMES (Aug. 19, 2013), http://articles.latimes.com/2013/aug/19/opinion/la-oe-sensenbrenner-data-patriot-act-obama-20130819 ("As I have said numerous times, I did not know the administration was using the Patriot Act for bulk collection, and neither did a majority of my colleagues."). *But see* ACLU v. Clapper, 959 F. Supp. 2d 724, 745 n.13 (S.D.N.Y. 2013) (questioning Rep. Sensenbrenner's claim of ignorance). In addition, the FISC's opinion failed to grapple with the disparity between the limited information gleaned by the now-archaic pen register in *Smith* versus the far richer telephony metadata gathered by the NSA. Jennifer Granick, *Debate: Metadata and the Fourth Amendment*, JUST SECURITY (Sept. 23, 2013, 2:00 PM), http://justsecurity.org/2013/09/23/metadata-fourth-amendment/. Perhaps the most troubling lapse in the opinion, however, was the absence of any mention, let alone discussion, of the Supreme Court's groundbreaking 2012 decision on high-tech surveillance and the Fourth Amendment, *United States v. Jones*, 132 S. Ct. 945 (2012). *See supra* notes 182–90 and accompanying text (discussing *Jones*).

269 But there were some warning signs. For instance, a few lawmakers spoke out about secret constructions of surveillance authority. "I want to deliver a warning this afternoon," said Senator Ron Wyden during a 2011 floor debate. "When the American people find out how their government has secretly interpreted the Patriot Act, they will be stunned and they will be angry." Charlie Savage, *Senators Say Patriot Act Is Being Misinterpreted*, N.Y. TIMES, May 27, 2011, at A17 (quoting Sen. Ron Wyden); *see also* Letter from Ron Wyden & Mark Udall, Sens., to Eric Holder, U.S. Att'y Gen. (Sept. 21, 2011), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/250829/wyden-udall-letter-to-holder-on-wiretapping.pdf (expressing concerns that "Justice Department officials have—on a number of occasions—made what we believe are misleading statements pertaining to the government's interpretation of surveillance law," and warning that "Americans will eventually and inevitably come to learn about the gap that currently exists between the public's understanding of government surveillance authorities and the official, classified interpretation of these authorities"). Around this time, one could discern a sizeable increase in the use of section 215. *See* Ellen Nakashima, *FBI Heads to Court More Often to Obtain Data on Personal Internet Usage*, WASH. POST, Oct. 26, 2011, at A6 (detailing increase in business record requests); *Foreign Intelligence Surveillance Act Court Orders 1979–2012*, EPIC, http://epic.org/privacy/wiretap/stats/fisa_stats.html (last updated May 4, 2012) (listing by year number of FISA applications for business records).

270 *See Department of Justice Oversight: Hearings Before the S. Comm. on the Judiciary*, 110th Cong. 6–7 (2007) (statement of Alberto Gonzales, U.S. Att'y Gen.) (noting that FISC had approved electronic surveillance).

specifically by statute.[271] Pursuant to section 702 of the FISA Amendments Act of 2008 (FAA), the government is allowed to intercept the communications of non-U.S. persons reasonably believed to be outside of the United States.[272] The government need not identify any particular target or facility to be monitored, nor does it have to provide probable cause to believe that the surveillance target is a foreign power (or its agent) that will use the facility to be monitored.[273] Instead, FISC approval occurs at a programmatic level—reviewing proposed procedures and official certifications[274]—with an order authorizing mass government surveillance. For instance, an order "could authorize the acquisition of all communications to and from specific geographic areas of foreign policy interest."[275]

FAA section 702 was challenged by a group of individuals and organizations whose communications were likely targets of NSA surveillance,[276] arguing that the provision "allows the executive branch sweeping and virtually unregulated authority to monitor the international communications . . . of law-abiding U.S. citizens and residents."[277] In its 2013 decision in *Clapper v. Amnesty International*, the Supreme Court held that the plaintiffs had failed to show a realistic threat of imminent injury and therefore lacked standing to challenge the law.[278] In dissent, Justice Stephen Breyer pointed out that the government had the means and motive to conduct such surveillance, with prior behavior providing every reason to believe it would occur.[279] To find standing, Justice Breyer concluded, "we need only assume that

---

271 For a half year, the surveillance program was governed by the Protect America Act (PAA) of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007). Although short-lived, it was the subject of the second opinion ever issued by the FISCR. *See In re* Directives [*redacted*] Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (Foreign Intelligence Surveillance Ct. Rev. 2008). The PAA was replaced by the FISA Amendments Act (FAA) of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (2008).

272 50 U.S.C. § 1881a (2006 & Supp. V 2011).

273 *See, e.g.*, Amnesty Int'l USA v. Clapper, 638 F.3d 118, 124 (2d Cir. 2011) (describing differences between section 702 and approach under preexisting FISA scheme), *rev'd*, 133 S. Ct. 1138 (2013).

274 *See* 50 U.S.C. § 1881a(a), (c)(1), (i)(2), (i)(3).

275 Brief for Respondents at 11, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) (No. 11-1025); *see also Amnesty Int'l USA*, 638 F.3d at 126 (listing Russia, Venezuela, and Israel as potential areas of foreign policy interest).

276 *Clapper*, 133 S. Ct. at 1145–56. Among other things, the "communications include discussions with family members of those detained at Guantanamo, friends and acquaintances of those persons, and investigators, experts and others with knowledge of circumstances related to terrorist activities." *Id.* at 1158–59 (Breyer, J., dissenting).

277 Complaint for Declaratory and Injunctive Relief at ¶ 1, Amnesty Int'l USA v. McConnell, No. 08 CIV 6259(JGK), 646 F. Supp. 2d 633 (S.D.N.Y. Aug. 20, 2009).

278 *See Clapper*, 133 S. Ct. at 1147–55.

279 *Id.* at 1159.

the Government is doing its job (to find out about, and combat, terrorism)."[280]

The government did not deny that communications by U.S. persons had been captured under section 702. Apologists for the program claim it is impossible not to examine discussions by Americans when using technology that collects millions of electronic messages, and, in fact, the inability to distinguish communications of Americans from those of foreigners was "one of the main things that drove" the government to press for the changes in the FAA.[281] Reportedly, NSA analysts use search terms designed to create at least 51% confidence in a target's "foreignness"[282]—hardly a rigorous standard and one virtually guaranteed to collect domestic communications. After *Clapper*, however, it seemed possible that the government would fully employ its powers under the FAA, countless communications of Americans would be captured thereby, and yet no one would ever be able to challenge the law.

IV
Defense Rights and Potential Barriers

All told, the government has the ability to track and record every aspect of someone's online life—and much of his offline, real-world behavior too.[283] Both Congress and the courts have facilitated domestic spying by creating a legal environment in which the government is only loosely bound by legislation and largely unchecked by meaningful judicial review, allowing the executive branch to take aggressive stances on statutory and constitutional interpretation that have largely eliminated any previous constraints on surveillance ostensibly for foreign intelligence purposes.[284] Given the government's ability to draw upon Big Data information, the issue here is the basic rights of criminal defendants to access that information as well. The following lays the groundwork for an extension of these rights to evidence of digital innocence. This Part then reviews two of the primary arguments likely to be made to deprive defendants of their rights of access: the state secrets privilege and agency alignment.

---

280 *Id.* at 1160 (Breyer, J., dissenting); *see also* Transcript of Oral Argument at 25–26, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) (No. 11-1025) (remarks of Justice Anthony Kennedy that "it's hard for me to think that the government isn't using all of the powers at its command under the law . . . in order to protect this country").

281 James Risen & Eric Lichtblau, *Extent of E-mail Surveillance Renews Concerns in Congress*, N.Y. Times, June 17, 2009, at A1 (quoting former Homeland Security Advisor).

282 Gellman & Poitras, *supra* note 82.

283 *See supra* Part II.

284 *See supra* Part III.

A. Government Surveillance and Defense Rights

In *Clapper*, the plaintiffs called the government's theory of standing "a bid for a kind of immunity" since the targets will never know they have been subjected to surveillance.[285] Even if criminal charges were brought against the target, the government alone decides whether to introduce any evidence derived from surveillance at trial, and "[i]t is not at all clear what must be disclosed" as a result of using such evidence.[286] "That contention is misplaced," the government responded, because a defendant would be provided notice of the prosecution's intent to use information obtained or derived from electronic surveillance.[287] At oral argument, Solicitor General Donald Verrilli reiterated that a defendant would have standing to challenge the law if prosecutors sought to introduce surveillance information at trial[288]—an assertion relied upon by the Supreme Court in writing its opinion in *Clapper*.[289]

As it turns out, however, the government was not notifying criminal defendants as Solicitor General Verrilli had claimed; and even when there was good reason to believe that NSA surveillance was involved in a given case, prosecutors insisted they had no obligation to inform the accused.[290] After some sort of internal struggle within the Justice Department, the government reversed course in the fall of 2013 and began to notify defendants that evidence had been derived from mass surveillance activities.[291] Since then, a few defendants have sought new trials and/or the suppression of evidence obtained or derived from electronic surveillance and bulk metadata collection,[292]

---

285 Brief for Respondents at 57, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) (No. 11-1025).

286 *Id.* at 58 n.22.

287 Reply Brief for Petitioners at 15, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) (No. 11-1025).

288 *See* Transcript of Oral Argument at 4–5, Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138 (2013) (No. 11-1025).

289 *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1154 (2013) ("[I]f the Government intends to use or disclose information obtained or derived from [electronic surveillance] in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition.").

290 *See* Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES, July 16, 2013, at A11; Devlin Barrett, *U.S. Spy Program Lifts Veil in Court*, WALL. ST. J., July 31, 2013, at A1; Ellen Nakashima, *NSA Surveillance Questioned in Plot Case*, WASH. POST, June 22, 2013, at A2; Eric Schmitt et al., *Mining of Data Is Called Crucial to Fight Terror*, N.Y. TIMES, June 8, 2013, at A1.

291 *See* Robert Barnes & Ellen Nakashima, *U.S. to Use Warrantless Evidence in Terror Case*, WASH. POST, Oct. 26, 2013, at A1; Charlie Savage, *Doors May Open for Challenge to Secret Wiretaps*, N.Y. TIMES, Oct. 17, 2013, at A3; Charlie Savage, *Justice Dept. Defends Its Conduct on Evidence*, N.Y. TIMES, Feb. 15, 2014, at A9; Charlie Savage, *Warrantless Surveillance Continues to Cause Fallout*, N.Y. TIMES, Nov. 21, 2013, at A20.

292 50 U.S.C. § 1806(e) (2006 & Supp. V 2011) (electronic surveillance); *id.* § 1845(e) (pen register and trap and trace devices); *see also id.* § 1825(f) (suppression motion for

challenging the lawfulness of their surveillance as violating statutory requirements and constitutional law.[293] Most importantly for present purposes, these defendants have also moved for disclosure of information related to their surveillance under the NSA programs and for access to that information.[294]

The ultimate resolution of this issue remains unclear. In an historic ruling in January 2014, a federal court in Chicago ordered the disclosure of FISA application materials to the defense.[295] But the ruling in *United States v. Daoud* was stayed so the appellate process could run its course, and even if the order is upheld, the revealed materials may not exonerate the defendant. Instead, it is more likely that the disclosures will "be highly embarrassing to the government."[296] And

---

FISA physical searches); *id.* § 1881e (stating that information acquired under FAA section 702 is governed by 50 U.S.C. § 1806). Patriot Act section 215 does not contain provisions concerning government notification and motions to suppress, which led the government to claim there is no remedy for any section 215 violation. *See* United States' Response and Opposition to Defendants' Joint Motion for New Trial at 17–19, United States v. Moalin, No. 10-cr-4246-JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013). This remarkable claim was not addressed in the district court's opinion. *See* United States v. Moalin, No. 10-cr-4246-JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013).

293 *See* Defendant's Motion to Suppress Evidence Obtained or Derived from Surveillance Under the FISA Amendments Act and Motion for Discovery at 20–47, United States v. Muhtorov, No. 12-cr-00033-JLK-1 (D. Colo. filed Jan 29, 2014) [hereinafter Muhtorov Motion] (on file with authors) (challenging constitutionality of electronic surveillance under section 702 of the FISA Amendments Act); Statement of Facts and Memorandum of Points and Authorities in Support of Joint Motion Pursuant to Rule 33, Fed. R. Crim. P., for a New Trial at 1–4, 11–25, United States v. Moalin, No. 10-cr-4246-JM, 2013 WL 6079518 (S.D. Cal. Nov. 18, 2013) [hereinafter Moalin Motion] (arguing for new trial based on, inter alia, unconstitutionality of bulk metadata collection program); Defendant's Motion Requesting that This Court Declare the FISA Amendments Act of 2008 Unconstitutional at 1, United States v. Qazi, No. 12-60298-CR-Scola/O'Sullivan (S.D. Fla. May 28, 2013) (on file with authors) (requesting that FAA be declared unconstitutional because it violates the First and Fourth Amendments, as well as Article III).

294 *See* Mohamud Motion, *supra* note 157, at 17–25; Muhtorov Motion, *supra* note 293, at 47–56; Moalin Motion, *supra* note 293, at 2–7, 25–34, 37–38.

295 United States v. Daoud, No. 12-cr-723, 2014 WL 321384, at *3 (N.D. Ill. Jan. 29, 2014). *But see In re* Grand Jury Proceedings of Special April 2002 Grand Jury, 347 F.3d 197, 203 (7th Cir. 2003) (noting that "every FISA wiretap review had been conducted *in camera* and *ex parte*"); *Moalin*, 2013 WL 6079518, at *9–10 (refusing to order defense access to surveillance-related materials). As of this writing, similar defense motions are pending in criminal cases in Colorado (United States v. Muhtorov, No. 12-cr-00033-JLK-1 (D. Colo.)), Florida (United States v. Qazi, No. 12-60298-CR-Scola/O'Sullivan (S.D. Fla.)), and Oregon (United States v. Mohamud, No. 3:10-cr-00475-KI (D. Or.)). Other motions may be forthcoming. *See* Ellen Nakashima, *No Warrant, Inmate Is Told*, WASH. POST, Feb. 26, 2014, at A4 (most recent government notification); Patrick C. Toomey, *In Reversal, DOJ Poised to Give Notice of Warrantless Wiretapping*, ACLU BLOG OF RIGHTS (Oct. 18, 2013), https://www.aclu.org/blog/national-security/reversal-doj-poised-give-notice-warrantless-wiretapping (listing affected cases).

296 Andrew Harris & Steven Church, *Terror Defendant's Lawyer Wins Access to Secret Court Papers*, BUS. WK. (Jan. 30, 2014), http://www.businessweek.com/news/2014-01-29/chicago-bomb-sting-defense-lawyer-allowed-to-see-fisa-papers-1 (quoting defense attorney Ronald Kuby) (internal quotations marks omitted).

therein lies a very real danger. In considering defense access to information, some may be tempted to view these cases as involving nothing more than suspected terrorists seeking to have damning evidence excluded at trial—or, worse yet, convicted terrorists attempting to overturn otherwise valid guilty verdicts—all in an attempt to avoid well-deserved punishment. As prominent jurists have noted in the past, "we are called on to decide whether evidence should be excluded only when a search has been 'successful,'"[297] and in this environment the protection of a constitutional right "is not apt to flourish where its advocates are usually criminals."[298]

But a nearsighted, subject-distorted approach is inconsistent with constitutional criminal procedure, which makes clear that basic rights are not diminished by the seriousness of the underlying crime.[299] Nor are rights dependent upon the likely guilt of the accused. "The constitutional rights of criminal defendants are granted to the innocent and the guilty alike,"[300] the Supreme Court has opined, recognizing that a basic right, "while sometimes a shelter to the guilty, is often a protection to the innocent."[301] The impact of decisions about access to information gleaned from mass eavesdropping and bulk-collection

---

297 Rawlings v. Kentucky, 448 U.S. 98, 121 (1980) (Marshall, J., dissenting).

298 Draper v. United States, 358 U.S. 307, 314 (1959) (Douglas, J., dissenting); *see also* Minnesota v. Carter, 525 U.S. 83, 110 (1998) (Ginsburg, J., dissenting) ("Other decisions have similarly sustained Fourth Amendment pleas despite the criminality of the defendants' activities." (internal citations omitted)); Brinegar v. United States, 338 U.S. 160, 181 (1949) (Jackson, J., dissenting) ("Only occasional and more flagrant abuses come to the attention of the courts, and then only those where the search and seizure yields incriminating evidence and the defendant is at least sufficiently compromised to be indicted.").

299 *See* Mincey v. Arizona, 437 U.S. 385, 395 (1978) (rejecting the notion that there is a "murder scene exception" to the Fourth Amendment). In the few instances when the Constitution does distinguish among crimes for purposes of individual rights, the relevant provisions were intended to provide *greater* protection to those facing more serious charges and greater punishment. *See* U.S. CONST. art. III, § 3, cl. 1 (heightened proof requirements for treason); *id.* amend. V ("No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury . . . ."); Alabama v. Shelton, 535 U.S. 654, 658 (2002) (recognizing that the right to counsel applies in any case where incarceration may result); Baldwin v. New York, 399 U.S. 66, 69 (1970) (holding that right to trial by jury applies whenever charged crime authorizes punishment of more than six months' imprisonment). In other words, the fact that the foregoing cases involve very serious criminal charges (i.e., terrorism) cannot justify lower constitutional protections. *But cf.* United States v. Abdulmutallab, No. 10-20005, 2011 WL 4345243, at *5–6 (E.D. Mich. Sept. 16, 2011) (expanding "public safety" exception to *Miranda* to terrorism investigations).

300 Kimmelman v. Morrison, 477 U.S. 365, 380 (1986); *see also* Ohio v. Reiner, 532 U.S. 17, 18 (2001) (per curiam) ("[O]ur precedents dictate that the privilege [against self-incrimination] protects the innocent as well as the guilty . . . ."); Trupiano v. United States, 334 U.S. 699, 709 (1948) ("The Fourth Amendment was designed to protect both the innocent and the guilty from unreasonable intrusions upon their right of privacy . . . ."), *overruled in part on other grounds*, United States v. Rabinowitz, 339 U.S. 56 (1950).

