TOTAL SURVEILLANCE, BIG DATA, AND PREDICTIVE CRIME TECHNOLOGY: PRIVACY'S PERFECT STORM

Kevin Miller[*]

* Kevin Miller is a graduate of the University of Florida Levin College of Law and has an MBA in Technology Management. He has published articles in the *Southern California Interdisciplinary Law Journal*, the *ILSA Quarterly*, and the *University of Florida Journal of Law & Public Policy*. He has also published a book on software development and presented papers at several technology conferences. He is currently employed at the intellectual property law firm of Saliwanchik, Lloyd & Eisenschenk in Gainesville, Florida. Prior to attending law school, he was a software engineer and technology specialist for several technology companies, including Microsoft, before founding his own software company.

I. INTRODUCTION

Since the first widespread uses of computer databases in the 1970s, experts have warned of the Orwellian "computer state" in which governments and private corporations collect, store, and share vast troves of data about citizens.[1] In the last decade or so, new technologies have been brought to bear upon the information management challenge posed by this deluge of data. These new techniques have targeted three distinct, but related, areas. First, they have enabled the cataloging of human behaviors that were previously ephemeral. These enhanced cataloging powers have coincided with an increasing willingness by law enforcement agencies to conduct—and courts to condone—widespread, total surveillance of citizens in the name of national security. Second, semantic query systems and "big data" analytical engines have introduced an approach to discerning patterns in data that prior systems lacked. The methodology underlying these approaches is tacit, but, I will argue, likely flawed. Third, these new techniques of surveillance gathering and data analysis have begun to transition into their next phase, prediction and scoring of individuals' risk of criminal behavior. Individualized suspicion of criminal activity once triggered a review of a person's data portfolio, but now the data portfolio triggers individualized suspicion.

While predictive techniques have been used in targeted areas of criminology for decades, this article argues that the move toward predictive policing using automated surveillance, semantic processing, and analytics tools magnifies each technology's harms to privacy and due process, while further obfuscating the systems' technological and methodological limitations. Furthermore, they do so with little offsetting diminishment of the risk of criminal activity or terrorism. The time is right to revisit predictive systems in light of these new advancements.

Legal protections for individual privacy are at a low ebb in the United States, as countless commentators and the recent release of long-secret FISA court opinions have demonstrated. A long string of cases interpreting the First and Fourth Amendments have shown that those legal doctrines are mostly inadequate to meet the challenges posed by the use of modern, technologically amplified surveillance and prediction techniques. My purpose here is to consider the legal, technical, and methodological issues raised by surveillance-fed predictive systems that may substantiate policy arguments against their widespread adoption. If this policy position is convincing, then legal and economic arguments

1. *See* WILLIAM BOGARD, THE SIMULATION OF SURVEILLANCE: HYPERCONTROL IN TELEMATIC SOCIETIES 2 (1996).

could be brought to bear to discourage the conditions which have fostered the explosive growth and abuse of these systems.

With those objectives in mind, the paper proceeds in four parts. Part II describes the paradigm of the "triple threat" to privacy which stems from total surveillance, big data analytics, and actuarial trends in policing. Part III surveys methodological problems with big data analytics and predictive policing which make these tools much less useful than advertised. Part IV considers the difficulties of using traditional First and Fourth Amendment doctrine in the light of technological advances. Finally, Part V discusses the possible methods of curbing the use of these flawed tools in the pre-crime prediction arena by exploring various expanded legal and economic approaches.

II. THE PARADIGM OF CRIME PREDICTION

A. *Brief Overview of Modern, Total Surveillance*

To best comprehend the full range of privacy concerns stemming from the use of predictive systems built on big data surveillance, it is critical to assess the technical and legal environment in which these systems are built and used. Recent disclosures by Edward Snowden about the data gathering practices of the National Security Agency (NSA) and other law enforcement agencies have been instructive in this regard.[2] The picture that emerges from these disclosures and others by prior whistleblowers such as Mark Kline and William Binney,[3] coupled with the cavalier attitude of current and former NSA directors[4] and charges by security experts that the NSA has for several years attempted to introduce subtle flaws into cryptographic encryption standards in order to make communications easier to analyze,[5] is a grim wake-up call to Americans and foreign citizens about how little privacy they possess.

The U.S. Government's ability to compromise the world's

2. The stories and commentary on the Snowden disclosures are too numerous to list individually, but the *Guardian* newspaper maintains a good launch point. *See, e.g.*, *The NSA Files*, GUARDIAN, Dec. 16, 2013, http://www.theguardian.com/world/the-nsa-files.

3. *See* JAMES BAMFORD, THE SHADOW FACTORY 188–91 (2008); James Bamford, *The NSA is Building the Country's Biggest Spy Center*, WIRED, Mar. 15, 2012, http://www.wired.com/threatlevel/2012/03/ff_nsadatacenter/.

4. *See* Yochai Benkler, *Fact: The NSA Gets Negligible Intel from Americans' Metadata*, GUARDIAN, Oct. 8, 2013, http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence.

5. Kim Zetter, *How a Crypto 'Backdoor' Pitted the Tech World Against the NSA*, WIRED, Sept. 24, 2013, http://www.wired.com/threatlevel/2013/09/nsa-backdoor/.

communications systems begins at the physical wire. Because a large portion of internet traffic is routed through the United States on the way to its final destination, total surveillance begins by tapping into key positions at the junction points where international undersea cables attach to U.S. networks.[6] However, these cables—docking in many places on both coastlines, including New Jersey, Miami, and San Francisco—are controlled by private telecom carriers, so their assistance is required.[7] At these junction points, in secret rooms full of NSA equipment, the optical signal carried by fiber optic cable is split and mirrored by sophisticated technology.[8] One signal is sent on its way normally through the network, while the mirrored copy is redirected to NSA storage and recording equipment.[9] AT&T, among others, has a history of colluding with the federal intelligence agencies going back decades.[10] In fact, some have suggested that one reason for the government's easing of the 1980s AT&T "breakup" consent decree, allowing the company to reestablish itself with much the same dominance as it had before the breakup, was to simplify NSA collusion by reducing the number of private telecom entities.[11] Most of this wiretapping assistance by private telecom companies was, in fact, illegal under federal and state laws until the FISA Amendments Act of 2008 bequeathed to them blanket and retroactive immunity from prosecution.[12]

Despite this elaborate setup, listening in on a raw data stream still has its difficulties. Network communication is broken up into discrete packets of data which, when jumbled together, make little sense.[13] Intelligence agencies cannot simply read a person's email off the wire without additional processing.[14] Reassembling all these discrete packets into a sensible narrative takes time, complex software, and a great deal of processing power.[15] To further complicate matters, some data traffic between consumers and companies is encrypted to make it unreadable to anyone merely listening in on the data stream.[16]

---

6. *See* BAMFORD, *supra* note 3, at 175–79.
7. *See id.* at 175–81.
8. *Id.* at 188–89.
9. *Id.* at 188–91.
10. *See id.* at 223–30.
11. TIM WU, THE MASTER SWITCH 250 (2010).
12. FISA Amendments Act of 2008, P.L. 110-261 (July 10, 2008).
13. *See* BAMFORD, *supra* note 3, at 191–94.
14. *See id.*
15. *See id.* at 194.
16. Google mail, for example, encrypts communication between the user and the service, and Google has recently stepped up efforts to encrypt communications between company data centers. *See* Craig Timberg, *Google Encrypts Data Amid Backlash Against NSA Spying*, WASH. POST (Sept. 6, 2013), http://www.washingtonpost.com/business/technology/google-encrypts-

In processing, the data is first culled by intelligent hardware solutions that clean the packets by filtering out unnecessary routing information, then attempt to reassemble them into a more sensible order based on rough targeting and selection parameters.[17] Once culled, the data is typically directed to NSA facilities, where it is stored until it becomes useful to analysts.[18] A recent executive order gave the NSA authority to store any and all traffic for up to five years.[19] Naturally, storing all the internet's traffic in raw form for that long requires a massive storage facility, and to keep up with the explosive data growth, a secret, new, $2 billion facility is being constructed in Utah.[20]

> Flowing through its servers and routers and stored in near-bottomless databases will be all forms of communication, including the complete contents of private emails, cell phone calls, and Google searches, as well as all sorts of personal data trails-parking receipts, travel itineraries, bookstore purchases, and other digital "pocket litter."[21]

Encrypted data, considered to be reason for suspicion in and of itself, may be stored indefinitely so that it can be deciphered even years later, as codebreaking technology improves.[22]

Given the technical and resource challenges, it would be far easier simply to secure the collusion of major internet service and content providers than to dissect and reassemble the packets one by one or to crack their encryption. In this way, information could be reviewed in the context of its creation. In fact, as the Snowden documents have revealed, this is precisely what the NSA has done, bringing legal pressure on dozens of major ISPs to assent to "information sharing" programs allowing direct or simplified NSA access to user data in its original context.[23]

---

data-amid-backlash-against-nsa-spying/2013/09/06/9acc3c20-1722-11e3-a2ec-b47e45e6f8ef_story.html.

17. *See* BAMFORD, *supra* note 3, at 192–94.

18. *See generally id.*

19. Glenn Greenwald & James Bald, *The Top Secret Rules that Allow NSA to Use US Data Without a Warrant*, GUARDIAN, June 20, 2013, http://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant; *see* Exec. Order No. 12,333, 3 C.F.R. 200 (1981), *available at* http://www.archives.gov/federal-register/codification/executive-order/12333.html.

20. BAMFORD, *supra* note 3, at 188–91.

21. *Id.*

22. Joshua Kroll, *Is the NSA Keeping Your Encrypted Traffic Forever?*, FREEDOM TO TINKER (Sept. 13, 2013), https://freedom-to-tinker.com/blog/kroll/is-the-nsa-keeping-your-encrypted-traffic-forever/.

23. *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 6, 2013), http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-inter

With the opening of the new storage facility in Utah and the cooperation of important ISPs, the agency's technical capabilities will be consistent with the recently publicized agenda of its leaders: total collection and total storage, with analysis to follow. According to a recent profile of General Keith Alexander, director of the NSA,

> [He] wants as much data as he can get. And he wants to hang on to it for as long as he can. . . . [H]e thinks he needs to be able to see entire networks of communications and also go "back in time," as he has said publicly, to study how terrorists and their networks evolve. To find the needle in the haystack, he needs the entire haystack.[24]

A former colleague has said, "Alexander's strategy is the same as Google's: I need to get all of the data."[25] These policies have met with little judicial resistance: the court charged with review of surveillance practices, the Foreign Intelligence Surveillance Court (FISC), has recently released a formerly secret court opinion sanctifying the widespread telephony metadata gathering program under Section 215 of the Patriot Act and the "third-party doctrine" interpretation of *Smith v. Maryland*.[26] Even after the outcry over the Snowden revelations, the FISC recertified the program.[27] The Senate Intelligence Committee also recently praised the NSA program and voted a bill out of committee which, if passed, would codify into law most of the current NSA

---

net-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Though, occasionally the ISPs have denied colluding with the NSA. *See, e.g.*, *id.*; Jon Brodkin, *AT&T Gives DEA 26 Years of Phone Call Records to Wage War on Drugs*, ARSTECHNICA (Sept. 3, 2013, 12:11 PM), http://arstechnica.com/tech-policy/2013/09/att-gives-dea-26-years-of-phone-call-records-to-wage-war-on-drugs/. One smaller provider of encrypted email service has resisted the NSA. Joe Mullin, *Lavabit's Appeal: We're Actually Not Required to Wiretap Our Own Users*, (Oct. 11, 2013, 2:25 PM), http://arstechnica.com/tech-policy/2013/10/lavabits-appeal-were-actually-not-required-to-wiretap-our-own-users/.

24. Shane Harris, *The Cowboy of the NSA*, FOREIGN POLICY (Sept. 9, 2013), *available at* http://www.foreignpolicy.com/articles/2013/09/08/the_cowboy_of_the_nsa_keith_alexander.

25. *Id.*

26. *Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Redacted]*, No: BR 13-109, *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf (last accessed Dec. 16, 2013); *see also* Jake Laperruque, *Intelligence Agencies Justify Collecting Your Personal Data by Applying the Six Degrees of Kevin Bacon*, CENTER FOR DEMOCRACY AND TECHNOLOGY (Nov. 20, 2013), *available at* https://www.cdt.org/blogs/nasreen-hosein/2011intelligence-agencies-justify-collecting-your-personal-data-applying-six-de.

27. Press Release, OFF. OF THE DIR. OF NAT'L INTELLIGENCE, Foreign Intelligence Surveillance Court Approves Government's Application to Renew Telephony Metadata Program (Oct. 11, 2013), *available* at http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/944-foreign-intelligence-surveillance-court-approves-government%E2%80%99s-application-to-renew-telephony-metadata-program.

policies on telephone metadata collection.[28]

Most of what has been discussed so far pertains to data surveillance—gathering transactions and other traces of human behavior that have already occurred. Biometric surveillance additionally ensures that watchers can always know who, and where, individuals are.[29] The widespread placement of video surveillance cameras, when linked with centralized facial image databases and facial recognition software, enables the identification of citizens in virtually any public or semi-private space.[30] New forms of digital identification, including passports and state driving licenses containing RFID chips, but also including "cardless" ID systems based on fingerprints, retinal scans, and voice patterns, ensure that all interactions with an individual are authenticated (and non-anonymous).[31] Automobile tracking devices such as the EZ-Pass toll system enable organizations to identify automobiles as they move through diverse checkpoints.[32] Tracking of cell phone data with "tower dumps," combined with statistical modeling of human movements,[33] can ensure that an individual's location is always known. Moreover, the unification of these diverse data sources is already under way. For example, the FBI's Next Generation Identification (NGI) program seeks to unify civilian, law enforcement, and military biometric databases with photographs and other data held by private institutions (*e.g.*, Facebook) into a centralized repository accessible to all governmental agencies.[34] This powerful combination, unifying data surveillance with centralized, mandatory biometric identity tracking, enables what Margaret Hu calls "bureaucratized surveillance,"[35] in which all encounters between state and citizen are screened, automated, and flagged when deemed to be suspicious.[36]

In addition to government surveillance, commercial entities use

---

28. *See* Matt Sledge, *Senate Intelligence Committee Passes Bill that Codifies, Expands NSA Powers*, HUFFINGTON POST (Oct. 31, 2013, 4:30 PM), http://www.huffingtonpost.com/2013/10/31/senate-bill-nsa_n_4183183.html.

29. *See* Margaret Hu, *Biometric ID Cybersurveillance*, 88 IND. L.J. 1475, 1475–81 (2013).

30. *See id.* at 1534–35.

31. *See id.* at 1480–81.

32. *See* Kashmir Hill, *E-Z Passes Get Read All Over New York (Not Just at Toll Booths)*, FORBES (Sept. 12, 2013, 4:44 PM), *available at* http://www.forbes.com/sites/kashmirhill/2013/09/12/e-zpasses-get-read-all-over-new-york-not-just-at-toll-booths/.

33. *See* Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCI. REP. 1376 (2013), *available at* http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html; *see also* David Kravets, *1.3M Cellphone Snopping Requests Yearly? It's Time for Privacy and Transparency Laws*, WIRED (July 7, 2012, 6:30 AM), http://www.wired.com/threatlevel/2012/07/mobile-data-transparency/all/.

34. *See* Hu, *supra* note 29, at 1552–53.

35. *Id.* at 1479.

36. *Id.* at 1500.

extensive tracking networks to collect and sell the behaviors of consumers, even going so far as to collect how long it takes to read an Amazon Kindle book.[37] Even children are not immune from surveillance. The Glendale, California school district has hired a private company, Geo Listening, to review its 13,000 students' social media activity and produce a daily report on problematic online conduct.[38] However, some school districts are becoming concerned about the vast explosion of data now being collected on children and shared with private entities.[39] Recent amendments to FERPA expanded the circle of parties with which student data can be shared.[40] Not only are the companies providing learning data systems often not clear about with whom they share data, parents are concerned about what will eventually come of behavioral data and other assessments—and whether that information will permanently limit their child's future.[41]

B. *The Rise of Big Data Analytics*

As we have seen, the NSA now has a massive collection of internet and telephone traffic, stored for up to five years. Internet content providers share with the NSA the contents of private databases and encrypted communications with customers. Private data brokers track every conceivable citizen encounter, then digest, codify, and sell those data collections to whoever will buy them. Biometric and location data is unified in centralized repositories. Data is everywhere, but what can be done to turn this morass of data into useful, actionable information? This question had a hesitant answer until the advent of the statistical modeling, data processing, and artificial learning techniques collectively called "big data analytics."[42]

Originally created to understand consumer behavior—will a person who buys product X also buy product Y?—big data analytics has increasingly come to be seen as the solution to any problem involving

---

37. *See, e.g.*, *Privacy and Consumer Profiling*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/profiling/ (last visited Dec. 17, 2013); Alexandra Alter, *Your E-Book is Reading You*, WALL ST. J. (July 19, 2012), http://online.wsj.com/news/articles/SB10001424052702304870304577490950051438304.

38. Tim Cushing, *CA School District Announces It's Doing Round-The-Clock Monitoring of Its 13,000 Students' Social Media Activities*, TECHDIRT (Sept. 10, 2013), http://www.techdirt.com/articles/20130902/13154624384/ca-school-district-announces-its-doing-round-the-clock-monitoring-its-13000-students-social-media-activities.shtml.

39. Natasha Singer, *Deciding Who Sees Students' Data*, N.Y. TIMES (Oct. 5, 2013), http://www.nytimes.com/2013/10/06/business/deciding-who-sees-students-data.html.

40. *Id.*

41. *Id.*

42. *See* Special Report, *Data, Data Everywhere*, ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557443.

large amounts of data, including determining how to influence voters, diagnosing medical conditions, and looking for cheaters in casinos.[43] Big data analytics has been seen as a panacea for data-heavy problems because it shortcuts the time-consuming process of forming a hypothesis, gathering data, and testing it—the classical method in all sciences.[44] It improves efficiency by using computation to examine large data sets for correlations between data entities, eschewing the deeper understanding given by theories with the power of causal explanation.[45] Chris Anderson has called this trend "the end of theory," as theory is irrelevant to the analytical framework—no theory is needed by the machine to initiate the relational analysis, and no theory of explanation results from it.[46] One commentator sums it up by saying, "The key is to forget about the truth. . . . Truth is not a make or break test."[47] This shotgun approach to finding correlations has been enabled by cheap data storage, cheap computing power, and the ever-increasing availability of feeder data[48] enabled by near-total government and private surveillance of humans' every action. In the words of one advocate, "More data is always better."[49]

Correlations are interesting and useful for categories of inquiry that can do without causal explanation. An oft-cited example is how Google can see influenza infection trends before the CDC by correlating search terms about flu remedies with geolocation data; however, it turns out that this "successful" example of data mining was exaggerated by a factor of two, according to a study in *Nature*.[50] In light of this, the areas where these methods are useful tend to be those where high rates of spurious correlation and false positives are acceptable, or where the model has low predictive power but is still better than existing methods by a few percent.[51] Big data began in marketing because that field's tolerance for error is so high.[52] The president of blog data miner

43. *See generally* STEPHEN BAKER, THE NUMERATI 12–15 (2008).

44. Chris Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, WIRED (June 23, 2008), http://www.wired.com/science/discoveries/magazine/16-07/pb_theory.

45. *Id.*

46. *Id.*

47. BAKER, *supra* note 43, at 90.

48. *See* VIKTOR MAYER SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 54–56 (Kindle ed. 2013).

49. BAKER, *supra* note 43, at 128 (quoting NSA's chief mathematician James Schatz).

50. Nick Bilton, *Disruptions: Data Without Context Tells a Misleading Story*, N.Y. TIMES (Feb. 24, 2013), http://bits.blogs.nytimes.com/2013/02/24/disruptions-google-flu-trends-shows-problems-of-big-data-without-context/.

51. *See* BAKER, *supra* note 43, at 89–90. During the Obama 2008 Presidential campaign, for example, big data was used to identify 75% of swing voters on three key issues, enabling the more efficient spending of vast amounts of advertising money. *Id.* at 89–90.

52. *Id.* at 116.

Umbria, Howard Kaushansky, says "We're providing qualitative research, not quantitative. . . . It's directional. It gives early indications of where things are going."[53] However, it remains to be seen whether certain problems of law and policy, such as how to predict the bad acts of potential lawbreakers before they happen, can be solved by methods which communicate no theory of causal understanding.