301 Murphy v. Waterfront Comm'n of N.Y. Harbor, 378 U.S. 52, 55 (1964) (internal quotation marks omitted).

activities will not be limited to accused and convicted terrorists seeking to suppress incriminating evidence.[302] These cases necessarily implicate the rights of those wrongfully accused and convicted of all sorts of crimes.[303]

The case for defense access is even more compelling given revelations of chronic government dissembling. A series of high-ranking officials have made public statements about surveillance activities that were shown to be misleading if not altogether false,[304] and some news stories provide reason to doubt government claims that it has reformed or discontinued certain mass surveillance programs.[305] Moreover, recently declassified FISC opinions reveal the government's repeated misrepresentations, omissions of material facts, and failure

---

302 In these cases, one of the key FISA provisions applies not just to suppression motions but also to "any motion or request . . . pursuant to any other statute or rule . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover [or obtain] evidence or information obtained or derived from electronic surveillance." 50 U.S.C. § 1806(f) (2006 & Supp. V 2011); *see also id.* § 1845(f)(1) (analogous provision for pen register and trap and trace devices).

303 Some defendants are now seeking discovery of mass surveillance and bulk metadata collection activities in criminal cases having nothing to do with terrorism or national security. *See, e.g.*, Notice of Motion and Motion to Compel Discovery of Defendant Lara, United States v. Diaz-Rivera et al., No. 12-cr-00030-EMC/EDL (N.D. Cal. Oct. 2, 2013) (on file with authors) (drug prosecution).

304 Perhaps the best-known example was Director of National Intelligence James Clapper's congressional testimony denying that the NSA was collecting data on millions of Americans. Clapper would latter describe his answer as the "'least untruthful'" and then later issue an apology for his "'clearly erroneous statements.'" James Risen, *Lawmakers Question White House Account of an Internet Surveillance Program*, N.Y. TIMES, July 4, 2013, at A6 (quoting Director Clapper); *see also* Spencer Ackerman, *Congressional Trio Criticize James Cole's NSA Testimony as Misleading*, THE GUARDIAN (Feb. 12, 2014), http://www.theguardian.com/world/2014/feb/12/nsa-james-cole-congress-testimony-surveillance-phone-records (characterizing Deputy Attorney General James Cole's statements as "not entirely accurate"); Greg Miller, *A Trail of Inaccuracy About NSA Programs*, WASH. POST, July 1, 2013, at A1 (discussing inaccuracies and careful phrasing in administration statements about NSA surveillance programs); Shaun Waterman, *NSA Chief's Admission of Misleading Numbers Adds to Obama Administration Blunders*, WASH. TIMES (Oct. 2, 2013), http://www.washingtontimes.com/news/2013/oct/2/nsa-chief-figures-foiled-terror-plots-misleading/ (discussing General Keith Alexander's testimony that the number of terrorist plots foiled was one or two, and not fifty-four as the Obama administration claimed). For earlier incidents of government misstatements regarding mass surveillance, see Charles Babington & Dan Eggen, *Gonzales Seeks to Clarify Testimony on Spying*, WASH. POST, Mar. 1, 2006, at A8; Dan Eggen & Walter Pincus, *Varied Rationales Muddle Issue of NSA Eavesdropping*, WASH. POST, Jan. 27, 2006, at A6 (noting that administration officials had "emphasized in testimony and public statements that the NSA was prohibited from engaging in domestic surveillance—even as the agency was clearly doing so" pursuant to President Bush's orders).

305 *See* Glenn Greenwald & Spencer Ackerman, *How the NSA Is Still Harvesting Your Online Data*, THE GUARDIAN (June 27, 2013), http://www.theguardian.com/world/2013/jun/27/nsa-online-metadata-collection ("A review of top-secret NSA documents suggests that the surveillance agency still collects and sifts through large quantities of Americans' online data—despite the Obama administration's insistence that the program that began under Bush ended in 2011.").

to abide by court orders.[306] This truth-telling deficit calls for circumspection about government claims regarding mass surveillance and justifies defense access in order to protect the rights of the accused.

In particular, the Bill of Rights contains a series of defense trial rights as part of "what might loosely be called the area of constitutionally guaranteed access to evidence."[307] Taken together, the provisions ensure the delivery of "exculpatory evidence into the hands of the accused, thereby protecting the innocent from erroneous conviction and ensuring the integrity of our criminal justice system."[308] Among other things, the Sixth Amendment guarantees the right of the accused "to have compulsory process for obtaining witnesses in his favor."[309] The Compulsory Process Clause has a parallel function to the Sixth Amendment's better-known Confrontation Clause: "Just as an accused has the right to confront the prosecution's witnesses for the purpose of challenging their testimony, he has the right to present his own witnesses to establish a defense."[310] By protecting the right to compel witness attendance, the Constitution guarantees "the right to present a defense, the right to present the defendant's version of the

306 *See, e.g.*, [*redacted*], No. [*redacted*], 2011 WL 10945618, at *5 & n.14, *6, *9 (Foreign Intelligence Surveillance Ct. Oct. 3, 2011) (noting that "for the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different from what the Court had been led to believe," and stating that the court was "troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program"); *In re* FBI for an Order Requiring the Production of Tangible Things from [*redacted*], No. BR 09-13, 2009 WL 9150896, at *2 (Foreign Intelligence Surveillance Ct. Sept. 25, 2009) (stating that it was "deeply troubled" by noncompliance incidents, which occurred shortly after the NSA's completion of "end to end review" of the relevant processes "and its submission of a report intended to assure the Court that NSA had addressed and corrected the issues giving rise to the history of serious and widespread compliance problems"); *In re* Production of Tangible Things from [*redacted*], No. BR 08-13, 2009 WL 9150913, at *2–9 (Foreign Intelligence Surveillance Ct. Mar. 2, 2009) (describing government misrepresentations and violations of court orders); *In re* Production of Tangible Things from [*redacted*], No. BR 08-13, 2009 WL 9157881, at *2 (Foreign Intelligence Surveillance Ct. Jan. 28, 2009) ("The Court is exceptionally concerned about what appears to be a flagrant violation of its Order in this matter . . . ."); Memorandum Opinion at 3, [*redacted*], No. PR/TT [*redacted*] (Foreign Intelligence Surveillance Ct. [*redacted*]) ("NSA exceeded the scope of authorized acquisition continuously during the more than [*redacted*] years of acquisition . . . ."), *available at* http://www.dni.gov/files/documents/1118/CLEAN EDPRTT%202.pdf; *see also In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620–21 (Foreign Intelligence Surveillance Ct. 2002) (describing government's "misstatements and omissions of material facts" in FISA applications), *rev'd on other grounds*, *In re* Sealed Case, 310 F.3d 717 (Foreign Intelligence Surveillance Ct. Rev. 2002).

307 United States v. Valenzuela-Bernal, 458 U.S. 858, 867 (1982) (referring to defense rights contained in the Fifth and Sixth Amendments).

308 California v. Trombetta, 467 U.S. 479, 485 (1984).

309 U.S. CONST. amend. VI.

310 Washington v. Texas, 388 U.S. 14, 19 (1967).

facts as well as the prosecution's to the jury so it may decide where the truth lies."[311]

At a minimum, the Supreme Court's jurisprudence establishes that a defendant has "the right to the government's assistance in compelling the attendance of favorable witnesses at trial and the right to put before a jury evidence that might influence the determination of guilt."[312] To be sure, the Court has also made clear that "the mere invocation of that right cannot automatically and invariably outweigh countervailing public interests."[313] Compulsory process cannot be used irresponsibly to undermine the basic goals of a criminal justice system by hampering the legal process or impeding the fact-finding function of a criminal trial.[314] But although officials have some latitude concerning the disclosure of information and its use in court, that flexibility has limits when it infringes upon a criminal defendant's right to "a meaningful opportunity to present a complete defense."[315]

The refusal to disclose potentially exonerating evidence undercuts the aims of the criminal justice system—most obviously, an accurate fact-finding process in pursuit of the truth. In holding that even the President could not resist a subpoena in a criminal case, the Supreme Court emphasized that the nation, through its Constitution and legal tradition,

> elected to employ an adversary system of criminal justice in which the parties contest all issues before a court of law. The need to develop all relevant facts in the adversary system is both fundamental and comprehensive. The ends of criminal justice would be defeated if judgments were to be founded on a partial or speculative presentation of the facts. The very integrity of the judicial system and public confidence in the system depend on full disclosure of all the facts, within the framework of the rules of evidence. To ensure that justice is done, it is imperative to the function of courts that compulsory process be available for the production of evidence needed either by the prosecution or by the defense.[316]

Another fundamental part of the defense right of access is the government's discovery obligations under the Due Process Clause. Pursuant to *Brady v. Maryland* and its progeny, the prosecution is required to disclose favorable evidence—essentially, exculpatory and

---

311 *Id.*

312 Pennsylvania v. Ritchie, 480 U.S. 39, 56 (1987).

313 Taylor v. Illinois, 484 U.S. 400, 414 (1988).

314 *See id.* at 414–15 ("The integrity of the adversary process, which depends both on the presentation of reliable evidence and the rejection of unreliable evidence, the interest in the fair and efficient administration of justice, and the potential prejudice to the truth-determining function of the trial process must also weigh in the balance.").

315 Crane v. Kentucky, 476 U.S. 683, 690 (1986) (quoting California v. Trombetta, 467 U.S. 479, 485 (1984)) (internal quotation marks omitted).

316 United States v. Nixon, 418 U.S. 683, 709 (1974).

witness impeachment evidence—that is material to the defense and in the possession of the government.[317] In post-conviction review, evidence is considered "material" to the defense if "there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different."[318]

The scope of the prosecution's duty includes learning of "any favorable evidence known to the others acting on the government's behalf in the case, including the police."[319] Moreover, Rule 16 of the Federal Rules of Criminal Procedure requires the prosecution to disclose to the defendant certain categories of information "within the government's possession, custody, or control," including "any relevant written or recorded statement by the defendant" and documents and other objects that are "material to preparing the defense" or that "the government intends to use . . . in its case-in-chief at trial."[320]

The right of access helps inform a fundamental premise: the government is not obliged to prosecute any case—the principle of "mandatory prosecution" is foreign in American criminal justice[321]—but once a criminal case is brought, a defendant is granted various constitutional rights that must be respected and even facilitated by the government.[322] This premise applies with full force to digital evidence. The government is not compelled to use Big Data or to engage in mass surveillance, and it certainly is under no obligation to prosecute cases as a result of the information it finds. But when it does, the government must provide a basic level of evidentiary access and ability to challenge the prosecution as required by the Constitution.[323]

---

317 *See* Brady v. Maryland, 373 U.S. 83, 87 (1963) (holding that "suppression 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"); Giglio v. United States, 405 U.S. 150 (1972) (holding that suppression of material impeachment evidence violates due process under *Brady*).

318 United States v. Bagley, 473 U.S. 667, 682 (1985). "A 'reasonable probability' is a probability sufficient to undermine confidence in the outcome." *Id.*

319 Kyles v. Whitley, 514 U.S. 419, 437 (1995); *see also Giglio*, 405 U.S. at 154 (noting that the prosecution has the burden of ensuring "communication of all relevant information on each case to every lawyer who deals with it").

320 FED. R. CRIM. P. 16(a)(1).

321 *See, e.g.*, THE PROSECUTOR IN TRANSNATIONAL PERSPECTIVE 84–86, 200–01 (Erik Luna & Marianne L. Wade eds., 2012) (discussing the broad charging discretion granted to American prosecutors).

322 *See generally* David A. Sklansky, *Quasi-Affirmative Rights in Constitutional Criminal Procedure*, 88 VA. L. REV. 1229, 1238–43 (2002) (discussing the rights that the government is required to provide criminal defendants, most notably, those rights granted by the Fifth and Sixth Amendments).

323 After revelations of warrantless mass surveillance under the Bush Administration—known as the "President's Surveillance Programs" (PSP)—the Inspector General admonished the Justice Department to review its discovery obligations for information derived from such surveillance. *See* OIG Report, *supra* note 250, at 19 (summarizing the Inspector

B. Barriers to Digital Innocence

A defendant's right to access Big Data information to prove his innocence faces several obstacles. The government's mass surveillance programs are ostensibly secret, despite appearing on the front page of every major newspaper. Moreover, defendants may have trouble accessing information that is available for use by law enforcement but is in the possession of another government agency or entity. Even though investigators can tap the information source in furtherance of a criminal probe, and prosecutors may rely upon the resulting information as evidence at trial, the government often balks at defense requests for information possessed by agencies outside of the law enforcement community. This section addresses these barriers to claims of digital innocence.

1. *State Secrets*

The so-called "state secrets privilege" provides the government a limited prerogative to withhold classified information (and perhaps nonclassified "state secrets") sought in court proceedings, most often in civil cases brought against the government and its private-sector partners. A related procedural bar can preclude judicial inquiry altogether where state secrets are essential to the litigation.[324] The Supreme Court has long acknowledged that "no governmental interest is more compelling than the security of the Nation."[325] This includes "protecting both the secrecy of information important to our national security and the appearance of confidentiality so essential to the effective operation of our foreign intelligence service."[326] For instance, terrorism investigations can implicate various types of information that, if disclosed, might aid terrorist organizations and further violent schemes. In the case of Zacarias Moussaoui, the so-called "20th Hijacker" in the 9/11 plot, the government argued:

General's report). In particular, the Inspector General called upon the Justice Department to: (1) "carefully consider whether it must re-examine past cases to see whether potentially discoverable but undisclosed Rule 16 or *Brady* material was collected under the PSP, and take appropriate steps to ensure that it has complied with its discovery obligations in such cases"; and (2) "implement a procedure to identify PSP-derived information, if any, that may be associated with international terrorism cases currently pending or likely to be brought in the future and evaluate whether such information should be disclosed in light of the government's discovery obligations under Rule 16 and *Brady*." *Id.*

324 *See, e.g.*, Tenet v. Doe, 544 U.S. 1, 11 (2005) (adhering to categorical bar announced in *Totten v. United States*, 92 U.S. 105 (1876), and emphasizing that the "state secrets privilege and the more frequent use of *in camera* judicial proceedings simply cannot provide the absolute protection" necessary in lawsuits against the government where the plaintiffs' success depends upon the existence of their alleged secret relationship with the government).

325 Haig v. Agee, 453 U.S. 280, 307 (1981).

326 Snepp v. United States, 444 U.S. 507, 509 n.3 (1980) (per curiam).

> Because al Qaeda operates as a clandestine force relying on sleeper agents to mount surprise attacks, one of the most critical fronts in the current war involves gathering intelligence about future terrorist attacks and how the terrorist network operates—identifying where its operatives are, how it plans attacks, who directs operations, and how they communicate.[327]

To do this, the government has developed the aforementioned, rather amazing surveillance apparatus. In the realm of national security, the government often works with the development and deployment assistance of the private sector.[328] This is particularly the case in Big Data data mining, where partnerships with Silicon Valley giants form the bedrock of the government surveillance program.[329] In many instances, the specifications and even the existence of the technology remain secrets of the state.[330] For evident reasons, the government often wishes to avoid disclosing information about hardware and software that could allow malefactors to thwart detection. Such information might fall into the hands of foreign enemies and accrue to their benefit, and typically to U.S. detriment as well. The same is true of information obtained from American allies, the secrecy of which has long been recognized as critical to the successful conduct of foreign affairs.[331] The government also has a clear interest in the anonymity of informants, many of whom are lodged within criminal schemes involving racketeering, drug trafficking, terrorism, and so on.

It should be noted, however, that in the case of mass electronic surveillance the biggest concern is not necessarily the existence of the programs, which are now generally acknowledged, nor is it the capability to gather information, since the systems are "full take." Rather, the issue may be the degree to which the government complies with the law. Oftentimes, legal limits are kept secret to prevent them from serving as a guide for evasion.[332] This creates an interesting effect: the

---

327 Hamdan v. Rumsfeld, 548 U.S. 557, 723–24 (2006) (Thomas, J., dissenting) (quoting Brief for the United States at 9, United States v. Moussaoui, 382 F.3d 453 (4th Cir. 2004) (No. 03-4792)) (internal quotation marks omitted).

328 *See, e.g.*, Richards, *supra* note 154, at 1934, 1958–59 (noting that private and public sector surveillance "use the same technologies and techniques" and "operate through a variety of public/private partnerships").

329 *See* Glenn Greenwald et al., *Microsoft Gave NSA Access to Users' Messages*, THE GUARDIAN, July 12, 2013, at A1 (describing partnerships between the NSA and several corporations).

330 *See, e.g.*, Greenwald, *supra* note 62 (explaining that Verizon could not "disclos[e] to the public either the existence of the FBI's request for its customers' records or the court order" compelling the production of those call records to the NSA).

331 *See, e.g.*, United States v. Curtiss-Wright Exp. Corp., 299 U.S. 304, 320 (1936) (noting that regarding foreign affairs, "[s]ecrecy in respect of information gathered by [government agents] may be highly necessary, and the premature disclosure of it productive of harmful results").

332 *See* Richards, *supra* note 154, at 1942–45 (criticizing surveillance law's limited protections where plaintiffs "can only challenge secret government surveillance they can

more careful the government is about respecting legal limits, the more it seeks to isolate discussions about those legal limits from the public.

The 1953 case of *United States v. Reynolds*[333] is frequently cited for recognizing the government privilege on state secrets, as well as establishing its boundaries and the process for invocation. Under *Reynolds*, the judge "must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect."[334] This requires a "formula of compromise," balancing the "circumstances of the case" and the requesting party's "showing of necessity" for the evidence versus the government's concerns that "compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged."[335]

In drawing upon the exercise of similar doctrines, the *Reynolds* Court apparently contemplated that the claimant could disclose to the judge enough information—perhaps filed under seal and reviewed in camera—so that the judge could determine the existence of the privilege and, if it existed, the extent to which it might be overridden by the opposing party's need for the information. If the judge decides there is a reasonable danger that disclosure would harm U.S. national security, "the claim of the privilege will be accepted without requiring further disclosure,"[336] and the relevant information will be considered unavailable for purposes of the litigation.