C. *Predictive Systems and the Dream of Total Knowledge*

Prediction in criminal justice is an old idea, used for decades in various contexts such as parole risk assessments, phrenology, and sentencing.[54] At the outset, it is useful to distinguish between actuarial and clinical methods of prediction. Clinical methods of prediction "rely on subjective expert opinion," such as expert psychiatric testimony, to assess individuals for criminal characteristics.[55] On the other hand, actuarial methods in criminal law seek to establish "statistical correlations between group traits and group criminal offending rates."[56] Actuarial techniques in criminology have been around at least since the 1930s, when they were first used in parole prediction, and have been cyclically in and out of vogue ever since.[57] Since 9/11, however, the actuarial approach has been turbocharged, both by an infusion of data resulting from the digitization and monitoring of everything, and by an infusion of method with big data analytical tools.[58] Naturally, law enforcement agencies are charging ahead to find ways to incorporate big data into crime prediction.

Predictive systems built on big data mark a turn from individualized analysis to event-based analysis.[59] In individualized analysis, surveillance data is used to provide evidence against someone already under suspicion.[60] For example, the total transparency of banking records allows the police to see the large cash withdrawal, helping to corroborate other evidence. Event-based analysis focuses on identifying patterns by correlating data with negative events (like prior terrorist attacks), then seeks to apply those correlations in reverse, predictively, to individuals or groups.[61] Such a system, for example, might correlate certain words in Facebook posts with potential school shootings, allowing police to scrutinize or arrest a list of individuals who fit a

53. *Id.* at 114.
54. *See generally* BERNARD E. HARCOURT, AGAINST PREDICTION 47–107 (2007).
55. *Id.* at 17.
56. *Id.* at 18.
57. *Id.* at 39.
58. *See* BAKER, *supra* note 43, at 123–53.
59. *See* CHRISTOPHER SLOBOGIN, PRIVACY AT RISK 191 (2007).
60. *See id.*
61. *See id.* at 193.

threatening pattern. The former method requires the suspect's data to be accessible to law enforcement with traditional warrants. The latter method demands vast quantities of "normal" (*i.e.*, non-criminal) behavioral data against which the analytical engine can test its statistical calibrations in order to develop models of deviance.[62]

This trend probably should not surprise us. Sociologists such as William Bogard have, for decades, forecast the likely outcome of increased "panoptic" surveillance: prediction.[63] In the classic panopticon of Bentham and Foucault, not knowing whether you were being watched has a normalizing influence on behavior.[64] However, as we have seen, total surveillance has finite limits because the illusion which drives this normalizing influence begins to break down when so much data exists that it could not possibly all be scrutinized. Predictive policing seeks to battle those limits with a new conceptual framework, "not just [] a technology of surveillance, but [] a kind of surveillance in advance of surveillance, a technology of 'observation before the fact.'"[65] What drives the "technology of surveillance" today is "the fantasy" of simulation.[66] In Bogard's words:

> [t]echnologies of simulation are forms of hypersurveillant control, where the prefix "hyper" implies not simply an intensification of surveillance, but the effort to push surveillance technologies to their absolute limit. That limit is an imaginary line beyond which control operates, so to speak, in "advance" of itself and where surveillance--a technology of exposure and recording--evolves into a technology of pre-exposure and pre-recording.[67]

No discussion of predictive systems would be complete without a passing mention of the book and film *Minority Report*, wherein "pre-crime" prediction is so effective that the police feel comfortable in arresting people for what they are foreseen to do.[68] In that dystopia, the

---

62. *See* BAKER, *supra* note 43, at 7–9.

63. *See* WILLIAM BOGARD, THE SIMULATION OF SURVEILLANCE: HYPERCONTROL IN TELEMATIC SOCIETIES 3–5 (1996). Bogard uses the word "simulation," by which he means more than prediction, but prediction is a species of simulation and the terms are equivalent for the present discussion. *See id.*

64. *See* JEREMY BENTHAM, THE PANOPTICON WRITINGS 29–80 (Miran Božovič ed. Verso 1995); *see generally* MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (Alan Sheridan trans., Vintage Books 1979).

65. *See* BOGARD, *supra* note 63, at 27 (emphasis removed).

66. *Id.* at 9.

67. *Id.* at 4 (emphasis removed).

68. *See* PHILIP K. DICK, THE MINORITY REPORT (1956); MINORITY REPORT (Twentieth Cent. Fox 2002).

prediction relies on clairvoyants, not computers. In ours, surveillance-fed predictive systems are now being used in a variety of contexts, both commercial and governmental. Predictive systems can take a variety of forms, ranging from individualized predictions based on individual biometric cues, to profiling based on group attributes gleaned from past behaviors, to more generalized "high crime area" targeting.

There are simply too many such programs to mention them all, much less discuss each fully. However, one recent exemplary program is the expanded TSA pre-flight check system, an expanded version of the controversial "no-fly" list.[69] This unnamed and unannounced program purports to "prescreen" travelers before they come to the airport by matching passport and other identity documents with a number of private and governmental databases, such as those maintained by the IRS, state law enforcement, airline frequent flyer programs, and credit risk scoring agencies.[70] Precisely what databases will be searched has not been divulged.[71] The goal of the program is to categorize passengers by "risk level" to receive higher or lower scrutiny once they arrive at the airport.[72]

Another typical program is the DHS Future Attribute Screening Technology (FAST) project, which assesses the future crime risk of individuals by collecting biometric behavioral data such as cardiovascular signals, pheromones, skin conductivity, eye blink rate, and respiratory patterns using an array of sensors, video, and audio recordings.[73] The technology was tested publicly in an undisclosed location in 2011.[74] According to the FAST privacy assessment, "The future time horizon can range from planning an event years in advance to planning to carry out the act immediately after passing through screening. The consequences to the actor (perceived as either positive or negative) can range from none to being temporarily detained to deportation, prison, or death."[75]

---

69. Susan Stellin, *Security Check Now Starts Long Before You Fly*, N.Y. TIMES, Oct. 21, 2013, *available at* http://www.nytimes.com/2013/10/22/business/security-check-now-starts-long-before-you-fly.html.

70. *Id.*

71. *See id.*

72. *Id.* ("'I think the best way to look at it is as a pre-crime assessment every time you fly,' said Edward Hasbrouck . . . [of] the Identity Project.").

73. See *Future Attribute Screening Technology (FAST) Project FOIA Request*, EPIC, http://epic.org/privacy/fastproject/; U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT 3 (2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_st_fast.pdf.

74. *Privacy and Consumer Profiling*, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/profiling/ (last visited Dec. 17, 2013).

75. U.S. DEP'T OF HOMELAND SEC., PRIVACY IMPACT ASSESSMENT FOR THE FUTURE ATTRIBUTE SCREENING TECHNOLOGY (FAST) PROJECT 2 (2008), *available at* http://www.dhs.gov/

According to a 2009 PBS story, the NSA is attempting to build sophisticated artificial intelligence and big-data-driven query systems capable of answering predictive questions about future world events, or even the future actions of individuals or groups.[76] Incorporating vast amounts of data from public and private sources, including a database of the world's newspapers, the system is dubbed AQUAINT, which stands for "Advanced QUestion Answering for INTelligence."[77] A later system, a so-called "Google for spies" called RIOT, has been built by intelligence contractor Raytheon for use by national security entities.[78] RIOT captures social networking data from sites such as Twitter and Facebook and constructs associational graphs of individuals' relationships, then allows crime or intelligence analysts to predict future movements and behaviors.[79]

Federal intelligence and security agencies are not the only users of predictive threat systems. A Memphis police department program begun in 2006 called Blue CRUSH, built on IBM analytics software, uses statistical modeling of past crime data to identify "hot spots."[80] Police are then directed to these hot spots to conduct sweeps, make arrests, and display a heightened presence to deter crime.[81] The apparent successes of the program in reducing crime were heralded by law enforcement and big data systems-builders alike.[82] However, an internal audit in 2011 determined that 79,000 police memos recording potential crimes had not been reported, and that further review of these memos would likely cause the crime rate to go "way up," calling into question many of the gains of the program.[83] Similar such systems have been installed in

---

xlibrary/assets/privacy/privacy_pia_st_fast.pdf. A later assessment minimizes these concerns, stating "FAST is not intended to provide 'probable cause' for law enforcement processes, nor would the technology replace or pre-empt the decisions of human screeners." *Id.*

76. James Bamford, *The New Thought Police: The NSA Wants to Know How You Think-Maybe Even What You Think*, PBS (Jan. 1, 2009), http://www.pbs.org/wgbh/nova/military/nsa-police.html.

77. *Id.*

78. Ryan Gallagher, *Software that Tracks People on Social Media Created by Defence Firm,* GUARDIAN, Feb. 10, 2013, http://www.theguardian.com/world/2013/feb/10/software-tracks-social-media-defence.

79. *Id.*

80. *Memphis Police Department Reduces Crime Rates with IBM Predictive Analytics Software*, IBM, *available at* http://www-03.ibm.com/press/us/en/pressrelease/32169.wss (last visited Dec. 17, 2013) [hereinafter *Memphis Police Department Reduces Crime Rates*].

81. *See* DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE 138–44 (2011).

82. *See Memphis Police Department Reduces Crime Rates*, *supra* note 80.

83. Amos Maki, *Crimes Lurk in Memphis Police Department Memos*, THE COMMERCIAL APPEAL (Jan. 25, 2012), http://www.commercialappeal.com/news/2012/jan/25/crimes-lurk-in-police-memos/?partner=RSS.

numerous cities nationwide, from Los Angeles to Richmond.[84]

III. TECHNOLOGICAL AND METHODOLOGICAL EFFECTIVENESS OF THE PREDICTIVE PARADIGM

An underlying presumption of predictive systems is that they function effectively now or will do so in the future. Reason tells us than an effective predictive system would need to outperform existing methods of crime prevention according to some valid metric without introducing side-effects that public policy deems excessively harmful. Moreover, our cost-benefit driven society would likely stipulate that these goals be achieved at a lower economic cost than existing methods. This section will assay the effectiveness of the predictive paradigm in view of the twin goals of performance and side-effects, focusing primarily on technological issues. Part IV will then address side-effects, barriers, and harms of a legal and privacy nature, most of which hinge on a concept of reasonableness and probability that predictive systems do not satisfy technologically.

A. *Performance: Data Quality, the Base Rate Fallacy, and Automation Bias*

To conceptualize the performance problem, we will first examine some of the successes and failures of recent predictive systems. Unfortunately, the successes have been troublingly hard to locate and quantify. Recently, revelations about NSA eavesdropping programs have prompted congressional hearings into the effectiveness of the programs in stopping terrorist activity. Initially, it was claimed by the Obama Administration that fifty-four terrorist plots had been thwarted by the NSA's metadata collection program, which is backed by big data analytics.[85] However, in recent testimony before Congress, NSA Director Gen. Keith Alexander was pressed by Senator Leahy on that metric and forced to admit that only one case, wherein a Somalian immigrant donated money to al-Shabaab, could be directly tied to the program.[86] Director of National Intelligence James Clapper then advocated a different metric, than the number of plots foiled, the "peace

84. *See* Robert L. Mitchell, *Predictive Policing Gets Personal*, COMPUTERWORLD (Oct. 24, 2013), http://www.computerworld.com/s/article/9243385/Predictive_policing_gets_personal.

85. Yochai Benkler, *Fact: The NSA Gets Negligible Intel from Americans' Metadata*, GUARDIAN, Oct. 8, 2013, http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence.

86. *Id.*

of mind" metric.[87] He explained that, after the Boston Marathon bombing, agencies were able to use the database to see "whether there was or was not a subsequent plot involving New York City."[88] Since no other conspirators were found, and no attack occurred, the program succeeded according to Clapper's new metric.[89]

Looking for results in other predictive systems also reveals few successes. The Suspicious Activity Reporting (SAR) program allows law enforcement, citizens, and others to increase scrutiny on individuals they deem as suspicious.[90] The individuals are added to a database called Guardian, triggering additional information collection and assessment algorithms.[91] As of December 2010, 161,948 SARs were in the database, of which 103 had been turned into full investigations, leading to five arrests and no convictions.[92] The Memphis BlueCRUSH program may owe its apparent early success to thousands of uncounted incidents. Other critics have contended that predictive policing software vendor PredPol, which sells risk-terrain modeling tools to police departments, has little evidence that its programs are effective, and no way of proving that its "crime reduction" statistics are not merely shifting crime to other, uncounted precincts.[93]

To go along with the lack of specific successes, there have been several egregious failures to predict and to control abuses. The Boston bombing case is the most notable recent example, but others are easy to locate. The widely reviled "no-fly list" incorrectly tags about 1500 airline passengers per week.[94] Some notable examples include an airline pilot who was detained over 80 times in a year, an Army major, two U.S. senators, and a 4-year-old.[95] Maryland state police used their

87. Ken Dilanian, *NSA Says It Considered Collecting Phone Call Location Data*, L.A. TIMES (Oct. 2, 2013), http://www.latimes.com/nation/la-na-nsa-surveillance-20131003,0,2535208.story.

88. *Id.*

89. *Id.*

90. *See* DANA PRIEST & WILLIAM M. ARKIN, TOP SECRET AMERICA: THE RISE OF THE NEW AMERICAN SECURITY STATE 144–47 (2011).

91. *Id.*

92. *Id.* at 148.

93. *See* Darwin Bond-Graham & Ali Winston, *All Tomorrow's Crimes: The Future of Policing Looks a Lot Like Good Branding*, S.F. WKLY., Oct. 30, 2013, http://www.sfweekly.com/2013-10-30/news/predpol-sfpd-predictive-policing-compstat-lapd/full/ (citing criminologist Ed Schmidt, who believes there is little data supporting the effectiveness of predictive policing); Tim Cushing, '*Predictive Policing' Company Uses Bad Stats, Contractually-Obligated Shills To Tout Unproven 'Successes*,' TECHDIRT (Nov. 1, 2013), *available at* http://www.techdirt.com/articles/20131031/13033125091/predictive-policing-company-uses-bad-stats-contractually-obligated-shills-to-tout-unproven-successes.shtml.

94. Danielle Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1256–57 (2008).

95. *Id.* at 1274–75; *see also* Valerie Hauch, *Disabled Woman Denied Entry to U.S. After*

access to data available through state-federal "fusion centers" to infiltrate and watch several political groups, classifying 53 activists—including two Catholic nuns—as terrorists.[96] These examples leave aside the litany of problematic automated decision-making systems used in administrative contexts such as Colorado's Medicaid and food stamp benefit program or the "deadbeat parent" locator program, many of which apply rules to individuals using similar techniques to crime-prediction systems.[97]

The reason for such dubious success rates is that predictive system performance is hindered on many levels, ranging from low quality data to flawed methodology to poor auditing and supervision. The first and most obvious barrier to predictive system performance is inaccurate input data. In part because of the constraints on commercial data gathering, the data shared through commercial websites is often "anonymized" in accordance with website policies to satisfy both consumers and commercial privacy laws.[98] Later, the data is de-anonymized by commercial aggregators, who have fewer constraints and an interest in knowing the specific individual.[99] This process is relatively simple, but often erroneous in details; for example, the aggregation might know a person's name, but be completely wrong about his age, race, or shopping habits. This problem is bad enough that at least one data broker, Acxiom, has recently released a tool on its website allowing consumers to correct erroneous data.[100] While the ramifications of such mistakes are arguably lower in commercial settings, commercial data is no longer used only commercially: the NSA and law enforcement agencies tie into these databases and use them to feed criminal prediction systems, magnifying the harms of data errors and flawed interpretations.[101] Moreover, the likelihood of such data

---

Agent Cites Supposedly Private Medical Details, STAR, Nov. 28, 2013, http://www.thestar.com/news/gta/2013/11/28/disabled_woman_denied_entry_to_us_after_agent_cites_supposedly_private_medical_details.html.

96. David C. Gray & Danielle Keats Citron, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 81 (2013).

97. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1256–57 (2008).

98. *See* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1703–06 (2010), *available at* http://www.uclalawreview.org/pdf/57-6-3.pdf.

99. *See id.*

100. Natasha Singer, *A Data Broker Offers a Peek Behind the Curtain*, N.Y. TIMES, Aug. 31, 2013, http://www.nytimes.com/2013/09/01/business/a-data-broker-offers-a-peek-behind-the-curtain.html.

101. *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST, June 6, 2013, http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/.

errors is even greater in non-structured data collection (*e.g.*, NSA systems that glean data directly from internet pipelines and attempt to decrypt, sort, and re-identify its source).

An intrinsic limitation of predictive systems that is often unrecognized or glossed over in discussions of effectiveness is the error rate—all predictive systems are wrong sometimes, and the algorithms must be "tuned" to find the right balance between false positives and false negatives.[102] In a criminal prediction context, a false negative is when the system mistakenly allows a guilty individual to slip through. However, a false positive is when an innocent person is suspected of being guilty, the consequences of which are unnecessary violations of that person's privacy and liberty interests. The true problem of false positives comes from a statistical phenomenon known as the "base rate fallacy," which emerges in situations where a large number of "normal" profiles have to be scrutinized, but the incidence of the target profile is very small.[103] This fundamental statistical limitation dictates that even an unrealistically accurate predictive model will likely create unacceptable error rates in a large population with a few rare matches.[104]

Security expert Bruce Schneier describes the problem with an example of a system designed to spot terrorist plots that is 99% accurate as to false-positives and 99.9% accurate as to false negatives. Assuming a volume of a trillion scrutinized events (ten calls, emails, web transactions, per U.S. citizen per day—likely a very low estimate), the system will create a billion false positives per day. Assuming that there are ten or so actual terrorists plotting at a given time, the resource requirements to investigate that many matches are unreasonable. Even "tuning" the algorithms to raise the false-positive accuracy to 99.9999% still creates 2,750 false alarms per day—also likely unworkable. More importantly, however, such tuning will now likely cause the system to miss a few of the 10 real plots. As a practical matter, such accuracy levels are probably unrealistic, anyway.[105] As a reality check on accuracy, the FBI considers it acceptable to make erroneous matches 20% of the time in its Next Generation Identification biometric matching program.[106]

However, human misunderstanding of the limits of automated predictive systems goes beyond a misapprehension of statistical theory.

---

102. Bruce Schneier, *Why Data Mining Won't Stop Terror*, WIRED, Mar. 9, 2006, http://www.wired.com/politics/security/commentary/securitymatters/2006/03/70357.

103. *Id.*

104. *Id.*

105. *See id.*; *see also* SLOBOGIN, *supra* note 59, at 194–95.

106. *EPIC FOIA - FBI Says 20% Error Rate Okay for Facial Recognition*, EPIC.ORG (Oct. 4, 2013), http://epic.org/2013/10/epic-foia---fbi-says-20-error-.html.

People have an intrinsic trust in computer-based operations generally—and machine computation specifically—which lacks a rational basis. Computer scientist Jaron Lanier has noted how readily humans will adapt their own expectations and behaviors to conform to the quirks of automated systems, often without noticing their tacit acceptance of new limitations.[107] In decision systems specifically, study after study across numerous disciplines has confirmed the phenomenon of "automation bias [that] occurs in decision-making because humans have a tendency to disregard or not search for contradictory information in light of a computer-generated solution that is accepted as correct."[108] This phenomenon occurs in part because of trust in automation and in part because, over time, people become unpracticed at applying the rules that systems help them automate.[109] In other words, humans learn by repeatedly practicing the menial rules that predictive systems automate for them.[110] When the time comes to review the machine's decisions, they lack both the confidence and the experience to overrule the machine's mistakes or to second-guess its decisions.[111] On its face, it seems a plausible claim that predictive crime systems would not be problematic because they are mixed-mode—subject to human review before any action is taken. Automation bias and its underlying causes are important to understand because they show that even mixed-mode systems have little chance of reducing errors in decision making or mitigating their consequences, even when malfunction is suspected by a supervising human.[112] Thus, "[a]utomation bias effectively turns a computer program's suggested answer into a trusted final decision."[113]

B. *Side-Effects: Bias and Norm-Shaping*

Aside from the concern that such systems may be too resource-burdensome to implement, one expert critic has noted, "Actuarial

107. *See* JARON LANIER, YOU ARE NOT A GADGET: A MANIFESTO 9–13 (2010) [hereinafter LANIER, YOU ARE NOT A GADGET].

108. M.L. Cummings, Automation Bias in Intelligent Time Critical Decision Support Systems 1 (unpublished manuscript, *available at* http://web.mit.edu/aeroastro/labs/halab/papers/CummingsAIAAbias.pdf) (last accessed Dec. 17, 2013).

109. *Id.* at 2.

110. *See* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1272 (2008).

111. *Id.*

112. *Id.* at 1271–72.

113. *Id.* at 1272; *see also* Sabrina A. Lochner, *Saving Face: Regulating Law Enforcement's Use of Mobile Facial Recognition Technology & Iris Scans*, 55 ARIZ. L. REV. 201, 220 (2013) (noting that the MORIS facial recognition system "seemingly creates a de facto lineup in the field where police must identify a person from three photographs returned after a database search" and recommending that police lineup procedures be used to avoid suggestive or biased results).

methods in the criminal justice field produce hidden distortions with significant costs for society."[114] One such distortion emerges from the ideological imprint inevitably left on a system during design, when policy rules are crafted into code. There are two aspects to this distortion which emerge at different levels of coding—research agenda bias and policy bias.