Due to the privilege's broad sweep, some courts have maintained that, "whenever possible, sensitive information must be disentangled from nonsensitive information to allow for the release of the latter."[337] In a simple example, secret information might be redacted from relevant pages instead of suppressing the whole document. Others have questioned the judiciary's ability to neatly separate classified and unclassified information in light of the so-called "mosaic theory," which postulates that an overall picture of national security efforts can be revealed by analyzing and fitting into place otherwise innocent "bits and pieces" of information.[338] As one court argued, "if seemingly innocuous information is part of a classified mosaic, the state secrets

---

prove," yet acknowledging the simultaneous benefits of such a standard, which provides security from potential crime).

333 345 U.S. 1 (1953).

334 *Id.* at 8 (citation omitted).

335 *Id.* at 9–11.

336 *Id.* at 9.

337 Ellsberg v. Mitchell, 709 F.2d 51, 57 (D.C. Cir. 1983); *see also* Doe v. Tenet, 329 F.3d 1135, 1152–53 (9th Cir. 2003), *rev'd*, 544 U.S. 1 (2005) (providing possible safeguards to prevent public exposure of secret materials).

338 *See, e.g.*, CIA v. Sims, 471 U.S. 159, 178 (1985).

privilege may be invoked to bar its disclosure and the court cannot order the government to disentangle this information from other classified information."[339]

Jewel v. National Security Agency provides an example of how these complex issues are resolved in an ongoing case.[340] In 2008, the plaintiffs in *Jewel* brought a challenge to the NSA warrantless mass surveillance program conducted by gathering Internet backbone information directly from telecommunications providers.[341] On remand from the Ninth Circuit,[342] Judge Jeffrey White considered whether the state secrets privilege barred the entire subject matter of the litigation because the programs themselves were secret, and whether the FISA section relating to procedures for use of electronic surveillance data, 50 U.S.C. § 1806(f), preempted the federal common law of state secrets.[343]

On the first question, Judge White determined that recent public disclosure of government mass electronic surveillance meant that there was no longer an interest in keeping the existence of the programs secret.[344] Obviously, this is an important point for those seeking disclosure of government surveillance information to prove their innocence. The surveillance programs are now public, and the data sought by run-of-the-mill defendants will not touch on national security. As such, there remains little in the way of a secret to keep were the government required to disclose non-sensitive data, such as information relevant to a defendant's alibi.

Judge White further developed this distinction between subject matter and individual data in his analysis of the FISA procedures for reviewing information derived from electronic surveillance. The court noted that 50 U.S.C. § 1806(f) provides the exclusive means for evaluating electronic surveillance evidence.[345] Because Congress chose to impose these rules "notwithstanding any other . . . law,"[346] and author-

339 Kasza v. Browner, 133 F.3d 1159, 1166 (9th Cir. 1998).

340 *See* Jewel v. NSA, No. C 08-04373 JSW, No. C 07-00693 JSW, 2013 WL 3829405 (N.D. Cal. July 23, 2013).

341 *Id.* at *23.

342 Jewel v. NSA, 673 F.3d 902, 913–14 (9th Cir. 2011).

343 *Jewel*, 2013 WL 3829405, at *7.

344 *Id.* In December 2013, the Director of National Intelligence, James Clapper, filed a declaration stating that the government was no longer asserting privilege over the existence of the warrantless mass surveillance program. Public Declaration of James R. Clapper, Director of National Intelligence at 2–6, Jewel v. NSA, No. C 08-04373 JW, No. C 07-00693 JSW, 2013 WL 3829405 (N.D. Cal. July 23, 2013), *available at* http://www.dni.gov/files/documents/1220/DNI%20Clapper%202013%20Jewel%20Shubert%20SSP%20Unclassified%20Signed%20Declaration.pdf. Nonetheless, the government continues to claim the state secrets privilege with regard to still-classified information on the program's scope and operational details. *See id.* at 6–21.

345 *Jewel*, 2013 WL 3829405, at *8.

346 50 U.S.C. § 1806(f) (2006 & Supp. V 2011).

ized the section as the "exclusive means by which materials [designated as sensitive by the government] shall be reviewed,"[347] the court determined that section 1806(f) preempted the state secrets privilege for purposes of evaluating evidence of electronic surveillance.

> The specific description leaves no room for application of the state secrets privilege and is, in effect, a "codification of the state secrets privilege for purposes of relevant cases under FISA, as modified to reflect Congress's precise directive to the federal courts for the handling of materials and information with purported national security implications."[348]

It remains to be seen how far this rationale extends. Not all cases involving surveillance will raise FISA claims; for instance, some will entail wiretapping under Title III. Moreover, section 1806(f) review goes to the lawfulness and appropriateness of the surveillance. It is not clear whether the in camera review imagined by section 1806(f) extends to all those seeking to "discover or to obtain" the fruits of government surveillance or only to those who challenge the legality or appropriateness of the surveillance. But the overall tenor of section 1806 is concerned precisely with use and disclosure of electronic surveillance in criminal cases, and the ability of "aggrieved persons" to challenge the collection and use of that data. It would be a strange reading of the statute if parties were permitted access to information for purposes of challenging the legality of that information but not for purposes of proving their innocence.

In addition, it must be kept in mind that criminal defendants seeking access to Big Data are in a different position from civil litigants. As the Supreme Court noted in *Reynolds*,

> The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense. Such rationale has no application in a civil forum where the Government is not the moving party, but is a defendant only on terms to which it has consented.[349]

This position is entirely consistent with the foregoing premise: the government is not required to prosecute a criminal case, but when it does, it must respect and at times facilitate the defendant's rights.[350]

---

347 18 U.S.C. § 2712(b)(4) (2012).

348 *Jewel*, 2013 WL 3829405, at *9 (quoting *In re* NSA Telecomms. Records Litig., 564 F. Supp. 2d 1109, 1119 (N.D. Cal. 2008)).

349 United States v. Reynolds, 345 U.S. 1, 12 (1953).

350 *See supra* Part IV.A.

Although lower court cases have subsequently concluded that the state secrets privilege does apply in criminal cases,[351] the doctrine has a more limited scope in light of the constitutional rights at stake, and it cannot defeat a claim of digital innocence backed by a sufficient showing that the government possesses relevant and potentially exculpatory evidence. Since the NSA scandal broke, defense attorneys have begun to seek government surveillance information as proof of innocence. In June 2013, lawyers for a robbery defendant filed a Rule 16 motion to require the government to hand over cell-site location information (CSLI), which, the defendant argued, would establish his innocence.[352] The court treated the motion as one under section 1806(f)[353] and ordered the government to respond, noting that "even if the Court determines that the surveillance was lawfully authorized or conducted, it must order discovery or disclosure to the extent that due process requires it."[354]

In an unredacted portion of its response, the government alleged that it did not receive CSLI "under this program."[355] Still, it appears increasingly likely that the government does receive this data under some program. After all, CSLI is a key component of the NSA cellphone tracking program CO-TRAVELER.[356] Moreover, CSLI is openly retained and recorded by almost every telecommunications carrier, which could be required to turn over this information as metadata within the purview of FISC orders.[357] Perhaps the qualifying language ("under this program") saves the government's assertions; or perhaps the government explained more in the redacted portions of its filing. In the end, the government's claim that it did not gather CSLI "under this program" appeared to convince the defendant, who withdrew his request before the judge ruled on the merits.[358] But the

351 *See, e.g.*, United States v. Aref, 533 F.3d 72, 79–80 (2d Cir. 2008) (holding that the state secrets privilege applies to requests for privileged information brought under the Classified Information Procedures Act in criminal cases).

352 Motion to Compel Production of Phone Records at 3, United States v. Davis, No. 11-cr-60285-RSR (S.D. Fla. filed June 9, 2013).

353 *See supra* notes 345–48 and accompanying text.

354 Order Requiring Response from Government at 3, United States v. Davis, No. 11-cr-60285-RSR (S.D. Fla. filed June 10, 2013), *available at* http://de.scribd.com/doc/147116286/Order-Requiring-Response-Re-FISA-Records.

355 Government's Response to the Court's Order and Motion for a Protective Order Pursuant to Section 4 of the Classified Information Procedures Act and Rule 16(d)(1) of the Federal Rules of Criminal Procedure and Memorandum of Law at 2, United States v. Davis, No. 11-cr-60285-RSR (S.D. Fla. filed June 19, 2013).

356 *See* Gellman & Soltani, *supra* note 5. The NSA Director, General Keith Alexander, testified that the NSA had run pilot projects collecting U.S. cellphone location data. Although claiming that the program was discontinued, General Alexander acknowledged that the NSA may resume the collection process in the future. *See id.*

357 *See supra* notes 261–68 and accompanying text.

358 *See* Reply to Government's Response to Defendant's Motion to Compel at 1, United States v. Davis, No. 11-cr-60285-RSR (S.D. Fla. filed June 20, 2013) ("Given the govern-

matter will have to be decided at some point—new defendants are already raising similar challenges, and they are unlikely to be dissuaded by government assurances.[359]

2. *Agency Alignment*

Another potential barrier to digital innocence claims is the divide between the law enforcement community and the intelligence community. As discussed earlier, the roots of the problem lie in the historical separation of intelligence gathering from criminal investigation—a separation that was always somewhat sketchy, given that the targets of intelligence agents are often involved in crime, while law enforcement has long relied upon information gleaned from intelligence operations. Moreover, the legal predicate for the separation no longer exists post–Patriot Act,[360] although the government continues to assert the division to limit defense access to information.[361]

Originally, the separation may have made some sense, as the goals of the two communities are not immediately congruent. The mission of the federal law enforcement community "is to identify, target, investigate, arrest, prosecute, and convict those persons who commit crimes in violation of Federal laws."[362] By contrast, the mission of the intelligence community—which includes more than a dozen government organizations, such as the CIA and the NSA[363]—"is to perform intelligence activities necessary for the conduct of foreign relations and the protection of the national security, including the collection of information and the production and dissemination of intelligence; and the collection of information concerning espionage, international terrorist activities, and international narcotics activities."[364]

Few published cases have provided guidance on discovery obligations for information held by the intelligence community.[365] In gen-

---

ment's representation, Mr. Brown concedes that the records will not assist him in establishing his innocence . . . [and] therefore withdraws his requests . . . .").

359 *See supra* note 294 and accompanying text.

360 *See supra* notes 232–35 and accompanying text.

361 *See, e.g.*, Mohamud Motion, *supra* note 157, at 46–50 (describing how prosecution narrowly construed its discovery obligations).

362 U.S. DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' MANUAL § 9-90.210(A) (rev. ed. 2008) [hereinafter USAM].

363 *See Mission: Member Agencies*, U.S. INTELLIGENCE COMMUNITY, http://www.intelligence.gov/mission/member-agencies.html (last visited Mar. 24, 2014).

364 USAM, *supra* note 362, § 9-90.210(A).

365 In *United States v. Libby*, a former White House official was charged with the unauthorized disclosure of classified information, namely, an undercover operative's affiliation with the CIA. Given "a rather free flow of documents" from the CIA to the special prosecutor's office, the trial judge concluded that the CIA was closely aligned with the prosecution for discovery purposes. United States v. Libby, 429 F. Supp. 2d 1, 11 (D.D.C. 2006); *see also* United States v. Diaz-Munoz, 632 F.2d 1330 (5th Cir. 1980) (determining that trial court

eral, the government's obligation to disclose goes beyond evidence known to be in its physical possession. The scope of this duty is not gauged by a prosecutor's knowledge, since information known to members of the "prosecution team"[366] can be imputed to the prosecutor. At times, prosecutors may be required to search for exculpatory evidence, including information maintained by government bodies that have a working relationship with the prosecution—or, as phrased by some courts, those agencies "closely aligned with the prosecution."[367] For example, cases have imputed to federal prosecutors evidence within the possession of the Drug Enforcement Agency, the Bureau of Prisons, and state law enforcement when these entities have been involved in case investigation or prosecution.[368]

The federal courts have differed on the appropriate standard for whether a given governmental body is aligned with the prosecution.[369] Some circuits have adopted "an expansive view" and "imputed a broad range of knowledge to the prosecution,"[370] placing an obligation on prosecutors to inquire of all agencies that have a potential connection with the case. Under this view, the government "is not a congery of independent hermetically sealed compartments," and "the prosecutor is duty bound to demand compliance with disclosure responsibilities by all relevant dimensions of the government."[371] Other circuits have taken narrower approaches to alignment, refusing to "infer the prosecutors' knowledge simply because some other government agents knew about the [information]."[372] Rather, alignment requires some form of cooperation between the prosecutor and the entity in question. The appropriate scope of alignment remains unresolved, as demonstrated by disagreement among judges within the same circuit.[373]

---

was required to undertake in camera review of CIA documents that defendant claimed were exculpatory); United States v. Poindexter, 727 F. Supp. 1470, 1487 (D.D.C. 1989) (determining that defendant was entitled to discovery of a limited set of documents prepared by the executive branch relating to the Iran-Contra affair).

366 *See, e.g.*, Moon v. Head, 285 F.3d 1301, 1309 (11th Cir. 2002).

367 *See, e.g.*, United States v. Brooks, 966 F.2d 1500, 1503 (D.C. Cir. 1992) (quoting United States *ex rel.* Smith v. Fairman, 769 F.2d 386, 391 (7th Cir. 1985)) (internal quotation marks omitted).

368 *See, e.g.*, United States v. Blanco, 392 F.3d 382, 393–94 (9th Cir. 2004) (DEA agents); United States v. Antone, 603 F.2d 566, 570 (5th Cir. 1979) (state agents); United States v. Burnside, 824 F. Supp. 1215, 1257–58 (N.D. Ill. 1993) (federal prison personnel).

369 *See* Afsheen John Radsan, *Remodeling the Classified Information Procedures Act (CIPA)*, 32 CARDOZO L. REV. 437, 454–57 (2010).

370 Smith v. Sec'y of N.M. Dep't of Corr., 50 F.3d 801, 825 n.36 (10th Cir. 1995) (citing United States v. Thornton, 1 F.3d 149, 158 (3d Cir. 1993)).

371 United States v. Osorio, 929 F.2d 753, 760, 62 (1st Cir. 1991).

372 United States v. Locascio, 6 F.3d 924, 949 (2d Cir. 1993).

373 *Compare* United States v. Safavian, 233 F.R.D. 12, 14 (D.D.C. 2005) (adopting an expansive view), *with* United States v. Libby, 429 F. Supp. 2d 1, 6 n.10 (D.D.C. 2006) (supporting a narrower view).

Regardless of the standard, however, it is clear that the government obligation to respond to defense requests for information does not stop at the edge of an agency's organizational chart. In the Oklahoma City Bombing case, the trial court noted that lack of agency alignment

> does not limit the duty to inquire of such agencies for information which may be exculpatory or impeaching as to the government's evidence or material to the preparation of the defense of Mr. McVeigh and Mr. Nichols. Accordingly, the prosecutors must respond to the defendants' requests for information from a broad perspective of the government as a whole.[374]

The trial court did acknowledge the strain placed upon the prosecutors in this case, and in terrorism cases in general,[375] but this did not reduce the government's obligation to comply with discovery rules.

> Application of the *Brady* doctrine to this case is especially difficult because the scope of inquiry is so broad and the information gathering capability of all government agencies is so great. The lawyers appearing on behalf of the United States, speaking for the entire government, must inform themselves about everything that is known in all of the archives and all of the data banks of all of the agencies collecting information which could assist in the construction of alternative scenarios to that which they intend to prove at trial. That is their burden under *Brady*[, and it] is not excused by any inconvenience, expense, annoyance or delay.[376]

Such exhortations are not always borne out in executive protocol, however. To this day, the *United States Attorneys' Manual* uses language that harks back to the pre-9/11 wall.[377] Both the law enforcement community and the intelligence community belong to the executive branch of government, but they maintain "very distinct identities, mandates, and methods," guided by different legal provisions and arrangements.[378] "Although coordination on matters of common concern is critical to the proper functioning of the two communities, prosecutors must be aware of the concomitant need of both communities to maintain a well-delineated separation between criminal prosecutions and foreign intelligence activities, in which less-stringent restraints apply to the government."[379]

Another policy document for federal prosecutors, the *Criminal Resource Manual*, recognizes that when the intelligence community

---

374 United States v. McVeigh, 923 F. Supp. 1310, 1315 (D. Colo. 1996).
375 *See* United States v. McVeigh, 954 F. Supp. 1441, 1450 (D. Colo. 1997).
376 *Id.*
377 *See supra* notes 221–23 and accompanying text.
378 USAM, *supra* note 362, § 9-90.210(A).
379 *Id.*

actively participates in an investigation or prosecution, "it likely has aligned itself with the prosecution and its files are subject to the same search as would those of an investigative law enforcement agency assigned to the case."[380] Examples would include cases where an intelligence agency provided information that served as a predicate for a search warrant or an indictment. The *Criminal Resource Manual* then turns to the question of when intelligence files should be searched even though the intelligence community (IC) was not actively involved in a criminal investigation. Specifically, it suggests a sliding scale where a greater demonstration by the defense is necessary to justify broader, more difficult searches. In any case, a prosecutor must search intelligence files when he has "direct or reliable knowledge of potential *Brady* and/or other discovery material in the possession of the IC" or when there "exists any reliable indication suggesting that the IC possesses evidence that meets the *Brady* case law standard of materiality."[381] Finally, certain types of cases may justify a "prudential search," defined as "one based not upon a known duty to the defendant or to a known nexus to national security matters but rather on the fact that the case meets a certain profile of cases likely to implicate such issues."[382]

According to one former federal prosecutor and CIA attorney, the actual search process can be somewhat circuitous and circumspect.