Long before specific rules and policies are encoded into a given automated predictive system, basic choices must be made by the tools vendors that develop big data analytics systems and software. The ultimate conclusion of predictive policing—that macro-level events (*i.e.*, human behaviors) can be predicted given enough data points and a sophisticated enough model—requires an almost ideological presumption of determinism.[115] While this presumption is overt among the leaders of Silicon Valley companies today,[116] it may or may not be shared by the population at large. Proponents have had difficulty in questioning the core principles of the "research agenda" of big data, acknowledging the validity of methodological critiques, and developing strategies to minimize bias.[117] The consequences have shown themselves through numerous high-profile research scandals and a general questioning of the validity of much scientific research.[118]

Before rules even begin to be coded, lead up activities can leave an impression. Early activities, such as the selection of initial databases to incorporate and search, the filtering and converting of data from those databases, and the type of data analysis to perform,[119] leave subtle traces. As one critic puts it: "Mathematicians model misunderstandings of the world, often using the data at hand instead of chasing down the hidden facts."[120] Biases which may have existed in those feeder databases, now masked by another layer of abstraction, combine with other biases to compound problems. Those early activities, in turn, create spurious correlations and errors which human analysis (again, potentially biased) must discount or emphasize. The recognition of patterns in data is "informed by values about what makes a pattern and

---

114. HARCOURT, *supra* note 54, at 21.

115. *See* Julie Cohen, *What Privacy is For*, 126 HARV. L. REV. 1904, 1924 (2013).

116. *See* JARON LANIER, WHO OWNS THE FUTURE? 165 (Kindle ed. 2013).

117. *See* Cohen, *supra* note 115, at 1924; *see also* John Timmer, *Is It Time to Up the Statistical Standard for Scientific Results?* ARSTECHNICA, Nov. 12, 2013, http://arstechnica.com/science/2013/11/is-it-time-to-up-the-statistical-standard-for-scientific-results/#p3 ("Research fraud is rising, but even studies that were performed properly sometimes either can't be reproduced or appear to suffer from bias.").

118. S*ee* David H. Freedman, *Lies, Damned Lies, and Medical Science*, ATLANTIC MONTHLY, Nov. 2010, at 40, *available at* http://www.theatlantic.com/magazine/archive/2010/11/lies-damned-lies-and-medical-science/308269/; *see also* Timmer, *supra* note 117.

119. *See* BAKER, *supra* note 43, at 83–89.

120. *Id.* at 215.

why."[121]

All of this occurs before predictive models are codified by dovetailing the patterns into more general public and administrative policy rules. To be sure, all policy-making is, in a sense, an effort to craft underlying values into administrable rules. However, during that process, programmer codification of the rules of complex policies may be biased or in error, ultimately amounting to hidden new policy.[122] Over time, there is even the worry that rules that are easier to code into automation systems may be self-selected and thus have a reverse influence on the definition of administrative policies, in essence the ultimate negative consequence of automation bias.[123] Even a seemingly simple act, such as setting initial tolerances for false positive and negatives, is often an obscure policy decision.

Once a predictive system has been implemented, other subtle side effects may emerge. The process of predictive simulation ultimately makes the model the "signifier of reference"—it reverses the normal flow wherein reality tests the model and instead makes the predictive model the validator of reality.[124] In the first place, this is a problem because any biases in the model introduced in the design process tend to be magnified by self-reinforcement. However, even relatively unbiased models may be plagued by self-reinforcement: police look for crime where the model tells them to look, and each time they find it the model seems more valid—much like the proverbial drunk who only looks for his keys under the streetlight because that is where the light is.[125] There is significant evidence that this kind of observation bias is already happening in existing predictive systems: San Francisco Police Department chief information officer Susan Merritt decided to proceed with caution, noting "In L.A. I heard that many officers were only patrolling the red boxes [displayed by the PredPol system], not other areas. People became too focused on the boxes, and they had to come up with a slogan, 'Think outside the box.'"[126]

---

121. Cohen, *supra* note 115, at 1924.

122. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1279 (2008) (describing the Colorado CBMS system and how "programmers changed hundreds of established rules when encoding them into the system, [with the consequence that] CBMS also articulates new rules. . . .").

123. *Id.* at 1297–98; *see also* Nate Anderson, *TSA's Got 94 Signs to ID Terrorists, But They're Unproven by Science*, ARSTECHNICA (Nov. 13, 2013), http://arstechnica.com/tech-policy/2013/11/despite-lack-of-science-tsa-spent-millions-on-behavioral-detection-officers/.

124. *See* WILLIAM BOGARD, THE SIMULATION OF SURVEILLANCE: HYPERCONTROL IN TELEMATIC SOCIETIES 72 (1996).

125. BAKER, *supra* note 43, at 216.

126. Darwin Bond-Graham & Ali Winston, *All Tomorrow's Crimes: The Future of Policing Looks a Lot Like Good Branding*, S.F. WEEKLY, Oct. 30, 2013, http://www.sfweekly.com/2013-10-30/news/predpol-sfpd-predictive-policing-compstat-lapd/full/.

Consider an extended example: Say that big data analysis tells the police that there is a minor correlation between speeding and drug-trafficking. As a result, speeding becomes a profiled characteristic in the predictive model. However, the correlation may occur only because traffic stops enable police to search the car, not because speeders tend to be drug traffickers. The "model" works: by stopping speeders, police do indeed arrest more drug traffickers, in line with the model's correlation. Over time, this leads to the conclusion that speeders traffic drugs, and the increased policing of speeders becomes a police focus.

One reason this happens is that the models tend to be evaluated according to their success rate in finding the crime, rather than their success rate in reducing the profiled crime and its societal policing costs.[127] According to one critic, even predictive systems with an accurate model suffer from a flawed assumption: that those in the predicted "profile" group react to policing efforts similarly to those not in the group.[128] In populations where they do not, policing the target group may not reduce the incidence of the targeted crime and may even increase it.[129] In our hypothetical, the undesirable result is that police have increased the resources devoted to policing speeders in service of a non-predictive correlation that merely regurgitates its own numbers back at a higher economic cost to society. In addition, society now has an unnecessary, and erroneous, group bias against speeders as being drug traffickers (*i.e.*, norms have been reshaped in service of the model, rather than being reflected in the model). Thus, even facially effective predictive models may have significant, negative societal side-effects.

IV. SIDE EFFECTS: PRIVACY HARMS

The right to privacy, though not specifically scripted in the Bill of Rights, emerges as a "penumbra" emanating from the First, Fourth, and Fifth Amendments.[130] Typically, the Fourth Amendment (and, to a lesser extent, the Fifth) has governed privacy in a criminal procedure context, while the First Amendment has sanctified privacy in intellect, association, communication, and the exploration of new ideas.

A. *Fourth Amendment*

In theory, the Fourth Amendment guards against unnecessarily intrusive breaches of individuals' privacy for the purposes of

127. HARCOURT, *supra* note 54, at 139–40.
128. *Id.* at 22–23.
129. *Id.* at 24.
130. Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

investigating or preventing criminal activities, serving "as a bulwark against law enforcement's teleological tendency toward a surveillance state."[131] The foundational concept in Fourth Amendment jurisprudence is "probable cause," and traditionally searches of persons, documents, and homes require a warrant in which the government must articulate a specific set of facts showing that it is reasonable to believe the targeted person has committed a crime.[132] Over time, however, that relatively rigorous standard has been relaxed for certain kinds of searches. For example, police may "stop and frisk" people if they have a "reasonable suspicion" that they may be engaged in criminal activity.[133] Other "special" kinds of searches, such as those inside a school, have gradually come to fall under this relaxed standard.[134] Much electronic information is accessible under an even lower standard, "relevance" to an investigation, which allows law enforcement to utilize subpoenas to accomplish most routine suspicion-less data gathering.[135] Furthermore, the development of the concomitant third-party doctrine and the "reasonable expectation of privacy" doctrine enables many electronic activities to be labeled "non-private," exempting them from even the low "relevance" standard.[136] There are so many exceptions to the warrant process now that individualized suspicion is no longer required for most types of searches, short of physical searches of one's home.[137]

While the widespread use of surveillance technology by federal agencies against a largely guiltless populace may, in itself, be legally questionable in light of the Fourth Amendment's prohibition against general warrants, that question will remain unexplored here. Even if total surveillance is legally justifiable, however, there remain several related questions concerning the scope of the use of transactional data in big data analytics and in criminal prediction.

It is worth noting that the term "probable cause" unavoidably requires a forward-looking viewpoint. Since probable cause analysis must be performed prospectively, the "probability" of the government finding what it asked to look for is inherent in the concept. Thus, what is at issue is not so much the use of predictive probabilities *per se*, but the balance between two aspects of the analysis: the quality and specificity of the prediction versus the depth and breadth of the privacy intrusion. This is, in essence, the proportionality principle which *Terry* purported to apply in order to arrive at the lower "reasonableness"

131. Gray & Citron, *supra* note 96, at 92.
132. JON L. MILLS, PRIVACY: THE LOST RIGHT 47 (2008).
133. Terry v. Ohio, 392 U.S. 1, 27 (1968).
134. New Jersey v. TLO, 469 U.S. 325 (1985).
135. MILLS, *supra* note 132, at 47–48.
136. *See id.* at 281–82.
137. DANIEL J. SOLOVE, NOTHING TO HIDE 126 (2011).

standard for stop and frisk situations.[138]

It is also helpful to distinguish two related understandings of "privacy intrusion" in the Fourth Amendment context. One way of understanding the privacy interest at stake in non-particularized searches is to consider the "unjustified burden" to those who would be searched unnecessarily.[139] Under this conception, mere information analysis is fair game because, so long as the person whose data is reviewed does not know about it, there is no violation of privacy because there is no troublesome intrusion.[140] Judge Richard Posner espoused this theory in a recent op-ed piece.[141] However, a related but more subtle way of understanding the privacy interest is as a "dignity interest," which perceives the search as an offense to dignity whether or not anyone knows about it.[142] Conceiving of the search this way would mean that using automated agents to predict behaviors qualifies as an offense to dignity and thus requires authorities to apply some form or proportionality review. The two views are not necessarily exclusive.

Professor Slobogin has argued that the jurisprudence that has emerged around the proportionality principle of *Terry* is flawed because the principle is applied selectively to special cases instead of uniformly to all Fourth Amendment analysis.[143] If properly applied to group searches, for example, the principle would dictate that the search yield a positive result for a substantial percentage of those searched.[144] This

---

138. *Terry*, 392 U.S. at 21.

139. LAWRENCE LESSIG, CODE: AND OTHER LAWS OF CYBERSPACE, VERSION 2.0, at 211 (2006), *available at* http://codev2.cc/download+remix/Lessig-Codev2.pdf.

140. *Id.*; *see also* Mike Masnick, *Mike Rogers: You Can't Have Your Privacy Violated If You Don't Know About It*, TECHDIRT (Oct. 30, 2013), http://www.techdirt.com/articles/20131029/18020225059/mike-rogers-you-cant-have-your-privacy-violated-if-you-dont-know-about-it.shtml (Recently, some have called this the "Rogers Doctrine," after Rep. Mike Rogers, who stated during recent NSA hearings that "You can't have your privacy violated if you don't know your privacy is violated.").

141. Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html.

> The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.

Id.

142. LESSIG, *supra* note 139, at 211–12.

143. SLOBOGIN, *supra* note 59, at 22–23.

144. LESSIG, *supra* note 139, at 212.

analysis is relevant here because widespread automated review of the private data of largely guiltless individuals is what might be considered a dragnet search that has low predictive specificity and quality, thus violating the dignity interest.[145] However, even if the argument can be made that the data is not private because of the reasonable expectation and third-party doctrines,[146] a significant proportion of false positives may mean that the privacy intrusion is too great to justify the results under the "unjustified burden" conception of the privacy interest.[147]

Considering some of the predictive crime models from the proportionality review perspective can be instructive. Take, for example, predictive models that direct police to "crime hot spots." Are officers able to stop and search people because the prediction itself satisfies some aspect of reasonable suspicion? It seems so. In *Illinois v. Wardlow*, the Supreme Court ruled that the moniker "high crime area" was a significant enough factor in the totality of the circumstances analysis of reasonable suspicion that it could be one of only two factors to justify a stop-and-frisk (the other being flight by the suspect upon seeing the police nearby).[148] A recent police stop captured on video in Philadelphia shows how quickly the second factor in the totality of the circumstances test can become merely nominative.[149] The video shows two men who were detained by police because they greeted another person while walking down the street.[150] According to the officers, greeting others in the high crime neighborhood was a sufficiently abnormal behavior to be worthy of suspicion.[151]

In *Wardlow*, the labeling of the area as "high crime," presumably justified by retrospective crime data, is somewhat different from the prospective designation of an area as likely to have a 10% increased chance of burglaries today, as determined by the systems in use in Memphis and other cities.[152] However, the parallels to predictive hot-spot modeling are clear: if the mere label of "high crime area" is almost completely sufficient for reasonable suspicion, a computerized

145. *Id.* at 211.

146. Slobogin would argue that both of these doctrines are flawed because they fail to conduct the proportionality analysis properly. *See* SLOBOGIN, *supra* note 59, at 31–32.

147. *See* LESSIG, *supra* note 139, at 211.

148. Illinois v. Wardlow, 528 U.S. 119, 124 (2000); *see also* United States v. Cortez, 449 U.S. 411, 417–18 (1981) (discussing the totality of the circumstances test).

149. *See* Josh Moyo, *Police Unlawful Harassment and Racial Profiling 9/27/13 Philly, Pa*, YOUTUBE (Sept. 30, 2013), http://www.youtube.com/watch?v=G4exZ-jXgWE; *see also* Morgan Winsor & Rande Iaboni, *16-minute Video of Philly Cops in Controversial Stop Sparks Criticism, Probe*, CNN (Oct. 17, 2013), http://www.cnn.com/2013/10/17/us/video-police-stop-philadelphia/ (link to full video in article).

150. Winsor & Iaboni, *supra* note 149.

151. *Id.*

152. *See Memphis Police Department Reduces Crime Rates*, *supra* note 80.

prediction will likely carry at least as much weight.

Considering *Wardlow* and its effect on subsequent police behavior, "area" crime prediction models have the potential to significantly impact individuals' privacy when they live or work in the targeted area. Behaviors as innocent as greeting someone may become suspicious, causing widespread, unjustified harassment of innocent persons and substantial damage to personal dignity, as is evident from the Philadelphia video.[153] These models should fail on proportionality review and on both the unjustified burden and dignity interest conceptions of the Fourth Amendment privacy guarantees.

A second predictive context is prediction based on shared group attributes, or profiling. Courts have generally been receptive to the idea of using shared group attributes as the basis for a police stop. In *United States v. Sokolow*, the Supreme Court upheld the DEA's use of a "drug courier profile" that consisted of several factors which, in and of themselves, were neither criminal nor suspicious.[154] The Court did not address the specific constitutionality of a predictive profile as such, but acknowledged that such a profile was not inappropriate merely by being probabilistic in nature and was allowable under a totality of the circumstances analysis.[155]

For the purposes of the present discussion, the relevant group attributes would have been culled from large volumes of data using big data analytics, and thus would possess value only as statistical correlation, not causal theory. On its face, the determinative issue in a proportionality analysis would seem to be how well the group attributes predict the crime (*i.e.*, finding most of the criminals with the least burden on the innocent). While false negatives are less of a problem for privacy, a large number of false positives should fail the proportionality review.

Interestingly, the Court in *Sokolow* lacked any objective evidence of the profile's predictive value, and looked dimly on the Ninth Circuit's belief that any was necessary.[156] This is troubling in light of the

---

153. *See* Winsor & Iaboni, *supra* note 149.

154. United States v. Sokolow, 490 U.S. 1, 8–9 (1989) (Two of the factors were paying cash for an airplane ticket and visiting Miami from Honolulu in July for only 48 hours).

155. *Id.* at 8–10

156. *Id.* at 6.

> The majority [of the Ninth Circuit judges] believed that such characteristics, "shared by drug couriers and the public at large," were only relevant if there was evidence of ongoing criminal behavior and the Government offered "[e]mpirical documentation' that the combination of facts at issue did not describe the behavior of 'significant numbers of innocent persons." Applying this two-part test to the facts of this case, the majority found that there was no evidence of ongoing criminal behavior, and thus that the agents' stop was

methodological questions raised earlier, especially the tendency for predictive systems to become self-reinforcing when officers begin to detain, disproportionately to other populations, those who fit the profile. This apparent success will further validate the use of such profiling in reasonable suspicion analysis.

No Supreme Court case seems to have dealt with the question of reasonable suspicion emerging purely and solely from a probabilistic system. However, it is clear from *Sokolow* that a profile, whether or not it has predictive value, may become sufficient for reasonable suspicion when added to some feeling, intuition, or observation the officer makes.[157] This suggests that a seemingly objective criterion is in fact much more prone to bias than it seems at first blush.[158] In fact, the lack of a case on the matter suggests not that the Court would prohibit a search where reasonable suspicion was based on pure probability, but instead that it is nearly always possible for an officer to find a feeling, intuition, or observation to purify a profile, before or after the fact.

How courts will ultimately rule on many of these questions is unknown, but it should be clear that predictive crime systems have the capability to factor significantly into future Fourth Amendment analysis. If those models are not predictively accurate, there will be harms to the privacy interests of individuals erroneously caught in their dragnet. Unless courts or legislatures undertake a substantial policy shift, few barriers remain in Fourth Amendment jurisprudence to hinder these damaging outcomes.

B. *First Amendment*

At first blush, it may be difficult to see what the First Amendment has to do with predicting criminal behavior. After all, the First Amendment is supposed to guarantee that the government does not restrict certain expressive activities—speech, association, belief, and religion—unnecessarily.[159] The First Amendment protects intellectual inquiry and allows individuals to find and discuss ideas with like-minded people; these activities are protected because they are considered essential to a functioning democracy.[160] However, death threats and conspiracy to commit murder—criminal in nature—are not

---

impermissible.

Id. (internal citations omitted).

157. *Sokolow*, 490 U.S. at 10.

158. *See* Charles L. Becton, *The Drug Courier Profile: "All Seems Infected That th' Infected Spy, As All Looks Yellow to the Jaundic'd Eye*," 65 N.C. L. REV. 417, 429–30 (1987).

159. *See* U.S. CONST. amend. I.

160. SOLOVE, *supra* note 137, at 27.

protected First Amendment behaviors.

In light of this, to paraphrase a common question, "Why do suspected criminals need protection against search, surveillance, and predictive analysis at all? If the systems work some of the time, why not use them? Those with nothing to hide have nothing to fear." Traditionally, the Fourth Amendment has been viewed as governing criminal procedure by regulating the boundaries of government conduct, and the First Amendment as governing a different thing altogether.[161] Yet, it would be narrow thinking to conclude that the Fourth Amendment has nothing to do with free speech. In fact, to understand the Fourth Amendment's common roots with the First Amendment is to understand the foundational harm of predictive systems.[162]

In the eighteenth century, the British government prosecuted thousands of individuals for sedition in order to quell dissent.[163] General warrants were common at the time and, in one famous case, were used to search the home and papers of John Wilkes, the anonymous publisher of a pamphlet criticizing the king.[164] Widespread celebration in the colonies ensued when Wilkes won his case by challenging the validity of the warrant.[165] Such events were the historical backdrop of the First Amendment right to speech, but also the Fourth Amendment prohibition against searches by the government to see what turns up. According to one commentator, "The Fourth Amendment emerges from 'a tradition that has more to do with protecting free speech than with regulating the police.'"[166]

To turn Justice Douglas's famous statement in Griswold on its head, it may be fairer to say that the necessity of intellectual privacy to a functioning democracy creates the penumbra that is the First and Fourth Amendments.[167] For this reason, Professor Solove believes that "The First Amendment should serve as an independent source of criminal procedure,"[168] especially in light of the limited usefulness of the Fourth Amendment in protecting informational privacy.[169] In other words, systems of information gathering and prediction that target criminal behavior should be explicitly analyzed with reference to their First Amendment effects on the populace as a whole.[170]

---

161. *Id.* at 146.

162. *Id.* at 147.

163. *Id.*

164. *Id.*; *see* Wilkes v. Wood, (1763) 98 Eng. Rep. 489 (K.B.).

165. SOLOVE, *supra* note 137, at 148.

166. *Id.* (citing William J. Stuntz, *The Substantive Origins of Criminal Procedure*, 105 YALE L.J. 393, 398 (1995)).

167. *See* Griswold v. Connecticut, 381 U.S. 479, 484 (1965).

168. SOLOVE, *supra* note 137, at 150.

169. *Id.* at 152.

170. *Id.*; *see also* Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV.