> [P]rosecutors do not rummage through an intelligence agency's vault and determine what needs to be disclosed file by file. Instead, an administrator without a law degree searches the intelligence files in response to a laundry list from the prosecutor. After the search is complete, the prosecutor, whose case—and license—are on the line, will travel to the intelligence agency and apply the rules of discovery to decide which of the found files, if any, need to be turned over to the defense.[383]

In this process, counsel for the given intelligence agency may intercede and advocate against disclosure. Sometimes spymasters and prosecutors disagree on whether alignment exists in a particular case.[384] These disagreements reinforce other differences. For instance, the "CIA does not gather and store its information in the same way that the FBI does," and the intelligence community "is not as concerned with chains of custody and the rules of evidence."[385]

---

380 *Id.* at § 2052(B)(1).
381 *Id.* at § 2052(B)(2)(a).
382 *Id.* at § 2052(B)(4).
383 Radsan, *supra* note 369, at 452.
384 *See id.* at 456.
385 *Id.* at 456–57.

The current system thus reflects a separation of agencies that does not track the post-9/11 realities of information sharing and interagency cooperation. In the end, courts may have the final say on disclosure but only after an opaque process involving file searches by intelligence agency staff and any negotiations between prosecutors and spymasters. Worse yet, although the walls between agencies have been torn down with respect to the flow of incriminating information, they have been actively reinforced with respect to exonerating information. Agency cooperation speeds the flow of incriminating information but impedes the flow of exonerating information. Automated searches of very large databases provide incriminating information, while exonerating evidence arises, if at all, from the fumbling searches of "administrators without a law degree."

Above all, defendants must know the path information has taken in order to locate potential sources of information that may prove them innocent. As noted earlier, intelligence and law enforcement agencies have actively shared information.[386] Reportedly, however, law enforcement officials have been instructed to hide the source of this information.[387] According to documents reviewed by the news agency Reuters, an entity within the Drug Enforcement Agency—the Special Operations Division (SOD)—funnels NSA intelligence to law enforcement officers but directs them to conceal the true origins of any resulting criminal investigation from defense attorneys, prosecutors, and judges.[388] To pull off this ruse, law enforcement is trained to "recreate" information through a process euphemistically termed "parallel construction": laundering the information in question by concocting independent sources through field interviews, confidential informants, physical searches and seizures, etc.[389]

Some legal experts have denounced the practice as more troubling than the NSA spying scandal itself.[390] Like the post-*Clapper* failure to provide notice to affected defendants,[391] parallel construction insulates the government's surveillance activities from legal scrutiny. By misleading the courts, it prevents the judiciary from fulfilling its

386 *See supra* notes 232–35, 290–96 and accompanying text.

387 *See* John Shiffman & Kristina Cooke, *U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS, Aug. 5, 2013, *available at* http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805?irpc=932; John Shiffman & David Ingram, *IRS Manual Detailed DEA's Use of Hidden Intel Evidence*, REUTERS, Aug. 7, 2013, *available at* http://www.reuters.com/article/2013/08/07/us-dea-irs-idUSBRE9761AZ20130807.

388 Shiffman & Cooke, *supra* note 387.

389 *See id.*; Shiffman & Ingram, *supra* note 387.

390 Even a current federal prosecutor acknowledged that "[l]ying about where the information came from is a bad start if you're trying to comply with the law because it can lead to all kinds of problems with discovery and candor to the court." Shiffman & Cooke, *supra* note 387 (quoting the prosecutor) (internal quotation marks omitted).

391 *See supra* notes 290–96 and accompanying text.

fundamental role in assessing the factual basis for court orders. Most of all, information laundering deprives the accused of a meaningful opportunity to defend himself at trial. Criminal defendants must know the path information has taken in order to locate sources of information that may prove them innocent. When the government obscures the origin and course of information, they not only inhibit the defense from challenging the information's origins but also undermine efforts to locate other discoverable, and perhaps exonerating, material. Defendants find themselves confronted with evidence that they have no way to contest or contextualize. For this reason, defense attorneys are now challenging the practice as a violation of the defendant's right to a fair trial, and they are making more aggressive discovery requests to ensure that potentially exculpatory evidence is not secreted in intelligence files.[392]

All of this justifies a straightforward approach: agency alignment should follow the movement of information, not arbitrary lines of agency organization. Where incriminating information flows between organizations, exonerating information must flow as well. This is a far simpler principle than attempting to unpack the organizational charts of agencies, which cooperate in providing incriminating information but too often refuse to assist in discovering proof of innocence.

V
Establishing Digital Innocence

To some extent, all criminal trials pit the rights of the accused against the interests of government. These conflicts are magnified, however, when a defendant seeks information that has been gathered as part of the national security apparatus. On the one hand, all agree that the government must function with some level of secrecy on issues of national security. This is particularly true when the information in question could be used against the United States by foreign powers, or when it might be exploited by terrorist organizations to plan and carry out violent attacks. On the other hand, removing the wall between intelligence surveillance and law enforcement has created a troubling asymmetry in the criminal justice system. The government acts expeditiously to secure those records that it needs to secure a conviction, but it may overlook or at least not pursue digital information that undermines the prosecution. Such duplicity is incompatible with a fair adversarial system committed to accurate

392 *See* David Ingram & John Shiffman, *U.S. Defense Lawyers to Seek Access to DEA Hidden Intelligence Evidence*, Reuters, Aug. 8, 2013, *available at* http://www.reuters.com/article/2013/08/08/us-dea-irs-idUSBRE9761AZ20130808.

fact-finding consistent with the long-accepted maxim concerning errors in criminal justice.[393]

Acknowledging that the competing values at stake are both of the highest order, the law should evolve to meet the resulting challenges. Among other things, we would advocate the inclusion of innocence-protective measures within the various privacy reforms currently under discussion in response to the NSA surveillance scandal. We are realistic, however, and recognize that such reforms may not be forthcoming. But this does not mean that claims of digital innocence cannot be raised within the current legal regime. In particular, this Part evaluates the prospects for such claims in two principal contexts: preventing wrongful convictions and exonerating innocent inmates.

The first category of cases is primarily concerned with ensuring that defense counsel will have access to proof of innocence prior to trial and can present it in a meaningful fashion before the finder of fact. Along these lines, the following considers the Classified Information Procedures Act—which governs when and how defense counsel can access protected federal government information—as well as the means to secure information from private third parties and from the United States as a third party. The second category of cases is concerned with making sure that those who are wrongfully convicted have the ability to contest their continued imprisonment based on proof of innocence. The challenge here is the procedural bar established by the Antiterrorism and Effective Death Penalty Act, which raises questions as to whether claims of digital innocence will free the wrongfully convicted even though the evidence only became available as a result of technological developments years after trial.

A. Access to Information at Trial

Imagine a defendant is charged as a participant in a bank robbery. The prosecution seeks to bolster its case by using cellphone call records to show the relationship among the actors. But it allegedly lacks cellphone records from the actual time of the robbery, which the defendant asserts would demonstrate that he was not at the scene of the crime. The prosecution's claim appears reasonable: the service provider no longer had the records.[394] While trial is pending, how-

---

393 *See* 4 WILLIAM BLACKSTONE, COMMENTARIES *352 ("[F]or the law holds, that it is better that ten guilty persons escape, than that one innocent suffer."); *see also* Letter from Benjamin Franklin to Benjamin Vaughan (Mar. 14, 1785), *in* 9 THE WRITINGS OF BENJAMIN FRANKLIN: COLLECTED AND EDITED WITH A LIFE AND INTRODUCTION 291, 293 (Albert H. Smyth ed., 1906) ("That it is better 100 guilty Persons should escape than that one innocent Person should suffer, is a Maxim that has been long and generally approved.").

394 This hypothetical is based on Order Requiring Response from Government at 1–2, United States v. Davis, No. 11-60285-CR-ROSENBAUM (S.D. Fla. June 10, 2013), ECF No. 786.

ever, disclosures from the NSA scandal make it a matter of public record that the U.S. government has stored every record of every call made by several carriers, including the one used by the defendant. Defense counsel then moves to compel the government to disclose the cell-site location information that may prove the defendant's innocence. The case raises issues as to the process under which the request for information will be reviewed and the circumstances that might permit the defendant to prove his innocence through government data. The following discussion is intended to show that claims of digital innocence cannot be dismissed as asking the impossible.

1. *CIPA and CIPA-like Processes*

In 1980, Congress adopted a statutory framework to evaluate the types of defense requests and government responses in situations involving government secrets, such as the NSA program in the above fact pattern.[395] The Classified Information Procedures Act (CIPA) sets out the process governing the disclosure and use in federal criminal trials of government secrets denominated as "classified information."[396] CIPA did not create new discovery and evidentiary rules nor did it limit those that already existed.[397] Instead, the scheme seeks to prevent unwarranted disclosure of such information, while at the same time protecting a defendant's constitutional rights.[398]

The prototypical case would involve spies who are charged with espionage, former clandestine agents or government officials who claimed their crimes were supported by the government, or whistleblowers who sought to reveal government misconduct.[399] In these situations, the government invokes CIPA to inhibit the defendant from disclosing classified information already in his possession. But the government can also use CIPA to prevent defendants from receiving classified information through the pretrial discovery process, a context that has become relatively common in post-9/11 terrorism prosecutions. The CIPA procedures are supposed to provide an opportunity for the government to make a fully informed judgment about the cost to national security of proceeding with the case, as well

395 Classified Information Procedures Act (CIPA), 18 U.S.C. app. 3 §§ 1–16 (2012).

396 *See id.* § 1 (defining "Classified information"); *see also* Exec. Order No. 13,526, 3 C.F.R. 298 (2010) (current executive order establishing "a uniform system for classifying, safeguarding, and declassifying national security information").

397 *See, e.g.*, United States v. Baptista-Rodriguez, 17 F.3d 1354, 1363 (11th Cir. 1994) ("CIPA does not create new law governing the admissibility of evidence."); United States v. Yunis (*Yunis II*), 867 F.2d 617, 621 (D.C. Cir. 1989) ("[CIPA] creates no new rights of or limits on discovery of a specific area of classified information.").

398 *See, e.g.*, United States v. O'Hara, 301 F.3d 563, 568 (7th Cir. 2002) ("[CIPA was intended] to protect classified information from unnecessary disclosure at any stage of a criminal trial . . . in a way that does not impair the defendant's right to a fair trial.").

399 *See* S. REP. NO. 96-823, at 1–4 (1980); H.R. REP. NO. 96-831, at 7 (1980).

as offering possible alternatives to disclosing classified information during discovery or trial.[400]

The relationship of the statutory scheme to the state secrets privilege is murky—"it merely presupposes"[401] a government privilege to avoid disclosing classified information. The precise privilege at issue, its relationship to CIPA, and the ensuing consequences have been the subject of debate.[402] Ultimately, these issues may not matter for purposes of digital evidence that could provide hard proof of innocence. As mentioned earlier, the *Reynolds* Court emphasized that a government privilege cannot deny a defendant the ability to effectively mount a defense.[403] Moreover, CIPA's legislative history made clear that "the defendant should not stand in a worse position, because of the fact that classified information is involved, than he would without this Act."[404] Were it otherwise, CIPA would be in tension with the defendant's right to present a complete defense. The government cannot prosecute an individual while at the same time hampering his use of information necessary to defend himself against the prosecution.[405] "Although CIPA contemplates that the use of classified information be streamlined, courts must not be remiss in protecting a defendant's right to a full and meaningful presentation of his claim to innocence."[406]

To facilitate early resolution of disputes concerning classified information, section 2 of CIPA permits either party or the court to call for a pretrial conference any time after the filing of an indictment "to consider matters relating to classified information that may arise in connection with the prosecution."[407] Section 6 governs hearings to determine the use, relevance, or admissibility of classified information, where such hearings must be held in camera on request of the Attorney General certifying that a public proceeding may result in the

---

400 *See, e.g.*, United States v. Collins, 720 F.2d 1195, 1197 (11th Cir. 1983).

401 United States v. Abu-Jihaad, 630 F.3d 102, 140 (2d Cir. 2010).

402 *Compare Yunis II*, 867 F.2d at 623 ("[T]he procedures [CIPA] mandates protect a government privilege in classified information similar to the informant's privilege . . . ."), *and* United States v. Sarkissian, 841 F.2d 959, 966 (9th Cir. 1988) ("[*A*]*rguendo* . . . the enactment of CIPA does not affect the validity of *Reynolds*."), *and* H.R. REP. NO. 96-831, at 15 n.12 ("[I]t is well-settled that the common law state secrets privilege is not applicable in the criminal arena."), *with* United States v. Aref, 533 F.3d 72, 78–79 (2d Cir. 2008) (holding that CIPA implicates the state secrets privilege), *and* United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) (same), *and* United States v. Garey, 2004 WL 2663023 (M.D. Ga. Nov. 15, 2004) (same).

403 United States v. Reynolds, 345 U.S. 1, 12 (1953).

404 S. REP. NO. 96-823, at 9.

405 *See* United States v. Fernandez, 913 F.2d 148, 154 (4th Cir. 1990); *cf.* United States v. Coplon, 185 F.2d 629, 638 (2d Cir. 1950) (Hand, J.) ("Few weapons in the arsenal of freedom are more useful than the power to compel a government to disclose the evidence on which it seeks to forfeit the liberty of its citizens.").

406 *Fernandez*, 913 F.2d at 154.

407 18 U.S.C. app. 3 § 2 (2012).

disclosure of classified information.[408] Most importantly for present purposes, section 4 addresses defense requests for discovery of information in classified documents.[409] The lower courts seem to agree that the standard for defense discovery under CIPA is the same hurdle to overcome other government privileges, which must give way if the information "is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause."[410]

Section 4 states that, "upon a sufficient showing," the judge can authorize the government to delete specified items of classified information from documents to be provided the defendant, to substitute a summary of the information contained in the documents, or to substitute a statement admitting relevant facts that the information would tend to prove.[411] Section 6 also deals with alternatives to government disclosure, stating that a court may authorize a substitution for classified material "if it finds that the statement or summary will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information."[412]

If substitution efforts fail, the government may still prevent the discovery of classified information by filing an affidavit from the Attorney General objecting to disclosure of the information in question.[413] "Should the government do so, however, its ability to continue the prosecution will be seriously damaged or ended."[414] Specifically, section 6 requires the trial judge to dismiss the indictment against the defendant or, when "the interests of justice would not be served by dismissal," to take other remedial action, including dismissing specific

---

408 *Id.* § 6(a). *But see In re* Washington Post Co., 807 F.2d 383, 393 (4th Cir. 1986).

409 18 U.S.C. app. 3 § 4.

410 Roviaro v. United States, 353 U.S. 53, 60–61 (1957); *see, e.g.*, United States v. Aref, 533 F.3d 72, 79–80 (2d Cir. 2008) (adopting "the *Roviaro* standard for determining when the Government's privilege must give way in a CIPA case" and citing other circuits that have adopted this standard). There is an ongoing debate as to whether the courts should impose a higher evidentiary threshold in CIPA cases by balancing the defendant's need for relevant classified information against the government's interest in national security. *Compare* United States v. Rosen, 557 F.3d 192, 198 (4th Cir. 2009) (accepting balancing approach), *and* United States v. Sarkissian, 841 F.2d 959 (9th Cir. 1988) (same), *with* United States v. Baptista-Rodriguez, 17 F.3d 1354, 1363–64 (11th Cir. 1994) (rejecting balancing approach), United States v. Libby, 453 F. Supp. 2d 35, 44 (D.D.C. 2006) (same), *and* S. REP. No. 96-823, at 9 (1980) (same). *But cf.* United States v. Yunis (*Yunis II*), 867 F.2d 617, 625 (D.C. Cir. 1989) (refusing to adopt or reject balancing standard). But even those CIPA cases acknowledging a higher evidentiary threshold have stressed that the government's interest in protecting national security cannot override the defendant's right to a fair trial. *See Fernandez*, 913 F.2d at 154 (discussing United States v. Smith, 780 F.2d 1102 (4th Cir. 1985) (en banc)).

411 18 U.S.C. app. 3 § 4.

412 *Id.* § 6(c)(1).

413 *Id.* § 6(e)(1).

414 United States v. Collins, 720 F.2d 1195, 1201 (11th Cir. 1983).

charges, finding against the government on issues related to the classified information, and striking or precluding witness testimony.[415]

Assuming discovery is forthcoming, CIPA safeguards classified information through protective orders and security procedures. Upon motion by the government, section 3 requires the court to issue a protective order against disclosure of any classified information provided by the government to the defendant.[416] Pursuant to section 9, the Chief Justice of the Supreme Court prescribed rules to prevent the unauthorized disclosure of classified information in the custody of federal courts.[417] Under these rules, the courts appoint security officers who are responsible for facilities and handling of documents in cases involving classified matters. Among other things, a court may require the defense to review classified information in a secure room ("Sensitive Compartmented Information Facility" or SCIF), typically located in the courthouse. Other than judges, court personnel do not have access to classified materials without obtaining a security clearance from the executive branch.[418]

Section 8 concerns the actual introduction of classified information into evidence. Recognizing that "classification is an executive, not a judicial function,"[419] the section explicitly states that the introduction of classified information in court does not change its classification status.[420] Unless fairness requires otherwise, a court may admit into evidence only part of the writing, recording, or photograph in question, or it may admit the entire item with redactions of classified information.[421] Finally, section 8 allows the government to object to any question or line of inquiry that might result in the witness divulging classified information not previously determined to be admissible.[422] The court is then required to take appropriate action to

---

415 18 U.S.C. app. 3 § 6(e)(2). Under CIPA § 7, the government can take an interlocutory appeal from district court rulings authorizing disclosure of classified information, imposing sanctions for nondisclosure of such information, or denying protective orders. *See id.* § 7(a); *see also* United States v. Clegg, 740 F.2d 16, 18 (9th Cir. 1984) (holding that appellate court has jurisdiction over disclosure of classified information to the public). The appeal may occur before or during trial and regardless of whether the defendant has been placed in jeopardy. The issue must be reviewed on an expedited basis by the appellate court, which is authorized to dispense with written briefs by the parties and the issuance of a written opinion in rendering its judgment. *See* 18 U.S.C. app. 3 § 7(b).

416 18 U.S.C. app. 3 § 3 (2012).

417 *See* Security Procedures Established Pursuant to Public Law 96-456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information (1981) (available in notes following 18 U.S.C. app. 3 § 9).

418 *See* United States v. Smith, 899 F.2d 564, 567 (6th Cir. 1990).

419 S. REP. NO. 96-823, at 10 (1980).

420 *See* 18 U.S.C. app. 3 § 8(a).

421 *See id.* § 8(b).

422 *See id.* § 8(c).

determine whether the anticipated response can be admitted without jeopardizing classified information.[423]

To be sure, the CIPA process can present difficult questions. For instance, protective orders under CIPA may require defendants and their counsel to obtain security clearances from the government before being allowed to review classified information.[424] Invariably, accused spies and terrorists will be deemed ineligible for security clearance.[425] Defense counsel may also be ineligible for security clearance, or, on occasion, they may be unwilling to submit to a background check.[426] In these circumstances, courts have appointed counsel with the requisite security clearance to handle issues involving classified information. Cleared counsel may be prevented from revealing classified information to either uncleared counsel or the defendant.[427] Although this does generate troubling constitutional issues, the most important point for present purposes is that CIPA would envision access for some defense representative to investigate a claim of digital innocence. Even circumscribed access to data proving innocence is better than none.

Substitutions under CIPA raise important questions as well. In digital innocence cases, an agreeable substitution format may be relatively straightforward. In the hypothetical provided at the beginning of this section—a defendant who seeks cellphone call records as proof that he was not at the site of the robbery—it is easy to imagine that any exculpatory data could be provided in an appropriately redacted document or through an agreed-upon stipulation or summary. Other potential pieces of evidence may prove more difficult because they contain information that might reveal the sources and methods of

---

423 *See id.*

424 *See* United States v. Moussaoui, No. CR. 01-455-A, 2002 WL 1987964, at *1 (E.D. Va. Aug. 23, 2002) (noting prior protective order that "prohibits the defendant from accessing classified information unless he first obtains the necessary security clearance from the Department of Justice, or other governmental or Court approval"); United States v. Rezaq, 156 F.R.D. 514, 524 (D.D.C. 1994) (providing reasons why an accused terrorist "has never had, nor is ever likely to have, a security clearance"), *vacated in part*, 899 F. Supp. 697 (D.D.C. 1995); *see also* 28 C.F.R. § 17.41(b) (2013).

425 This requirement is not unique to the defense. Law clerks, secretaries, bailiffs, and other court staff may be required to undergo security clearances as well. *See, e.g.*, United States v. Smith, 899 F.2d 564, 567 (6th Cir. 1990). Indeed, judges hearing civil suits challenging the NSA's warrantless mass surveillance program were not allowed to possess the parties' filings but instead had to make appointments to review the documents. The judges were even directed to write their decisions on computers supplied by the Department of Justice. *See* Adam Liptak, *Secrecy at Issue in Suits Opposing Domestic Spying*, N.Y. TIMES, Jan. 26, 2007, at A1.

426 *See, e.g.*, United States v. Abdi, 498 F. Supp. 2d 1048, 1087 (S.D. Ohio 2007) (defense counsel unwilling to submit to background check); United States v. Al-Arian, 267 F. Supp. 2d 1258, 1266 (M.D. Fla. 2003) (same).

427 *See, e.g.*, *In re* Terrorist Bombings of U.S. Embassies in East Africa, 552 F.3d 93, 128 (2d Cir. 2008); United States v. Abu Ali, 528 F.3d 210, 253–54 (4th Cir. 2008).

government surveillance. For instance, the government's security interest in intercepted communications may rest "not so much in the contents of the conversations, as in the time, place, and nature of the government's ability to intercept the conversations at all."[428] At the same time, however, it may be necessary to place the data in context, attributing statements to their sources or phrasing them as quotations, to ensure that the trier of fact can give the information its full weight as evidence of innocence.[429] As the Supreme Court has said, "A syllogism is not a story, and a naked proposition in a courtroom may be no match for the robust evidence that would be used to prove it."[430]

The CIPA procedures have been understood as providing substantial latitude to protect both national security and basic constitutional rights. A substitution does not have to be of "precise, concrete equivalence," the House Report on CIPA emphasized, and the "fact that insignificant tactical advantages could accrue to the defendant by the use of the specific classified information should not preclude the court from ordering alternative disclosure."[431] Rather, as the Fourth Circuit has noted, the basic purpose of a CIPA substitution is "to place the defendant, as nearly as possible, in the position he would be in if the classified information . . . were available to him."[432] More generally, courts have many tools available to protect classified information disclosed to the defense as part of a digital innocence claim. When national security is at stake, documents containing classified information can be sealed;[433] gag orders can be placed on the parties;[434] pretrial hearings can be closed to the public;[435] witness identities can be protected by pseudonyms;[436] and even proceedings in open court can employ special procedures to prevent disclosure of government secrets.[437] Again, this Article does not advocate these procedures,

---

428 United States v. Yunis (*Yunis II*), 867 F.2d 617, 623 (D.C. Cir. 1989).

429 *See* United States v. Rezaq, 134 F.3d 1121, 1142 (D.C. Cir. 1998) (stating that placing facts in context should work to protect the interests of the defendant).

430 Old Chief v. United States, 519 U.S. 172, 189 (1997).

431 H.R. REP. NO. 96-1436, at 12–13 (1980).

432 United States v. Moussaoui, 382 F.3d 453, 477 (4th Cir. 2004).

433 *See, e.g.*, United States v. Aref, 533 F.3d 72, 77 (2d Cir. 2008) (describing court's denial and grant of motions under seal); United States v. Ressam, 221 F. Supp. 2d 1252, 1259 (W.D. Wash. 2002) (discussing statutory provisions that permit sealing of information sensitive to national security).

434 *See, e.g.*, United States v. Koubriti, 305 F. Supp. 2d 723, 728 (E.D. Mich. 2003) (issuing gag order); United States v. McVeigh, 931 F. Supp. 756, 757 (D. Colo. 1996) (describing gag order).

435 *See, e.g.*, United States v. Abu Marzook, 412 F. Supp. 2d 913, 915 (N.D. Ill. 2006) (granting government's motion to close hearing to the public).

436 *See, e.g.*, United States v. El-Mezain, 664 F.3d 467, 491 (5th Cir. 2011) (permitting use of pseudonyms for witnesses in certain cases).

437 *See, e.g.*, United States v. Zettl, 835 F.2d 1059, 1063 (4th Cir. 1987) (describing procedures used to avoid disclosing government secrets during proceedings in open court).

which raise important constitutional concerns (mostly for the defendant). Instead, it simply points out the various means by which judges can protect state secrets. Although the government may be worried about revealing its methods of surveillance, the federal courts have decades of experience protecting not just information but also the systems that generate such information.[438]

It is conceivable that digital innocence claims could face an entirely different challenge: the information sought from government-controlled Big Data is considered privileged but is not classified, and thus, it does not fit cleanly within CIPA. Nonetheless, courts retain the authority to analyze a government claim of privilege and the possibility of substitutions under procedures styled after CIPA. On a showing of "good cause," for instance, Rule 16 of the Federal Rules of Criminal Procedure allows a court to "deny, restrict, or defer discovery or inspection, or grant other appropriate relief."[439] According to the Advisory Committee's notes on Rule 16, the limitation was intended to ensure, among other things, "the protection of information vital to the national security," permitting the government to make the showing in camera when "matters of national security are involved."[440]

Similarly, a district court decision recognized a statutory privilege for the NSA under the National Security Agency Act,[441] which may be invoked to protect unclassified information.[442] The court went on to analyze the protected information under a CIPA-type process.[443] Another example comes from the prosecution of the aforementioned "20th Hijacker," Zacarias Moussaoui, who requested pretrial access to enemy combatants detained in Guantanamo Bay and their production as witnesses at trial. CIPA did not apply in this context, but both the district court and the Fourth Circuit relied upon the statutory provisions because CIPA provided "a useful framework" for whether the enemy combatant witnesses would be relevant and helpful to Moussaoui's defense and whether substitutions would be appropriate.[444]

---

438 *See* United States v. Lopez, 328 F. Supp. 1077, 1086 (E.D.N.Y. 1971) (describing efforts taken to prevent disclosure of sensitive programmatic information in a criminal case).

439 FED. R. CRIM. P. 16(d)(1).

440 *Id.* 16(e) and advisory committee's notes.

441 *See* National Security Agency Act of 1959, § 6(a), 50 U.S.C. § 3605 (2006 & Supp. V 2011) (stating that nothing in statute, with limited exceptions, should be construed to require disclosure from the NSA).

442 *See* United States v. Drake, No. RBD 10-181, 2011 WL 2175007, at *5 (D. Md. June 2, 2011) ("Section 6(a) . . . provides the NSA with a statutory privilege protecting against the disclosure of information relating to its activities . . . .").

443 *See id.* at *3–4 (beginning CIPA analysis).

444 *See* United States v. Moussaoui, 382 F.3d 453, 471 n.20 (4th Cir. 2004) (stating that even though CIPA does not apply, it still provides a useful framework for evaluating defendant access to enemy combatant witnesses); United States v. Moussaoui, 333 F.3d 509, 513 (4th Cir. 2003) (discussing the district court's application of the CIPA procedures).

There are constitutional limits to these and other procedures,[445] and consistent with our standing caveat, we do not necessarily endorse CIPA and CIPA-like approaches. In fact, we harbor some misgivings about these processes. Of particular concern here is a maneuver not required by law but one that has become a standard government practice: filing materials ex parte in response to defense discovery motions.[446] Under CIPA section 4, the court may authorize the government to make submissions to be reviewed by the court alone,[447] but nothing in the law's language or history suggests that ex parte filings are mandatory. To the contrary, section 4 was intended to clarify a court's authority under Rule 16 of the Federal Rules of Criminal Procedure[448]—which, in turn, explicitly rejected language that would have made ex parte filings a matter of right[449] and instead embodied the principle that "ex parte proceedings are disfavored and not to be encouraged."[450]

The vices of ex parte proceedings are well known, such as the tendency to undermine the appearance if not reality of fairness and impartiality in judicial decision making.[451] In an adversary system, the ability of counsel to participate in proceedings is necessary not merely to present the defense perspective but also to correct or contradict the information and reasoning forwarded by a partisan in the process (i.e., the prosecutor).[452] Ex parte proceedings carry an "enormous risk of error," such that "the very foundation of the adversary process

---

445 *See* Waller v. Georgia, 467 U.S. 39, 46 (1984) (a public trial is a guarantee provided by both the First and Sixth Amendments); United States v. Aref, 533 F.3d 72, 83 (2d Cir. 2008) (transparency in court judgments is essential to constitutional system of checks and balances); United States v. Abu Ali, 528 F.3d 210, 255 (4th Cir. 2008) (hiding evidence from the defendant, but giving it to the jury, is a violation of the Confrontation Clause).

446 *See* Joshua L. Dratel, *Section 4 of the Classified Information Procedures Act: The Growing Threat to the Adversary Process*, 53 WAYNE L. REV. 1041, 1042–47 (2007).

447 18 U.S.C. app. 3 § 4 (2012).

448 *See* S. REP. NO. 96-823, at 6 (1980).

449 *See* FED. R. CRIM. P. 16 advisory committee notes ("The Committee changed the [proposed] mandatory language to permissive language. A Court may, not must, conduct an ex parte proceeding if a party so requests.").

450 H.R. REP. NO. 94-247, at 16 (1975).

451 *See* United States v. Carmichael, 232 F.3d 510, 517 (6th Cir. 2000) ("[E]x parte communications with the court are an extraordinarily bad idea [particularly in criminal cases because] giving the government private access to the ear of the court is not only 'a gross breach of the appearance of justice,' but also a 'dangerous procedure.'" (quoting United States v. Minsky, 963 F.2d 870, 874 (6th Cir. 1992))); American-Arab Anti-Discrimination Comm. v. Reno, 70 F.3d 1045, 1069 (9th Cir. 1995) (noting that judges "are necessarily wary of one-sided process" and "fairness can rarely be obtained by secret, one-sided determination") (internal quotation marks omitted); Abourezk v. Reagan, 785 F.2d 1043, 1060–61 (D.C. Cir. 1986) (stating that party access to case evidence is a hallmark of American adjudication and "serves to preserve both the appearance and the reality of fairness in the adjudications of United States courts"); *see also* MODEL CODE OF JUDICIAL CONDUCT Canon 3(B)(7) (2004) (setting out a general rule against ex parte communications).

452 *See* United States v. Abuhamra, 389 F.3d 309, 322–23 (2d Cir. 2004).

assumes that use of undisclosed information will violate due process."[453] At the pretrial stage of discovery pursuant to CIPA section 4, the court alone does not have the basis to assess the veracity of the government's contentions, which is only exacerbated by the technical complexity of information relevant to a claim of digital innocence.[454] Nor can judges be expected to appreciate all the facts and issues that could impact defense claims of innocence. In rejecting ex parte review of electronic surveillance that may have been illegal, the Supreme Court once observed:

> An apparently innocent phrase, a chance remark, a reference to what appears to be a neutral person or event, the identity of a caller or the individual on the other end of a telephone, or even the manner of speaking or using words may have special significance to one who knows the more intimate facts of an accused's life. And yet that information may be wholly colorless and devoid of meaning to one less well acquainted with all relevant circumstances. . . . [T]he task is too complex, and the margin for error too great, to rely wholly on the *in camera* judgment of the trial court to identify [the relevant records] . . . .
>
> . . . .
>
> Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny [demanded].[455]

Even more problematic is relying upon the prosecution—the advocate for conviction—to make the case for exculpatory evidence.[456] Indeed, candid prosecutors will concede that they are not in a position to assess the materiality of information for the defense.[457] As discussed earlier, the government has a less-than-stellar track record of truthfulness when it comes to its mass surveillance programs,[458] and the law enforcement practice of "parallel construction" is nothing less

---

453 *American-Arab Anti-Discrimination Comm.*, 70 F.3d at 1069–70.

454 *See* United States v. Abu Marzook, 412 F. Supp. 2d 913, 921 (N.D. Ill. 2006) ("It is a matter of conjecture whether the court performs any real judicial function when it reviews classified documents . . . . Without the illumination provided by adversarial challenge and with no expertness in the field, . . . the court has no basis on which to test the accuracy of the government's claims." (quoting Stein v. Dep't of Justice, 662 F.2d 1245, 1254 (7th Cir. 1981) (internal quotation marks omitted))).

455 Alderman v. United States, 394 U.S. 165, 182–84 (1969).

456 *See* DiSimone v. Phillips, 461 F.3d 181, 195 (2d Cir. 2006) (stating that to allow the prosecution to assess the value of exculpatory information "would be to appoint the fox as henhouse guard").

457 *See Panel Discussion: Criminal Discovery in Practice*, 15 GA. ST. U. L. REV. 781, 785–86 (1999) (U.S. Attorney acknowledging the difficulty in "convincing my Assistant U.S. Attorneys that they often don't know what may be material to the defense").

458 *See supra* notes 285–91, 304–05 and accompanying text.

than a fraud on the court.[459] Most telling of all are the FISC opinions exposing the government's serial misrepresentations,[460] none of which resulted in the court stopping a mass surveillance program.[461] Such prevarications, and the spy court's failure to discipline the government for them, reinforce the argument against secret ex parte proceedings.

The incidents also help make the case for installing a civil liberties advocate in the FISC to argue against the government's position, which has been recommended by President Obama's blue-ribbon advisory committee[462] and endorsed by the President himself.[463] When the issue is discovery under CIPA section 4, however, the process already provides for an advocate in the form of security-cleared defense counsel. In *Daoud*, the government offered no meaningful response to the contention that national security interests are not implicated when defense counsel has the required security clearances, other than to say that it had never been done before.[464] "That response is unpersuasive where it is the government's claim of privilege to preserve national security that triggered this proceeding," the court opined, finding that "the probable value of disclosure and the risk of nondisclosure outweigh the potential danger of disclosure to cleared counsel."[465] Unless CIPA is a charade, security-cleared counsel should be allowed to participate in the discovery process in order to secure exculpatory evidence.

2. *Obtaining Information from Private Third Parties*

There is another way for the wrongfully accused and convicted to access Big Data. The government seeks the vast majority of its information from telecommunications firms and ISPs. These commercial enterprises maintain the comprehensive user records that feed programs like PRISM. So rather than seeking exculpatory evidence from the government, defendants could obtain this information directly

---

459 *See supra* notes 387–92 and accompanying text.

460 *See supra* note 306 and accompanying text.

461 *See* Jennifer S. Granick & Christopher J. Sprigman, *FISA Court Rolls Over, Plays Dead*, FORBES (Aug. 28, 2013, 10:50 AM), http://www.forbes.com/sites/jennifergranick/2013/08/28/fisa-court-rolls-over-plays-dead/.

462 *See* PRG REPORT, *supra* note 9, at 36, 203–05.

463 *See* Obama, *supra* note 12 ("To ensure that the court hears a broader range of privacy perspectives, I am also calling on Congress to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court.").

464 United States v. Daoud, No. 12-cr-723, 2014 WL 321384, at *2 (N.D. Ill. Jan. 29, 2014). As discussed earlier, the *Daoud* case involved the analogous situation of a FISA suppression motion in which the government sought to file materials ex parte and in camera. *See supra* notes 295–96 and accompanying text.

465 *Daoud*, 2014 WL 321384, at *2.

from third-party Internet intermediaries.[466] Although national security may not be a concern when pursuing information from ISPs, defendants still must overcome restrictions and hurdles to access the data.

As a starting point, defendants may be able to access social media data merely by examining what is publicly available. Social media is built on widespread sharing. Consider a Facebook wall: the account of the wall owner not only contains information on the user but also information regarding any of the other social network users who have permitted their content to be published to friends. Access to any one of a number of accounts will yield the information. Defense attorneys must be cautious to abide by ethical guidelines barring the use of deception in seeking social media connections that might reveal such information (such as deceptively seeking "friend" status on Facebook to obtain semi-private information), but broad-based sophisticated searches of publicly available information do not normally raise such concerns.[467]

As for nonpublic or formerly public information, criminal defendants usually seek relevant materials through a subpoena.[468] Onerous or oppressive subpoenas can be quashed or limited, but the advent of fast software forensic tools means that producing even quite large amounts of data is not presumptively burdensome.[469] Once a party has received a subpoena, the party must comply, move to quash, or face a motion to compel and the possibility of being held in contempt of court.[470]

Silicon Valley firms uniformly, and usually successfully, resist such subpoenas pursuant to the Stored Communications Act (SCA), codified at 18 U.S.C. §§ 2702 and 2703. These provisions, which are part of the larger Electronic Communications Protection Act, regulate the ability of Internet intermediaries to release the contents of stored electronic communications. The SCA is based on the technological balance between client and server that existed at the time of the law's passage, when users generally downloaded information from e-mail servers and accessed it locally.[471] More than a quarter-century later, this structure is not only outdated, it has been completely reversed as

466 *See* Zwillinger & Genetski, *supra* note 42, at 585 (stating that certain exceptions permit a criminal defendant to obtain his own messages or messages intended for him).