If First Amendment issues are appropriate to consider in the criminal prediction context, then it is critical to understand precisely how these systems, built on total surveillance, may damage democratic societies. Our society highly prizes human freedom, creativity, and uniqueness. Our desire to preserve these human qualities places them among the fundamental normative concepts in the pantheon of democratic values.[171] The Constitution recognizes that overly constraining human behavior with legal restrictions might have the effect of quelling the development of ideas at the margins of normality, and that often those borderline ideas are where progress is made in society. It is widely believed by scholars that widespread surveillance damages the ability of humans to engage in those "abnormal" behaviors because it deters people from "engaging in thoughts or deeds that others might find deviant. Surveillance thus menaces our society's foundational commitments to intellectual diversity and eccentric individuality."[172] In situations where people are constantly watched, the psychological pressure to conform to norms is extremely high, even when those watched have only a generalized idea of why they are being watched and what constitutes the "normal" behavior.[173] In short, "surveillance inclines us to the mainstream and the boring,"[174] and this shift, over time, may cause a society to lose its creativity and stagnate. The "chilling effect" doctrine of First Amendment law recognizes that, as a society, we should be suspicious of attempts to regulate speech, even borderline speech, and should err on the side of permissiveness.[175] However, scholars have only recently begun to criticize the chilling effect of widespread surveillance on First Amendment grounds, and to argue that a notion of "intellectual privacy" is needed to protect these core values against surveillance.[176] "For better and for worse . . . privacy is sponsor and guardian to the creative and the subversive."[177]

Prediction of behavior is the final extension into spatial privacy, imposing normalization by its preemption of free action.[178] Predictive

---

1934, 1951 (2013) (noting that courts are mistaken to view surveillance solely as a Fourth Amendment issue, and should also consider First Amendment values).

171. Richards, *supra* note 170, at 1946–47.

172. *Id.* at 1948; *see also, e.g.*, BENTHAM, *supra* note 64, at 29–80; FOUCAULT, *supra* note 64.

173. Richards, *supra* note 170, at 1948–49; *see generally* BOGARD, *supra* note 1, at 55–77.

174. Richards, *supra* note 170, at 1948.

175. *Id.* at 1949-50; *see also* N.Y. Times Co. v. Sullivan 376 U.S. 254, 271–72 (1964).

176. Richards, *supra* note 170, at 1950; *see also* United States v. Jones, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring).

177. Richards, *supra* note 170, at 1950 (quoting TIMOTHY MACKLEM, INDEPENDENCE OF MIND 36 (2006)).

178. *See* JULIE COHEN, CONFIGURING THE NETWORKED SELF 143, 149 (2012).

systems amplify and multiply the chilling effect of surveillance in several ways. First and most obviously, predictive systems make surveillance known to people by integrating it into systems that actually constrain their free behavior.[179] The vague instinct one is being watched becomes tangible when a person is placed on a watch list like the "no fly" list and denied access to air travel or subjected to heightened screening procedures; denied access to jobs or credit; or subjected to a "stop and frisk." As Jay Stanley of the ACLU put it, "over time, as the ramifications of big data analytics sink in, people will likely become much more conscious of the ways they're being tracked, and the chilling effects on all sorts of behaviors could become considerable."[180]

Citizens do not really know which behaviors have contributed to their placement on the heightened scrutiny list; and they do not precisely know how they were watched to be placed there.[181] However, they will self-censor to conform to an illusory model of normality—the second way predictive systems amplify the harms to First Amendment values.[182] When humans are merely watched, they will confine themselves to behaviors that they view to be un-embarrassing and relatively mainstream.[183] When humans are subjected to analysis by a predictive system built on actuarial data, they will adapt their behavior not even to that robust "normal" man or woman, but to a shallow caricature—a predictive "straw man" normal.[184] In part, this occurs because people will conform their behavior to make it more interpretable to technology, rather than demanding that technology conform to their quirks.[185] Thus, the age of prediction marks the next transition in our relationship with images.[186] The images used in prediction "now have the function of concealing the fact that reality itself is absent behind its representation."[187] The profiles created are false, but they come to have more reality than the real behaviors from which they are compiled.[188] Because the profile is guaranteed to "serve up an offender," it is "true" regardless of its accuracy, and the real

179. *Id.* at 140–41.

180. Jay Stanley, *The Potential Chilling Effects of Big Data*, ACLU BLOG (Apr. 30, 2012), https://www.aclu.org/blog/technology-and-liberty/potential-chilling-effects-big-data.

181. *Id.*

182. *Id.*

183. *Id.*

184. *Id.* (recalling his own self-consciousness about clicking on friends' updates after hearing about an applet which utilized Facebook data to rate how much people "stalked" their friends).

185. *See* LANIER, YOU ARE NOT A GADGET, *supra* note 107, at 32.

186. *See* BOGARD, *supra* note 1, at 11 (summarizing the work of Baudrillard).

187. *Id.*

188. *Id.* at 27.

individual who fits the profile is largely irrelevant.[189] Thus, this shadow of correlations becomes the model of reference by which citizens self-censor.

There are now such a quantity and diversity of federal crimes that government agencies cannot even count them, much less prosecute everyone who commits a crime.[190] Today, perhaps the biggest guarantor of intellectual privacy is that the sheer volume of people and behaviors to assess means that most citizens "slip by" under the radar when they innocently commit a crime or engage in several behaviors that together might make a profile.[191] However, when predictive analysis of behavior is automated by linked databases and statistical techniques, intellectual privacy is harmed by allowing punishment (and normalization) to become total, inexorable, and non-discretionary. Because the ultimate objective of surveillance is not prosecutorial evidence-gathering but the disciplined self-normalization of behavior by the citizenry—optimally, without governmental expenditure—certain elements within society will not necessarily regard these trends with alarm.[192] However, that hegemony is problematic because it removes what Julie Cohen calls "semantic discontinuity," a by-product of disparate systems which "preserv[es] breathing room for personal boundary management and the play of everyday practice."[193]

That "breathing room" is none other than the disorganization that creativity needs to synthesize new ideas—the very same creativity we try to preserve with First Amendment protections. It is necessary also for a very simple technical reason: big data cannot correlate data that does not yet exist. Predictive systems are all about constraints, but humans must have enough room to move so that they can freely act outside the models that constrain them, otherwise those models have no new input. In the words of one critic of big data:

> What is greatest about human beings is precisely what the algorithms and silicon chips don't reveal, what they can't reveal because it can't be captured in data. It is not the "what is," but the "what is not": the empty space, the cracks in the sidewalk, the

189. *Id.* at 28.

190. Moxie Marlinspike, *Why 'I Have Nothing to Hide' is the Wrong Way to Think About Surveillance*, WIRED (June 6, 2013), http://www.wired.com/opinion/2013/06/why-i-have-nothing-to-hide-is-the-wrong-way-to-think-about-surveillance/ (citing law professor James Duane and Justice Breyer).

191. One attorney has estimated that Americans commit three felonies per day. *See generally* HARVEY SILVERGLATE, THREE FELONIES A DAY (2009).

192. *See* Mike Masnick, *Creating Chilling Effects on Speech is a Feature, Not a Bug, Of the Surveillance State*, TECHDIRT (Aug. 23, 2013), http://www.techdirt.com/articles/20130822/19270124286/.

193. Cohen, *supra* note 115, at 1931–32.

> unspoken and the not-yet-thought. This has important implications for the notion of progress in society. Big data enables us to experiment faster and explore more leads. These advantages should produce more innovation. But the spark of invention becomes what the data does not say. . . . If Henry Ford had queried big-data algorithms for what his customers wanted, they would have replied "a faster horse."[194]

V. SPECULATIONS AND POSSIBILITIES

Potential refinements to traditional legal doctrine have been discussed above, including undertaking a more robust Fourth Amendment proportionality review and re-conceptualizing the First Amendment as integral to a criminal procedure analysis. However, it seems unlikely that minor tweaks to the existing First and Fourth Amendment canon will constitute a complete solution in the face of rapid technological change. New and different conceptions of data, privacy, and the scope of free human action—conceptions capable of incorporating the technological and economic drivers of the twenty-first century—will likely be needed.

A. *"Quantitative" Privacy Rights*

The advent of gigantic databases filled with personal, behavioral, and biometric data has prompted some commentators to note a disparity between traditional analyses of privacy violations and the new technological realities.[195] Traditional analyses of privacy have focused on the quality of the intrusion—whether the person was in a private space and whether personal chattel was touched by law enforcement.[196] However, the fundamental premise of big data processing techniques is that the discrete bits of data assembled in databases together can form a sufficient picture of an individual to predict his or her behavior. So far, privacy law has been mostly unable to grapple with the notion that thousands of small acts of data gathering—each individually unharmful, authorized by the user, or gathered by different parties—may in their total, quantitative volume create a privacy violation.[197]

Recently, however, a concept of "quantitative privacy" has gained traction with the Supreme Court; in *United States v. Jones*, five justices

---

194. VIKTOR MAYER SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 196–97 (Kindle ed. 2013).

195. *See* Gray & Citron, *supra* note 96, at 83–92.

196. *Id.* at 83–84.

197. *Id.* at 67–68.

voiced concerns about the total effect of this massive data gathering.[198] The five justices appeared to endorse a case-by-case test for each specific investigation to determine whether the volume and type of data gathering was proper under the Fourth Amendment.[199] Thus, the analysis might focus on whether, in the hypothetical case of Bob, it was proper to do phone location tracking for a day, a week, or a month. This interpretation seems to be consistent with a case prior to Jones heard by the D.C. Court of Appeals.[200] Commentators have labeled this the "mosaic" theory.[201]

However, the mosaic theory has been criticized for appearing to conflict with prior Court doctrine and for lack of justiciability.[202] Primarily, the mosaic theory fails to account for technological advances, depending too much on the outdated crutches of reasonable expectation and the third-party doctrine for its analysis.[203] Some critics advocate a different approach: if an investigative technology can "facilitate broad programs of indiscriminate surveillance," then that particular technology is subject to Fourth Amendment regulation.[204] A court would review the suspect technology generally,[205] then approve technology-specific rules, procedures, and practices that balance citizen and law enforcement interests.[206] This approach has the advantage of using traditional procedural methods to challenge the constitutionality of general police procedures, a particular warrant, or conduct during a search, but it rationalizes a different inquiry from the classic third-party and reasonable expectation doctrine which has become so difficult to effectively apply in the advancing technological age.[207]

B. *A Right to Due Process in Automated Systems*

The term "black box effect" is sometimes used to express human uncertainty about a technological system when biases, unknowns, complexity, and secrecy compound to such an extent that the system seems incomprehensible. The term connotes a system in which inputs—

198. *See* United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring); *see id.* at 957 (Alito, J., concurring).