467 *See* Shirin Chahal, Note, *Balancing the Scales of Justice: Undercover Investigations on Social Networking Sites*, 9 J. TELECOMM. & HIGH TECH. L. 285, 306 (2011) (detailing ethical restrictions on defense use of deception to gain access to social media information).

468 FED. R. CRIM. P. 17(c).

469 *See id.*

470 *See id.*

471 *See* Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1396–97 (2004).

a result of cloud computing that permits more secure access of content on more devices. Today, the SCA's presumption—that content left on the server is unimportant or abandoned—is incorrect.

Because of this basic technological change, the balance struck by the SCA between account holders and the government now produces a variety of unintended consequences, including its largely underexplored impact on the ability of civil parties and criminal defendants to access information that has migrated from filing cabinets to file servers.[472] While the SCA enumerates provisions for disclosure of this information to government entities, it is silent on access by criminal defendants and civil litigants. Courts have read this silence as prohibiting access by these parties,[473] and yet the underlying obligation to comply with a subpoena remains. This lack of clarity has caused confusion and excess litigation when defendants seek information to which they have a constitutional right in order to prepare their case, with ISPs resisting on the ground that the disclosure of communications content is unlawful.[474]

Section 2702 prohibits Internet intermediaries from releasing the contents of stored electronic communications,[475] where an "electronic communication" is defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electronic or photo-optical system that affects interstate or foreign commerce."[476] Intermediaries are divided into two now-archaic classes based on what they do with electronic communications. An "electronic communication service" is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications," while a "remote computing service" is one that engages in the "provision to the public of computer storage or processing services by means of an electronic communications system."[477] Although the advance of cloud computing and the general progress of technology have rendered these categories largely obsolete, the distinction has real differences for the means by which the content may be obtained.[478]

---

472 *See* Zwillinger & Genetski, *supra* note 42, at 579–81 (stating that the SCA is broad enough to include e-mails stored on ISP servers that are not in temporary storage).

473 *See id.* at 580 (discussing Theofel v. Farey-Jones, 359 F.3d 1066 (9th Cir. 2004)).

474 *See id.* (detailing the need for a search warrant to access stored communications).

475 *See* 18 U.S.C. § 2702(a) (2012); *see also Theofel*, 359 F.3d at 1076–77 (interpreting section 2702(a)).

476 *See* 18 U.S.C. § 2510(12).

477 *Id.* §§ 2510(15), 2711(2).

478 *See* Zwillinger & Genetski, *supra* note 42, at 581 n.62 ("The distinction between materials in 'electronic storage,' and materials that may just be stored electronically is crucial.").

There are limited exceptions to the prohibition on disclosing content to private parties. Of interest to criminal defendants are two exceptions contained within section 2702, which permit disclosure of the contents of communication to "an addressee or intended recipient of such communication" or "with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service."[479] Section 2702 also references non-content in the form of customer records and other subscriber information.[480] Although Internet intermediaries are barred under this provision from providing any "record or other information pertaining to a subscriber to or customer of such service . . . to any governmental entity,"[481] records or information "not including the contents of communications"[482] may be provided "to any person other than a governmental entity."[483]

Government entities may access both content and non-content information pursuant to the mandatory disclosure provisions of section 2703. Obtaining the content of communications stored for less than 180 days requires a warrant,[484] while a subpoena will suffice for content stored for a longer period of time.[485] As a consequence, procuring records and information (although not content) may be simpler for a nongovernment entity through section 2702 than it is for a government entity through section 2703. Obtaining content is very difficult for nongovernment entities, however, with the only clear path being the consent of the originator, addressee, recipient, or subscriber.[486]

With respect to Big Data, the SCA's rules have interesting interactions with new forms of storing and accessing data. The SCA does not prohibit the release to a defendant of information about him or herself, including content information.[487] Given Big Data tracking, this can be a treasure trove of material for the defense. Consider, for example, the data collected about a user for the purposes of targeted advertising. As discussed earlier, most users' physical location or location-based IP address are constantly tracked by advertisers. That infor-

---

479 18 U.S.C. § 2702(b)(1), (3).

480 *See id.* § 2702(a)(3).

481 *Id.*

482 *Id.*

483 *Id.* § 2702(c)(6).

484 *Id.* § 2703(a).

485 *Id.* § 2703(b)(1)(B).

486 *See* Zwillinger & Genetski, *supra* note 42, at 585 ("Even a close examination of all three of the provisions cited in this exception reveals no pathway for anyone other than a government entity to compel disclosures of contents of customer communications.").

487 *See* 18 U.S.C. § 2702(b)(1), (b)(3), (c)(2); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 972 n.16 (C.D. Cal. 2010) (describing when an electronic communication service (ECS) provider may divulge the contents of a communication).

mation can serve as a comprehensive record of where the defendant was on a particular day and time. Companies may still object, of course, but they will be unlikely to prevail in such straightforward requests for production. When Yahoo refused to provide a defendant with the contents of his own e-mail accounts, for instance, the court noted that a motion to compel production from Yahoo would be the next best step to obtain the data.[488]

More difficult will be attempts to obtain content information that does not fall under the defendant's own consent exceptions in section 2702. The antiquated SCA framework contemplates that parties will seek disclosure directly from senders or recipients rather than from an ISP.[489] Under this framework, the defendant could locate the relevant originator or recipient by accessing non-content identifying information, such as an IP address, and then seek production directly.[490] Changes in technology make this problematic, however. Even the originator or recipient may no longer have a deleted text message or may not remember a password to an old social media account. Moreover, much cloud data only barely touches the local computer. For instance, Facebook accounts are not stored on a user's hard drive.

Although courts have avoided the question of whether the SCA's lack of an exception for a criminal defendant would impermissibly impact his confrontation and compulsory process rights, there has been a more robust discussion of the pure statutory issue in civil cases. Courts agree that the SCA creates no exception for civil subpoenas directed at third-party ISPs or social networks. Based on the seminal case of *Crispin v. Christian Audigier, Inc.*, a consensus has evolved that the statute does not inherently permit an exception for response to a court subpoena.[491] But where such an exception does exist—most notably, the "lawful consent" exception—courts have been willing to

---

488 *See* United States v. Amawi, 552 F. Supp. 2d 679, 680 (N.D. Ohio 2008) ("[M]oving to compel disclosure from the providers directly does seem to be the more appropriate . . . route for the defendant to take.").

489 *See, e.g.*, O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 88–89 (Cal. Ct. App. 2006) (stating that prohibition of discovery from ISPs imposes no new burdens on litigants and encourages the development of digital communications); Facebook, Inc. v. Aguayo-Gomez, No. A13-0579 (Minn. Ct. App. May 1, 2013) (granting writ of prohibition stopping district court's order to compel disclosure by Facebook).

490 *See, e.g.*, *Amawi*, 552 F. Supp. 2d at 680.

491 717 F. Supp. 2d at 975; *see* Mintz v. Mark Bartelstein & Assocs., Inc., 885 F. Supp. 2d 987, 991 (C.D. Cal. 2012); Flagg v. City of Detroit, 252 F.R.D. 346, 350 (E.D. Mich. 2008) ("[A]s noted by the courts and commentators alike, § 2702 lacks any language that explicitly authorizes a service provider to divulge the contents of a communication pursuant to a subpoena or court order."); Viacom Int'l Inc. v. Youtube Inc., 253 F.R.D. 256, 264 (S.D.N.Y. 2008); *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008); *O'Grady*, 44 Cal. Rptr. 3d at 89.

craft relief that satisfies the SCA and makes sure that parties receive discovery to which they are entitled.[492]

In civil cases, parties often seek the communications, records, or social media information of the opposing party.[493] Discovery of this sort of information has become routine, with the request directed at the opposing party rather than at the service provider.[494] For discovery purposes, the information is deemed to be in the control of the party required to produce it.[495] So, for example, plaintiffs whose social media posts contradict their personal injury claims are usually required to consent to the social network provider's disclosure of account information and posts.[496]

Courts make sure that such social network access is not a mere fishing expedition by, for instance, restricting access and discovery by time or by subject.[497] But they do order plaintiffs to consent to the access if there is a basis for the request.[498] As noted by the court in

---

492 *See, e.g.*, Juror No. One v. Superior Court, 142 Cal. Rptr. 3d 151, 156 (Cal. Ct. App. 2012) ("One exception is recognized where the customer or subscriber has given consent to the disclosure."); *see also* 18 U.S.C. § 2702(b)(3) ("A provider . . . may divulge the contents of a communication . . . with the lawful consent of the originator or an addressee or intended recipient of such communication . . . .").

493 *See* Offenback v. L.M. Bowman, Inc., No. 1:10-CV-1789, 2011 WL 2491371 (M.D. Pa. June 22, 2011); Levine v. Culligan of Florida, Inc., No. 50-2011-CA-010339-XXXXXMB, 2013 WL 1100404, at *3 (Fla. Cir. Ct. Jan. 29, 2013) ("Similarly, courts seem to be in agreement that the [SCA] prohibits records from being subpoenaed directly from Facebook and other social networking sites. However, in Florida, in certain circumstances, courts may require a plaintiff to provide a signed authorization for the production of relevant social media discovery to allow an opposing party to obtain those records directly." (citations omitted)); EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 434 (S.D. Ind. 2010); Romano v. Steelcase Inc., 907 N.Y.S.2d 650, 657 (Sup. Ct. 2010); Zimmerman v. Weis Markets, Inc., No. CV-09-1535, 2011 WL 2065410 (Pa. Ct. Com. Pl. May 19, 2011); McMillen v. Hummingbird Speedway, Inc., No. 113-2010 CD, 2010 WL 4403285 (Pa. Ct. Com. Pl. Sept. 9, 2010).

494 *See, e.g.*, *Romano*, 907 N.Y.S.2d at 651; Largent v. Reed, No. 2009-1823, 2011 WL 5632688, at *11 (Pa. Ct. Com. Pl. Nov. 8, 2011) ("*Crispin* is distinguishable. In that case, the defendants sought information via subpoena to Facebook and other social networking sites. In this case, [defendant] seeks the information directly from [plaintiff]."); *Zimmerman*, 2011 WL 2065410; *McMillen*, 2010 WL 4403285.

495 *See supra* note 494.

496 *See supra* notes 491–93 and accompanying text.

497 *See, e.g.*, Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387 (E.D. Mich. 2012) (rejecting social media discovery request as overbroad); *Levine*, 2013 WL 1100404, at *4 (refusing access to Facebook information where defendant "failed to establish a factual predicate with respect to the relevance [*sic*] of the evidence" and finding that the defendant "essentially sought permission to conduct 'a fishing expedition' into plaintiff's Facebook account based on the mere hope of finding relevant evidence" (quoting McCann v. Harleysville Ins. Co. of New York, 910 N.Y.S.2d 614 (App. Div. 2010)) (internal quotation marks omitted)); *see also* Winchell v. Lopiccolo, 954 N.Y.S.2d 421, 424 (Sup. Ct. 2012) (finding defendant's request for unrestricted access to social media accounts was overbroad).

498 *See* Flagg v. City of Detroit, 252 F.R.D. 346, 363 (E.D. Mich. 2008) ("[I]t is not an 'oxymoron' to conclude, under the particular circumstances presented here, that a party may be compelled to give its consent. It is a necessary and routine incident of the rules of discovery that a court may order disclosures that a party would prefer not to

O'Grady v. Superior Court, "[w]here a party to the communication is also a party to the litigation, it would seem within the power of a court to require his consent to disclosure on pain of discovery sanctions."[499] Under the cases lies a broad streak of rough fairness: when a personal injury plaintiff brings allegations that may be disproved by evidence over which she exercises some control via her consent to disclosure, the plaintiff must exercise this power to make the evidence available to the other party. The upshot is that while the SCA is held to bar direct subpoenas to service providers, the problem is vastly ameliorated in practice.

This solution seems readily applicable to claims of digital innocence. If the government chooses to prosecute, it is obliged to provide access to information not only within its immediate possession but also within its reach. This argument carries even greater force in criminal prosecutions. Criminal cases implicate strong constitutional interests vindicated by providing a reasonable process for accessing potentially exonerating evidence. Moreover, prosecutors bear a higher burden of accuracy and care than do civil plaintiffs. While tort and contract litigants are free to be as partisan as the rules of civil procedure and ethics allow, prosecutors have a special obligation to support the truth-seeking functions of the court and a "duty to refrain from improper methods calculated to produce a wrongful conviction."[500]

The law in this area is developing rapidly, and the decisions are often unpublished because they relate to discovery disputes in cases that often settle. Nonetheless, there appears to be movement on this front toward ordering access. In *Juror Number One v. Superior Court*, a California appellate court upheld a trial judge's order requiring a juror to consent to defense counsel's access of his Facebook profile.[501] The court referenced the SCA bar, the lawful consent exception, and the judicial authority to order consent for purposes of discovery.[502]

---

make. . . . [T]his power of compulsion encompasses such measures as are necessary to secure a party's compliance with its discovery obligations. In this case, the particular device that the SCA calls for is 'consent,' and [d]efendant . . . has not cited any authority for the proposition that a court lacks the power to ensure that this necessary authorization is forthcoming from a party with the means to provide it. Were it otherwise, a party could readily avoid its discovery obligations by warehousing its documents with a third party under strict instructions to release them only with the party's 'consent.'").

499 O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 88 (Cal. Ct. App. 2006); *see also In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 613 n.5 (E.D. Va. 2008) (detailing discovery options that would avoid discovery sanctions).

500 Berger v. United States, 295 U.S. 78, 88 (1935).

501 *See* 142 Cal. Rptr. 3d 151, 153 (Cal. Ct. App. 2012).

502 *See id.* at 155–56 ("[T]he SCA creates a set of Fourth Amendment-like protections that limit both the government's ability to compel ISP's to disclose customer information and the ISP's ability to voluntarily disclose it. . . . One exception is recognized where the customer or subscriber has given consent to the disclosure.").

Moreover, it noted the reasoning in *O'Grady* and other cases that a judge's "power of compulsion encompasses such measures as are necessary to secure a party's compliance with its discovery obligations. In this case, the particular device that the SCA calls for is 'consent' . . . ."[503] Although the order in *Juror Number One* focused on a juror, the reasoning of *O'Grady* is not so constrained and has been instrumental in persuading other courts to direct discovery requests to the person in control of the information.

Unsurprisingly, Facebook has subsequently received discovery orders in criminal cases based on the precedent of *Juror Number One*. In a 2013 case, for instance, the trial court "require[d] Facebook to disclose the content of an alleged crime victim's Facebook communications" in response to a defense subpoena.[504] Upon receiving Facebook's response, the trial court asked the defendant to respond to the claim that the information would be available by way of an order directed to the alleged crime victim—precisely the path described above.[505] The defendant withdrew the subpoena, mooting the request, and the court denied Facebook's request to adjudicate the question.[506]

There are some additional wrinkles as these discovery disputes unfold. Perhaps anticipating the success of court-ordered consent in the criminal context, Facebook has begun asserting that section 2702, which references voluntary disclosure, nonetheless permits the company to refuse access even if it has received "lawful consent."[507] Such an approach would permit Internet intermediaries to refuse disclosure, in the face of lawful consent and a court order, to the point that it could deny access to a defendant's own data even if the information could prove her innocence. Needless to say, this construction goes far beyond any legally viable purpose of the statute.

The line of reasoning also ignores the structure of the statute, which bars an ISP from producing the information sought only if there is no exception. Lawful consent is just such an exception.

---

503 *See id.* at 158 (quoting *Flagg*, 252 F.R.D. at 363).

504 *See* Application for Leave to File Amicus Curiae Brief and Amicus Curiae Brief of Electronic Frontier Foundation in Support of Plaintiff and Petitioner Facebook, Inc. at 2, Facebook, Inc. v. Superior Court, No. B248609, 2013 WL 2391432, at *1 (Cal. Ct. App. May 28, 2013).

505 *See id.*

506 *See id.*

507 *See* Facebook, Inc.'s Motion to Quash Subpoena in a Civil Case at 7, *In re* Facebook, Inc., 923 F. Supp. 2d 1204 (N.D. Cal. 2012) (No. C 12–80171 LHK (PSG)); *see also In re* Facebook, Inc., 923 F. Supp. 2d 1204, 1206 (N.D. Cal. 2012) (quashing subpoena and noting, "Nor is the court persuaded that Applicants' consent on Sahar's behalf distinguishes these precedents so as to justify compelling production. Under the plain language of Section 2702, while consent may *permit* production by a provider, it may not *require* such a production.").

Issuing a subpoena directly to a provider is entirely consistent with the SCA, which does not prevent the provider from performing its legal duties once lawful consent for disclosure has been obtained. Conversely, allowing Internet intermediaries to refuse to produce data even when they have received consent would upset the fragile balance achieved in the civil context, where the SCA has been left intact largely because direct discovery is possible. What is more, this would permit the precise outcome that concerned the *O'Grady* court: parties immunizing themselves from discovery merely by using cloud storage from a service that refuses to disclose. In the long run, this cannot, and will not, be the interpretation adopted by courts.

Another emerging path to the content of communications is through the terms of the Internet intermediaries' own license agreements or terms of service. Almost all software "End User License Agreements" and website "Terms of Use" include provisions allowing for disclosure of content information and subscriber information.[508] As a result of their careful drafting, Internet intermediaries may have built "lawful consent" to disclose into many online agreements. This question was raised by the court in *Juror Number One*, which noted that "we have no information as to the terms of any agreement between Facebook and Juror Number One that might provide for a waiver of privacy rights in exchange for free social networking services."[509] But given that Facebook's Mark Zuckerberg views privacy as dead,[510] it should be unsurprising that the company's "Data Use Policy" seems to vitiate significantly any privacy interests and includes an express provision for consent to disclose information.[511]

Another path to content data may be through Internet intermediaries' own advertising ecosystems. The SCA's prohibition on disclosure by a remote computing services (RCS) states that:

> a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of

---

508 *See* Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717, 729–30 (2013) (giving examples of popular services with such EULAs).

509 *See* Juror No. One v. Superior Court, 142 Cal. Rptr. 3d 151, 158 (Cal. Ct. App. 2012).

510 *See* Bobbie Johnson, *Privacy No Longer a Social Norm, Says Facebook Founder*, THE GUARDIAN (Jan. 10, 2010, 8:58 PM), http://www.theguardian.com/technology/2010/jan/11/facebook-privacy.

511 *See Data Use Policy*, FACEBOOK, https://www.facebook.com/full_data_use_policy (last modified Nov. 15, 2013) ("We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so."). The policy is phrased in terms of Facebook's own belief as to whether it is obligated to comply—that is, it may disclose if it believes it may disclose—which may mean that its obligation to disclose under the lawful consent obtained in its terms of service may rest on its own beliefs about whether it may disclose. Whether courts will accept such a circular argument remains to be seen.

> any communication which is carried or maintained on that service . . . solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.[512]

Unlike electronic communication service (ECS) providers, RCS providers are defined by the fact that they offer services beyond transitory electronic communications to the public.[513] Many popular Internet sites are RCS providers.[514] For example, Google has created an entire online ecosystem of services that go beyond mere transmission of e-mail, and yet many of these services are likely not covered by the RCS restrictions. Google (and many other free e-mail providers) scan e-mails for purposes of targeted advertising, with statements to this effect included in the company's terms of service and privacy policies.[515] As such, much of the information stored with Google is not "solely for the purpose of providing storage or computer processing services," and in addition, Google is "authorized to access the contents of . . . communications for purposes of providing . . . services other than storage and computer processing."[516] As noted by the court in *Juror Number One*, "if the service *is* authorized to access the customer's information for other purposes, such as to provide targeted advertising, SCA protection may be lost."[517]

On this statutory reading, the prohibition of section 2702, which is the bedrock of the SCA, would apply to nearly no cases of cloud data. The ECS prohibition would only apply to content in "electronic storage," which is "temporary, intermediate storage . . . incidental to . . . electronic transmission" or storage "for purposes of backup protection."[518] The courts have interpreted this expansively, however. In determining whether Facebook wall postings and comments were recoverable with a civil subpoena, the *Crispin* court held that "Facebook and MySpace are ECS providers as respects wall postings and comments and that such communications are in electronic stor-

---

512 18 U.S.C. § 2702(a)(2)(B) (2012).

513 *See id.* § 2711(2).

514 *See* Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256 (S.D.N.Y. 2008).

515 *See* 18 U.S.C. § 2702(a)(2)(B).

516 *Id. Compare Google Privacy Policy*, GOOGLE, http://www.google.com/intl/en/policies/privacy/ (last modified June 24, 2013), *and Google Terms of Service*, GOOGLE (Mar. 1, 2012), http://www.google.com/intl/en/policies/terms/ (last modified March 1, 2012), *with* 18 U.S.C. § 2702(a)(2).

517 Juror No. One v. Superior Court, 142 Cal. Rptr. 3d 151, 156 (Cal. Ct. App. 2012); *see also* William J. Robison, Note, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1212–14 (2010) (explaining that cloud computing may not be protected under the SCA or the RCS because of the use of information for targeted advertising).

518 *See* 18 U.S.C. § 2510(17).

age."[519] For this reason, a number of cases have held that there is no implied exception in the SCA for discovery subpoenas under the Federal Rules of Civil Procedure.[520]

But in criminal cases, the constitutional dimension of a defendant's right to present a defense affects the function of a subpoena issued pursuant to Rule 17 of the Federal Rules of Criminal Procedure. In interpreting the role of subpoenas under the SCA, one court differentiated between civil discovery and constitutional criminal procedure: "Rule 17 is not a discovery device, but rather a vehicle by which to obtain compulsory process."[521] In all likelihood, a defendant denied access to data held by Internet intermediaries might be able to claim a violation of several defense rights.[522] Responding to this tension, "some trial courts in California have issued bench orders and oral rulings finding that the restrictions . . . threaten to interfere with the defendant's constitutional rights to due process and effective assistance of counsel."[523]

The SCA's permissions are much more lenient for non-content data, including metadata, which is significant because, in many ways, Big Data is more about metadata than content. Data about communications—the location of the person sending a communication, the IP address accessed, login time, amount of traffic, type of traffic, and so on—can tell a powerful story. Disclosure of non-content data to nongovernment entities is not barred by the SCA, and, in fact, it is the one category of data that is easier to obtain by private parties than it is by government entities.[524] The ISPs have written exceptions for themselves in their user agreements and privacy policies that permit them to disclose subscriber information in response to a subpoena. In fact, metadata disclosure has become almost routine in other areas of the law. Consider, for example, the cases in which the recording industry regularly and successfully used subpoenas to discover the IP addresses and, in many cases, the identities of peer-to-peer file sharers.[525] This information is stock non-content information about a subscriber

---

519 *See* Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989 (C.D. Cal. 2010).

520 *See* Mintz v. Mark Bartelstein & Assocs., Inc., 885 F. Supp. 2d 987, 991 (C.D. Cal. 2012); *Crispin*, 717 F. Supp. 2d at 975; Flagg v. City of Detroit, 252 F.R.D. 346, 350 (E.D. Mich. 2008); *In re* Subpoena Duces Tecum to AOL, LLC, 550 F. Supp. 2d 606, 611 (E.D. Va. 2008); O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72, 89 (Cal. Ct. App. 2006).

521 *See* FTC v. Netscape Commc'ns Corp., 196 F.R.D. 559, 561 (N.D. Cal. 2000) (citing United States v. Nixon, 418 U.S. 683, 698–99 (1974)).

522 *See* Zwillinger & Genetski, *supra* note 42, at 595–96 (citing Coleman v. Alabama, 399 U.S. 1, 9 (1970); Pennsylvania v. Ritchie, 480 U.S. 39, 40, 56 (1987)).

523 *Electronic Communications Privacy Act and the Revolution in Cloud Computing: Hearing Before the Subcomm. on the Constitution, Civil Rights & Civil Liberties of the H. Comm. on the Judiciary*, 111th Cong. 7 (2010) (statement of Marc J. Zwillinger), *available at* http://scholarship.law.georgetown.edu/cong/109.

524 *See* 18 U.S.C. § 2702(c)(6) (2012).

525 *See, e.g.*, Interscope Records v. Does, 558 F. Supp. 2d 1176, 1179–80 (D. Kan. 2008).

under the SCA but was readily available by subpoena. Moreover, compliance with a subpoena is hardly burdensome, given that most companies have set up a regular path and fee structure. All one needs to do is serve the subpoena on the company's custodian of records and pay the fee, and the company provides the information.

3. *Obtaining Information from the United States as a Third Party*

A more onerous and convoluted process may apply when state criminal defendants seek information from the federal government. To be sure, officials such as FBI agents often cooperate with state requests for information or witness testimony. If the federal government proves recalcitrant, however, the seemingly proper approach would be for the defense to serve a subpoena on the relevant federal agency. Although the issue is "infrequently presented," it turns out to be "a difficult and important one."[526] A federal judge formulated the question as follows: "How, if at all, may a defendant in a state criminal prosecution obtain from unconsenting federal officials . . . information in their custody that may be material and favorable to his state-court defense?"[527]

Pursuant to the so-called "housekeeping statute," Congress has authorized federal agencies to manage themselves by promulgating regulations, including those for "the custody, use, and preservation of its records, papers, and property."[528] For present purposes, the regulations governing the Justice Department, and thus the FBI, provide an apposite example.[529] When a defendant makes a state court–backed demand for information possessed by federal law enforcement, the served employee cannot provide that material without notifying the U.S. Attorney for the district in which the issuing court is located, and then receiving the approval of the "responsible official"—that is, the U.S. Attorney and/or a high-ranking Justice Department official.[530] In turn, the responsible official must contact the "originating component," such as the head of the FBI field office where the information was gathered.[531] In the interim, the responsible official may engage in negotiations with the state court, prosecutor, and defendant prior to any decision—and if necessary, file legal motions—all intended to limit the demand for information.[532]

---

526 Smith v. Cromer, 159 F.3d 875, 883 (4th Cir. 1998) (Phillips, J., dissenting).

527 *Id.* (citation omitted).

528 5 U.S.C. § 301 (2012). Most federal agencies have created such regulations. *See, e.g.*, 10 C.F.R. §§ 202.21–202.26 (2013) (regulations for the Department of Energy).

529 *See* 28 C.F.R. §§ 16.21–16.29 (2013).

530 *See id.* §§ 16.22, 16.24.

531 *See id.* § 16.24(a).

532 *See id.* § 16.24(c).

Ultimately, the responsible official may only authorize the production of the requested material if the originating component has no objection and the disclosure would be appropriate under the procedural rules governing the underlying case and the relevant law concerning government privileges.[533] Among other things, the disclosure must not violate a specific regulation or statute (e.g., grand jury secrecy); it must not impair the effectiveness of investigative techniques and procedures; and, of particular concern, it must not reveal classified information.[534] In theory, the Deputy or Associate Attorney General could permit disclosure of information revealing a confidential source or investigative techniques and procedures if he or she "determines that the administration of justice requires disclosure."[535] But he or she "will not approve disclosure" if it would reveal classified information.[536]

These daunting procedures may seem unlikely to produce information helpful to a digital innocence claim. Sometimes a less formal process might provide a bit of relief; in one case, for instance, a federal prosecutor responded to a state subpoena by relating that "the FBI would be willing to sign a stipulation declaring that they have no responsive documents."[537] In practice, however, state subpoenas to federal agencies may follow an almost standard course leading to denial: After deciding not to produce the information, an agency official will move to quash the subpoena in state court. If the state court denies the motion, the agency will invoke a federal statute to remove the case to U.S. district court,[538] where the agency will once again move to quash the subpoena based on the doctrine of sovereign immunity and the Supremacy Clause of the U.S. Constitution.[539] The federal court will then quash the state subpoena pursuant to, inter alia, the Supreme Court's decision in *United States ex rel. Touhy v. Ragen*,[540] which has been interpreted as precluding state court jurisdiction to proceed against a federal employee (i.e., to hold him in

533 *See id.* §§ 16.24(b)(1)–(2), 16.26(a).

534 *See id.* §§ 16.24(b)(3), 16.26(b).

535 *See id.* § 16.26(c). In making such a decision, the official must take into consideration: "(1) [t]he seriousness of the violation or crime involved, (2) [t]he past history or criminal record of the violator or accused, (3) [t]he importance of the relief sought, [and] (4) [t]he importance of the legal issues presented." *Id.*

536 *Id.*

537 FBI v. Superior Court, 507 F. Supp. 2d 1082, 1086 (N.D. Cal. 2007).

538 *See* 28 U.S.C. § 1442(a)(1) (2012); *see also* Willingham v. Morgan, 395 U.S. 402, 405, 407 (1969) (holding that federal officers and the federal government can require a federal forum to justify a wider reading of § 1442).

539 *See, e.g.*, Boron Oil Co. v. Downie, 873 F.2d 67, 69 (4th Cir. 1989).

540 340 U.S. 462 (1951).

contempt) when he is acting in accordance with agency regulations.[541]

This understanding is flawed, and the exculpatory power of digital information could provide opportune moments to correct a jurisprudential misstep. To begin with, the housekeeping statute was intended to be just that—an explicit call for an agency to keep its house in order, so to speak. The original housekeeping statute was only supposed to "help General Washington get his administration underway by spelling out the authority for executive officials to set up offices and file Government documents."[542] When agencies began citing the housekeeping statute as authority to withhold information from the public, federal lawmakers balked at the statute being "twisted from its original purpose" and misinterpreted to "let every file clerk become a censor," a result that "would have aroused Madison, Jefferson, Mason, and the rest of the statesmen who put so much trust in popular rights to information."[543] The current housekeeping statute was intended "to correct that situation,"[544] as evidenced by the statute's last sentence: "This section does not authorize withholding information from the public or limiting the availability of records to the public."[545] Nothing in the legislative history or text suggests that the statute provides substantive grounds for a federal agency to withhold information from the public,[546] let alone a criminal defendant attempting to prove his innocence.

The lower court interpretation of *Touhy* is also problematic. In that case, the Supreme Court decided a narrow question—whether an agency head could deny his subordinates the authority to produce documents in response to a subpoena. In ruling that the Attorney General could withhold such power from lower-ranked officials, the *Touhy* Court explicitly refused to consider a far broader issue of constitutional dimension. "We find it unnecessary . . . to consider the ultimate reach of the authority of the Attorney General to refuse to produce at a court's order the government papers in his possession,"[547] said Justice Stanley Reed in his majority opinion. "The constitutionality of the Attorney General's exercise of a determinative

---

541 *See, e.g.*, Kasi v. Angelone, 300 F.3d 487, 504–06 (4th Cir. 2002); United States v. Williams, 170 F.3d 431, 433 (4th Cir. 1999); Smith v. Cromer, 159 F.3d 875, 878–81 (4th Cir. 1998); Louisiana v. Sparks, 978 F.2d 226, 236 (5th Cir. 1992); *FBI v. Superior Court*, 507 F. Supp. 2d at 1092–95.

542 H.R. REP. NO. 85-1461, at 1 (1958).

543 *Id.* at 2.

544 *Id.*

545 5 U.S.C. § 301 (2012).

546 *See, e.g.*, Chrysler Corp. v. Brown, 441 U.S. 281, 310 (1979); United States *ex rel.* O'Keefe v. McDonnell Douglas Corp., 132 F.3d 1252, 1255–56 (8th Cir. 1998); United States v. Henson, 123 F.3d 1226, 1237 (9th Cir. 1997).

547 United States *ex rel.* Touhy v. Ragen, 340 U.S. 462, 467 (1951).

power as to whether or on what conditions or subject to what disadvantages to the Government he may refuse to produce government papers under his charge must await a factual situation that requires a ruling."[548] Justice Felix Frankfurter's concurrence took up this precise point, emphasizing that "the decision and opinion in this case cannot afford a basis for a future suggestion that the Attorney General can forbid every subordinate who is capable of being served by process from producing relevant documents."[549]

As such, neither the housekeeping statute nor *Touhy* provides federal agencies immunity from, or a substantive privilege against, state judicial processes. This does not mean that an agency cannot argue sovereign immunity or invoke an executive privilege when confronted with a subpoena from a state criminal court. Rather, those claims must meet the doctrinal criteria of the relevant substantive law. Subpoenas from state courts are barred by sovereign immunity unless a federal official's withholding of information is unconstitutional or otherwise beyond his legal authority.[550] In turn, whether or not the official's actions are unconstitutional or ultra vires requires a judicial assessment of the information in question and the asserted right to such information, namely, the defendant's "constitutionally guaranteed access to evidence"[551] under the Fifth and Sixth Amendments.

In *Smith v. Cromer*,[552] perhaps the leading case on state criminal court subpoenas of federal officials, the U.S. district court acknowledged that the state defendant's compulsory process rights were at stake and then balanced those rights against a federal agency's interest in protecting its employees from being subpoenaed by state courts.[553] The Fourth Circuit affirmed the district court's assessment of constitutional rights versus governmental interests and its conclusion that the defendant had made an insufficient showing through "unrelated allegations."[554] Quoting a prominent CIPA case, the *Cromer* court noted that the defendant was required to "come forward with something more than speculation as to the usefulness of [the] disclosure."[555]

Implicit within these words is a judicial obligation: when a state criminal defendant makes a sufficient claim of digital innocence—that is, a plausible showing that the federal government possessed rel-

548 *Id.* at 469.
549 *Id.* at 472 (Frankfurter, J., concurring).
550 *See, e.g.*, Larson v. Domestic & Foreign Commerce Corp., 337 U.S. 682, 690 (1949).
551 United States v. Valenzuela-Bernal, 458 U.S. 858, 867 (1982).
552 159 F.3d 875 (4th Cir. 1998).
553 *See id.* at 878, 881–83; *id.* at 886 (Phillips, J., dissenting).
554 *See id.* at 881–83 (majority opinion).
555 *See id.* at 883 n.2 (quoting United States v. Smith, 780 F.2d 1102, 1108 (4th Cir. 1985) (en banc)) (internal quotation marks omitted).

evant and potentially exculpatory data—it would be incumbent upon a federal judge to order at least an in camera inspection of the sought-after information.[556] The same analysis should apply when the federal government raises a claim of privilege. In particular, the government's assertion of the state secrets privilege can be reviewed under CIPA or CIPA-like procedures. Judicial practice and a federal regulation assume as much.[557] Moreover, a state proceeding removed to U.S. district court is derivative of the state court's jurisdiction over criminal cases. Thus, a federal court evaluating an issue of classified information within the context of a motion by the federal government to quash a subpoena is, in fact, exercising jurisdiction over a criminal case (albeit a state case). This would seem to trigger CIPA's provisions or at least make CIPA "a useful framework."[558] The resulting in camera review and the aforementioned substitution process could help protect the rights of state criminal defendants with viable claims of digital innocence—at least more so than a perfunctory quashal without any independent review of the information in question.

Even if the foregoing arguments fall flat in court, a state criminal defendant may still have a remedy. For instance, he can challenge a federal agency's decision not to disclose information by bringing a separate civil action under the Administrative Procedure Act (APA)[559] or perhaps by seeking a writ of mandamus against the appropriate federal official (e.g., the U.S. Attorney General).[560] This is exactly what happened in *Johnson v. Reno*.[561] On trial for capital murder, the state defendant had been frustrated in his attempt to obtain relevant materials from a series of federal law enforcement agencies that had participated in the underlying criminal investigation. There was no doubt that the information in question would have been discoverable *Brady* material had the defendant been prosecuted federally.[562]

Emphasizing the importance of this information to the defendant given the serious criminal charges he was facing, the *Johnson* court referenced an opinion by Judge Learned Hand.[563] "While we must accept it as lawful for a department of the government to suppress documents, even when they will help determine controversies between third persons," Judge Hand wrote, "we cannot agree that this

556 *Cf.* Pennsylvania v. Ritchie, 480 U.S. 39, 60 (1987) (ordering such an in camera review by a state trial court).

557 *See, e.g.*, Kasi v. Angelone, 200 F. Supp. 2d 585, 596 (E.D. Va. 2002) (discussing a state court performing an in camera review), *aff'd*, 300 F.3d 487 (4th Cir. 2002); 28 C.F.R. § 17.17(b) (2013).

558 *See supra* note 444 and accompanying text. *See generally supra* Part V.A.1.

559 *See* 5 U.S.C. §§ 701–706 (2012).

560 *See* 28 U.S.C. § 1361 (2012).

561 92 F. Supp. 2d 993 (N.D. Cal. 2000).

562 *See id.* at 995.

563 *See id.* at 994.

should include their suppression in a criminal prosecution, founded upon those very dealings to which the documents relate, and whose criminality they will, or may, tend to exculpate."[564] After citing Hand's opinion, the *Johnson* court ordered the production of the information, finding that the agencies' decisions were "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law," as well as contrary to the defendant's constitutional rights.[565]

Admittedly, the APA/mandamus route may prove to be a dead end for digital innocence claims, and, if nothing else, requiring a state criminal defendant "to file a separate mandamus action or a cumbersome APA suit in the middle of his [case] is so burdensome that it effectively eviscerates his right."[566] In the face of a recalcitrant federal agency and an unduly compliant federal court, the state defendant's best (or only) option may be to take the issue out of federal hands and pursue a remedy against the underlying state case itself. State courts have the authority to dismiss a criminal case or make adverse findings against the prosecution if state officials' invocation of privilege results in their refusal to disclose potentially exonerating evidence.[567] A state court should have the same power when the noncompliant entity is a federal agency. The federal government may have the absolute prerogative to withhold certain secrets, but criminal courts in both the federal and state systems need not tolerate an incomplete and potentially erroneous truth-finding process.

B. Post-Conviction Relief

Where proof of innocence is only found after conviction, defendants face a range of legal arguments intended to limit post-conviction challenges. Some restrictions are considered necessary to stop repetitive and abusive petitions, but they can also severely restrict the ability of the actually innocent to exonerate themselves. This section considers the procedural bar to habeas relief imposed by the Antiterrorism and Effective Death Penalty Act (AEDPA),[568] before turning to recent developments in the law that may provide hope for the wrongfully convicted who discover digital evidence of actual innocence.

---

564 United States v. Andolschek, 142 F.2d 503, 506 (2d Cir. 1944).

565 *Johnson*, 92 F. Supp. 2d at 995 (quoting 5 U.S.C. § 706(2)(A)–(B) (2012)) (internal quotation marks omitted). In the alternative, the *Johnson* court found that the mandamus requirements were met because: (1) the defendant's claim was "clear and certain"; (2) the agencies had ignored and/or violated the standards delimiting their discretion; and (3) no other adequate remedy was available. *Id.* (internal quotation marks omitted).

566 *In re* Boeh, 25 F.3d 761, 770 n.4 (9th Cir. 1994) (Norris, J., dissenting).

567 *See, e.g.*, Hines v. Superior Court, 251 Cal. Rptr. 28, 30 (Cal. Ct. App. 1988) (laying out guidelines for California courts making adverse findings after privilege is invoked by state officers).

568 Pub. L. No. 104-132, 110 Stat. 1214 (codified as amended in scattered sections of the U.S. Code).

1. *Habeas and AEDPA*

Arguably, AEDPA has been the largest obstacle for wrongful conviction claims. Prior to the law's enactment in 1996, the Supreme Court had held that the "great writ" of habeas corpus was subject to various procedural defaults—for instance, a defendant's submitting "successive" or "abusive" petitions, his failing to develop facts in state court, or his defying state procedural rules such as filing deadlines—which thereby precluded federal court review of state court judgments. For its part, AEDPA further imposes a one-year statute of limitations on federal habeas petitions.[569] To date, the Supreme Court has not recognized a freestanding claim of actual innocence,[570] meaning that an inmate raising a wrongful-conviction argument must shoehorn the issue through some other viable legal ground—most frequently, a Sixth Amendment claim of ineffective assistance of counsel.

AEDPA itself contains an exception to the otherwise stringent one-year deadline for claims of newly discovered evidence, so long as the petition is filed within one year of "the date on which the factual predicate of the claim or claims presented could have been discovered through the exercise of due diligence."[571] In essence, this provision triggers a new one-year limitations period starting with the time at which the evidence should have been discovered by a conscientious defense.[572] The operative inquiry then is one of "reasonable diligence" and whether its exercise would have uncovered exonerating information.[573] The question is not unfamiliar to courts in other contexts, and there is a developed jurisprudence of diligence.[574] While a literature survey is beyond the present scope, the following will identify trends in the interpretation of the diligence requirement that might provide some guidance for inmates seeking exoneration based on strong digital evidence.

Broadly stated, the cases suggest that a petitioner must move promptly to develop relevant facts. A petitioner proceeding pro se and developing legal arguments from a prison library is held to tight deadlines. Lack of education is not an excuse, nor are limited facilities, limited ability to access the law, constrained or nonexistent access

---

569 *See* 28 U.S.C. § 2244(d)(1)(A) (2012) ("A 1-year period of limitation shall apply to an application for a writ of habeas corpus by a person in custody pursuant to the judgment of a State court.").

570 *See, e.g.*, Herrera v. Collins, 506 U.S. 390, 404–05 (1993) ("We have never held that it extends to freestanding claims of actual innocence.").

571 28 U.S.C. § 2244(d)(1)(D).

572 *See id.*

573 *Id.* § 2244(c).

574 *See, e.g.*, Lee Kovarsky, *Death Ineligibility and Habeas Corpus*, 95 CORNELL L. REV. 329, 342 (2010) (discussing AEDPA's statute of limitations requirement).

to counsel, and so on. Of concern here, the restrictions placed on prisoners in one technical field—law—may in the future be applied with equal narrowness to the requirements that an inmate somehow secure help in conducting sophisticated data searches.[575] Although prisoners are expected to be expert lawyers and clerks in order to protect their rights, thus far the courts do not expect prisoners to be technical scientists. Hopefully, prisoners will not be required to add a computer science Ph.D. to their J.D. in the year following conviction.

For digital innocence, the salient feature is that while huge amounts of information are being stored now, the existence of a particular piece of evidence, or its meaning in relation to other pieces of evidence, may only be found years later. To be useful in digital innocence claims, this store-now, parse-later trend requires the refinement of digital analysis tools. Parsing algorithms must grow in strength and become available to the broader public beyond Big Data firms.[576] Moreover, discovery may have to wait until databases become big enough or connected enough for meaningful analysis. But if this happens, the facts should rise to the surface as storage costs fall and search algorithms improve.[577]

Consider the following example: A man is wrongfully accused of murder but is convicted nonetheless and sent to prison for a crime he did not commit. A decade later, an innocence project runs a "search bot" over social networking data and finds that the defendant could not have committed the offense. A geolocated and time-stamped picture of the defendant was posted from an acquaintance's smartphone to a now-defunct social photography service. This photograph demonstrates that the defendant was, as he claimed, many miles away at the time of the murder. Because AEDPA conceptualizes exonerating evidence as single, discrete pieces of information, the question is when the data should have been found by the exercise of reasonable diligence.

More problematic under AEDPA is proof of innocence that does not involve a single, crucial, game-changing piece of evidence but instead comes from the ability of data-mining software to discover

---

575 *See, e.g.*, Emily G. Uhrig, *The Sacrifice of Unarmed Prisoners to Gladiators: The Post-AEDPA Access-to-the-Courts Demand for a Constitutional Right to Counsel in Federal Habeas Corpus*, 14 U. PA. J. CONST. L. 1219, 1243 (2012) (discussing the doctrine of equitable tolling).

576 *See* Gruenspecht, *supra* note 113, at 545 ("[B]ecause of the networking of digital storage, third parties are now significantly more likely to possess digital data, such as personal communications and stored documents, created by others."); Richards, *supra* note 154, at 1939 (describing the concept of Big Data and its potential implications); Schwartz, *supra* note 63 (examining the legal issues surrounding GPS data privacy).

577 *See* Daniel M. Katz, *Quantitative Legal Prediction—or—How I Learned to Stop Worrying and Start Preparing for the Data-Driven Future of the Legal Services Industry*, 62 EMORY L.J. 909, 943 (2013) ("The decrease in data storage cost and increase in processor speed has brought with it a massive proliferation of electronically stored information . . . .").

patterns. This is consistent with the way the technology works: digital parsing tools reveal patterns,[578] and a pattern is not one fact in isolation but rather a set of relationships between different parts.[579] In pattern recognition, some parts of the pattern will become apparent before others, and at times almost the entire pattern will be available with just a few pieces missing to make the picture complete. The facts will become known at different times, although some, if not most, may already be known at the time of trial. Generally speaking, this situation is the mosaic theory redux.[580] As the Supreme Court said in *CIA v. Sims*, "bits and pieces of data may aid in piecing together bits of other information even when the individual piece is not of obvious importance in itself."[581]

Now consider the question from the perspective of a prisoner who finds a fact that tends toward her exoneration. Should she file within a year, even though she has not obtained corroborating evidence, or should she seek to corroborate that evidence? If she waits but the first fact is the only one she finds, the defendant will have lost her only chance to challenge her imprisonment.[582] But if she files within the deadline despite the fact that there is much more to find, the defendant will have foregone her best chance to convince the court that she is innocent based on multiple corroborating data points. The tradeoff between time and certainty may impel prisoners to file under-supported claims before the deadline runs, regardless of how much corroboration they have obtained.

The speed of a database claim may be inversely related to its reliability as a hard proof of innocence. Some pieces of a data puzzle will be open and obvious from the outset. The pattern may not be convincing until the pattern is complete, but at that point it may be completely convincing. The fact that data mining excels at matching pieces of data over time complicates things for the courts. If they permit prisoners to file habeas petitions based on the timing of the last fact discovered, past-known facts would be grandfathered in based on the discovery of some new fact.[583] If courts instead focus solely on the

---

578 *See* Richards, *supra* note 154, at 1939.

579 *See id.* ("[D]ata in one area can be linked to other areas and analyzed to produce new inferences and findings.").

580 *See supra* notes 338–39 and accompanying text.

581 471 U.S. 159, 178 (1985) (quoting Halperin v. CIA, 629 F.2d 144, 150 (1980)) (internal quotation marks omitted).

582 *See* Kovarsky, *supra* note 574, at 341 (illustrating that roughly "four percent of post-AEDPA capital cases include a time-barred claim").

583 *See* Jennifer G. Case, *How Wide Should the Actual Innocence Gateway Be? An Attempt to Clarify the Miscarriage of Justice Exception for Federal Habeas Corpus Proceedings*, 50 WM. & MARY L. REV. 669, 679 (2008) (examining a circuit split "as to whether the *Schlup* standard 'requires newly discovered evidence or merely newly presented evidence'" (quoting Wright v. Quarterman, 470 F.3d 581, 591 (5th Cir. 2006))).

date of the first related fact necessary to complete the pattern, they could effectively foreclose the "new evidence" exception for an entire category of digital innocence cases.

2. *Actual Innocence*

With sufficiently strong proof of digital innocence, however, petitioners may be able to avoid the procedural bars of AEDPA. In its recent decision in *McQuiggin v. Perkins*,[584] the Supreme Court considered whether there was an actual innocence exception to AEDPA's diligence requirement, and if so, how strong the evidence must be to pass through this gateway. The pre-AEDPA jurisprudence had recognized a "miscarriage of justice" exception to overcome procedural defaults in filing a habeas petition.[585] In particular, an inmate who could not provide good cause for a procedural default, such as abusive or successive uses of the writ of habeas corpus, nonetheless "may have his federal constitutional claim considered on the merits if he makes a proper showing of actual innocence."[586] A credible showing of actual innocence could overcome procedural bars to relief, "grounded in the 'equitable discretion' of habeas courts to see that federal constitutional errors do not result in the incarceration of innocent persons."[587]

To be viable today, this exception would need to have survived AEDPA's enactment, and the relationship between pre-AEDPA law and post-AEDPA deadlines is thorny. AEDPA's statute of limitations can be equitably tolled if the petitioner has acted diligently with regards to the claim's development and was prevented from filing by some extraordinary event. These criteria were not met in *Perkins* because the statute of limitations had expired and the defendant had

584 *See* 133 S. Ct. 1924, 1928 (2013) (holding that evidence of actual innocence can overcome the habeas statute of limitations if "in light of the new evidence, no juror, acting reasonably, would have voted to find him guilty beyond a reasonable doubt").

585 *See, e.g.*, Keeney v. Tamayo-Reyes, 504 U.S. 1, 12 (1992) ("A habeas petitioner's failure to develop a claim in state-court proceedings will be excused . . . if . . . a fundamental miscarriage of justice would result from failure to hold a federal evidentiary hearing."); Coleman v. Thompson, 501 U.S. 722, 750 (1991) ("[F]ederal habeas review of the claims is barred unless the . . . failure to consider the claims will result in a fundamental miscarriage of justice."); McCleskey v. Zant, 499 U.S. 467, 494–95 (1991) ("[T]he failure to raise the claim in an earlier petition may nonetheless be excused if . . . a fundamental miscarriage of justice would result from a failure to entertain the claim."); Murray v. Carrier, 477 U.S. 478, 495–96 (1986) ("[V]ictims of a fundamental miscarriage of justice will meet the cause-and-prejudice standard." (quoting Engle v. Isaac, 456 U.S. 107, 135 (1982)) (internal quotation marks omitted)); Kuhlmann v. Wilson, 477 U.S. 436, 454 (1986) ("[S]uccessive federal habeas review should . . . be available when the ends of justice so require.").

586 Herrera v. Collins, 506 U.S. 390, 404 (1993); *see also Carrier*, 477 U.S. at 496 ("[A] federal habeas court may grant the writ even in the absence of a showing of cause for the procedural default.").

587 *Herrera*, 506 U.S. at 404 (quoting *McCleskey*, 449 U.S. at 502).

not diligently pursued his rights,[588] thereby adding another prerequisite to the defendant's actual innocence claim: time must not be of the essence in any preexisting, court-crafted, AEDPA-surviving exception.

The *Perkins* Court concluded that "actual innocence, if proved, serves as a gateway through which a petitioner may pass whether the impediment is a procedural bar, . . . or, as in this case, expiration of the statute of limitations."[589] When faced with an actual-innocence gateway claim, "a federal habeas court . . . should count unjustifiable delay on a habeas petitioner's part, not as an absolute barrier to relief, but as a factor in determining whether actual innocence has been reliably shown."[590] As a threshold requirement, the defendant must persuade a habeas court that, "in light of the new evidence, no juror, acting reasonably, would have voted to find him guilty beyond a reasonable doubt."[591] Moreover, Justice Ruth Bader Ginsburg's majority opinion cautioned "that tenable actual-innocence gateway pleas are rare."[592] For defendant Perkins, his claim on remand was predestined for denial, given the district court had already concluded the defendant "had not shown that, taking account of all the evidence, 'it is more likely than not that no reasonable juror would have convicted him,' or even that the evidence was new."[593]

Without a doubt, however, the *Perkins* framework will be a positive development for the use of Big Data to exonerate, since the removal of the time bar is critical for digital innocence claims. Indeed, a forgiving standard may be in order given the aforementioned difficulties attending the procurement and analysis of the underlying data. Technology can deliver new evidence of innocence, but the necessary progress takes time. In the case of DNA testing, the technology to prove innocence took decades to develop. If time alone barred the wrongfully convicted from challenging their incarceration, innocence derived from new technological advances would be useless in many cases. And, as noted previously, it may take time for a pattern to become complete. Some pieces of the data puzzle may be missing at first and only become evident over time. But when the puzzle is

---

588 *See Perkins*, 133 S. Ct. at 1936 ("[E]quitable tolling was unavailable to Perkins because he could demonstrate neither exceptional circumstances nor diligence.").

589 *See id.* at 1928.

590 *Id.*

591 *Id.* (quoting Schlup v. Delo, 513 U.S. 298, 319 (1995)) (internal quotation marks omitted).

592 *Id.*

593 *Id.* at 1930 (quoting the district court's opinion); *see* Perkins v. McQuiggin, No. 2:08-cv-139, 2013 WL 4776285, at *3 (W.D. Mich. Sept. 4, 2013) (dismissing petition on remand).

finally completed, the provably innocent must have an avenue to overturn their convictions.

Certainly, *Perkins* requires strong proof to reach the gateway, but Big Data technology delivers precisely this kind of hard evidence of actual innocence. Geolocation information will establish alibis. Tagged photographs and facial recognition will prove innocence by showing that someone else committed an act. Telephony metadata records will demonstrate that a conspiracy had some members but that others were outside of the circle. Social network maps will prove who-knew-whom for purposes of evaluating witness and informer testimony. The list goes on and on. What is most important is that when this proof of innocence is unearthed by quickly growing information technology, there will be a path to justice for the wrongfully convicted.

Conclusion

In the wake of the Snowden disclosures, Americans are being forced to weigh the costs and benefits of Big Data and mass surveillance in terms of their privacy and security. To date, however, the analysis has failed to consider an important consequence: as a result of their spying en masse, the government and commercial entities assume an obligation to provide criminal defendants access to potentially exculpatory evidence. The depth and breadth of corporate and government surveillance virtually guarantee that evidence of digital innocence will be found using the tools of Big Data. This Article has sought to identify and describe the relevant technology, and to suggest a path forward to prevent wrongful convictions and exonerate the actually innocent already behind bars. We do not revel in the emergence of a surveillance society and an Orwellian national security apparatus. But we do want to make clear one unavoidable consequence for the watchers. Conceptualizing digital innocence is just the first step, but a necessary one, to ensure that Big Data and data mining are not reserved solely for convictions.