199. *See id.* at 954 (Sotomayor, J., concurring); *see id.* at 964 (Alito, J., concurring).

200. *See* United States v. Maynard, 615 F.3d 544, 562 (D.C. Cir. 2010).

201. *See, e.g., id.*; Christopher Slobogin, *Making the Most of* United States v. Jones *in a Surveillance Society: A Statutory Implementation of Mosaic Theory*, 8 DUKE J. CON. L. & PUB. POL'Y 1 (2012).

202. *See, e.g.*, *Jones*, 132 S. Ct. at 953–54.

203. *See* Gray & Citron, *supra* note 96, at 67–73.

204. *Id.* at 71–72.

205. *Id.*

206. *Id.*

207. *Id.* at 144.

here, statistical behavioral and biometric data—are converted into adjudications (risk of criminality), but the machinations inside the "black box" are impenetrable to those being judged and often opaque even to their custodians. All of these problems exist in an environment that lacks a meaningful process for challenge.

Contributors to the black box effect may be found on each level of system design, implementation, functioning, and maintenance, and examples of each in automated systems are common. At the most basic level, citizens being judged and scrutinized by "secret" systems like those developed by the NSA are the ultimate black box victims in that they do not even know whether or how their lives are being impacted.[208] Additionally, the data forming the source for judgment may be flawed, and because it is compiled from so many diverse systems it is difficult even to know this.[209] Furthermore, in Part III, this Article alluded to the subtle biases that can creep into systems when policy rules are coded into algorithmic rules and when statistical predictions begin to self-reinforce. A corollary to the problem of algorithmic bias is complexity—code may return incorrect results because of unintended flaws in the algorithms, and the overall complexity of the system may make it difficult or impossible to perceive these flaws, much less correct them.[210] For example, a senior intelligence official recently admitted to Congress that the NSA had failed to fully inform the FISC court of necessary details about a call-monitoring program because "no one at NSA had a full understanding of how the program was operating at the time."[211]

Lastly, adjudications and results may be shared between entities, further compounding the difficulties with challenging outcomes and auditability. In a particularly egregious example, it was recently revealed that the NSA was sharing information with the DEA and other agencies.[212] Because the NSA's systems were top secret, DEA agents had to re-develop the provided evidence by other means.[213] Some have

208. *See, e.g.*, Mike Masnick, *Court Says Feds Don't Have to Reveal Secret Evidence It Gathered Against 'Terror' Suspect Using FISA*, TECHDIRT (Aug. 30, 2013), http://www.techdirt.com/articles/20130829/16135324356/court-says-feds-dont-have-to-reveal-secret-evidence-it-gathered-against-terror-suspect-using-fisa.shtml.

209. *See* text accompanying notes 99–102.

210. *See* text accompanying notes 116–24.

211. Cyrus Farivar, *NSA: No One "Had a Full Understanding" of 2009 Call-checking Program*, ARSTECHNICA (Sept. 10, 2013), http://arstechnica.com/tech-policy/2013/09/nsa-no-one-had-a-full-understanding-of-2009-call-checking-program/ (quoting Robert Litt, general counsel of the Office of the Director of National Intelligence).

212. John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

213. *Id.*

argued that this violates a fundamental rule of criminal procedure by not allowing the accused to confront and challenge the evidence against them in court.[214] Even those vaguely aware of the capabilities of NSA tracking were surprised to find that it had violated its mandate to pursue only international targets and was also supplying information for domestic drug enforcement.[215]

Some commentators have noted that these biases, errors, and unknowns collectively form a critical mass of harms that deprives citizens of their Fifth Amendment rights to due process.[216] Professor Danielle Citron argues that, in the first instance, certain kinds of systems should not be automated because they have a significant component of human discretion that makes them problematic to codify into rules.[217] With their judgment clouded by the promises of automation in a technological age, builders of systems have failed to see that the reduction of all adjudicatory process to rules-based systems rather than standards-based systems may not be appropriate.[218] The advent of big-data has worsened this trend by convincing technologists that they can build systems to predict behavior, even when lacking a "theory" of causal relationship between attributes and outcomes. In predictive policing, this trend has been exacerbated by several years of penalty standardization whose goal was to reduce discretion in sentencing.[219] According to Citron, however, systems should be automated only when the "risks associated with human bias outweigh that of automation bias" and "situation-specific discretion" is not required.[220]

Once systems have been automated, processes need to be in place to challenge the perception of infallibility that automated decisions engender. This starts with meaningful notice to those targeted by the adjudication that provides them with an audit trail of the discrete

214. *Id.*; *see also* Mike Masnick, *Congress Asks Eric Holder to Explain Why NSA Supplies DEA Info Which It Then Launders to Go After Americans*, TECHDIRT (Aug. 28, 2013), http://www.techdirt.com/articles/20130827/17564624327/congress-asks-eric-holder-to-explain-why-nsa-supplies-dea-info-which-it-then-launders-to-go-after-americans.shtml.

215. Michael Froomkin, *Encryption: The Sky *IS* Falliing*, DISCOURSE.NET (Sept. 5, 2013), http://www.discourse.net/2013/09/encryption-the-sky-is-falliing/.

216. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1305 (2008).

217. *Id.* at 1304.

218. *See id.* at 1301–03; *see also* LANIER, YOU ARE NOT A GADGET, *supra* note 107, at 9-13, 26.

219. *See, e.g.*, *Overview*, UNITED STATES SENTENCING COMMISSION, http://www.ussc.gov/About_the_Commission/index.cfm (last visited Dec. 17, 2013).

220. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1303 (2008).

component decisions made along the way.[221] Notice allows individuals to invoke further administrative processes to challenge decisions, correct data, explain misinterpretations, and so on. By its very nature, notice and auditing requires that systems are not secretly applied to individuals without their knowledge and requires vendors to build systems and algorithms that they, themselves, can understand well enough to divulge. Requiring openness in auditing combats the institutional mentality of secrecy, which allows agencies to hide behind complexity. Each time an agency claims that a system's inner workings must remain secret for national security reasons it would be required to defend that position. Some systems might even be appropriate for complete transparency, wherein the system's source code is published[222] for review and comment by auditors, academics, and public interest watch groups.

The formal methods of challenge which need to attend every automated system are mostly lacking today. For example, passengers supposedly have the right to petition for removal from the TSA no-fly list, but for most challengers, the petitions go unanswered by the agency.[223] The NSA finds its systems too complex to communicate fully to the FISA Court, the judicial body that supposedly reviews its actions for Fourth Amendment compliance.[224] Finally, individuals investigated by the DEA based on information from the NSA are unable to challenge the evidence because inter-agency secrecy requires DEA to conceal its source.[225]

To help remedy these problems, front-line hearing officers should be trained to accept the fallibility of their systems and understand problem areas.[226] The auditing trail above will assist in explanation, but administrative and district courts need to be trained in automation and statistical issues and accustomed to invoking needed procedural remedies to combat automation bias.[227] Agencies need to become comfortable defending their position from courts without reluctance or indignation.[228] Finally, adjudicatory bodies will need to adjust their

---

221. *Id.* at 1305.

222. *See id.* at 1308.

223. Natasha Lennard, *No-fly Lists: A New Tactic of Exile?*, SALON.COM (Feb. 5, 2013), http://www.salon.com/2013/02/05/no_fly_lists_a_new_tactic_of_exile/.

224. *See* Farivar, *supra* note 211.

225. *See* Masnick, *supra* note 208.

226. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1306 (2008).

227. *Id.* at 1307.

228. *Id.* The "state secrets privilege" also may represent a barrier to victims challenging private vendors in tort for incorrect judgments and harms arising from errors in diagnostic systems. In *Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070 (9th Cir. 2010) (en banc), the state secrets privilege barred the plaintiff from suing a private company that helped with

understanding of the traditional *Mathews v. Elderidge*[229] cost-benefit analysis, wherein the level of due process owed to an individual in an agency action is balanced against the cost and benefit of additional procedures to remedy wrongs.[230] Adjudicators should recognize that, in evaluating the benefit of a single due process challenge, a positive outcome might correct thousands of false or inaccurate predictions.[231]

C. *Economic Rights in My Virtual Proxy?*

In the United States, the law views assemblages of personal data as belonging to the collector of the assemblage, not to the "creator" of the data (*i.e.*, the being whom the data is "about").[232] Thus, Facebook, Acxiom, and Google "own" the data of consumers because they took the trouble to gather it and, to the extent that customers have relinquished any privacy right in the data by agreeing to click-through terms of use, those companies may transfer the data to third parties at will.[233]

While this presumption is so fundamentally ingrained in U.S. law that citizens hardly notice it, it is not the only way of conceiving of personal data. In fact, in the European Union and in many other countries, the law conceives of data as belonging to its creator, not to its collector, consequently giving citizens a much more robust right of control over their data.[234] For example, the E.U. Directive prohibits the "processing" of personal data without the authorization of the person, subject to certain exceptions.[235] In addition, several South American nations have enshrined a constitutional right of "*habeas data"* that protects a person's freedom of information, self-determination, and ability to obtain information about oneself.[236]

In these legal regimes, permission to use the data is exclusively the prerogative of the individual, a notion which maps closely to the traditional bundle of property rights which includes "the right to

---

logistical planning for his extraordinary rendition. However, new policies announced by Attorney General Eric Holder on Sept. 23, 2009 may impact the use of the privilege in litigation.

229. 424 U.S. 319 (1976).

230. Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1283 (2008).

231. *Id.* at 1308.

232. *See* MILLS, *supra* note 132, at 62–63.

233. *See id.*; Rick Burgess, *Federal Court: If Users Don't Click, Your Terms of Service is Invalid*, TECHSPOT.COM (Nov. 2, 2012), http://www.techspot.com/news/50689-federal-court-if-users-dont-click-your-terms-of-service-is-invalid.html (noting a recent Nevada federal court ruling requiring the user to "click" for the click-through terms-of-service to be valid).

234. *See* MILLS, *supra* note 132, at 83.

235. *Id.*

236. *Id.* at 93.

possess, to use, to exclude, to profit, and to transfer."[237] Thus, using property law notions to protect privacy is not new; even U.S. courts have used property theory to restrict access to personal information or to provide remedies and damages, albeit under limited circumstances.[238] A key use is the privacy tort of "right of publicity," which is a statutory cause of action in many states.[239] It covers the "unpermitted use of identity" stemming from a "property right in [the] persona" measured by "damage to the value of [the] identity/persona."[240] However, the tort has had limited impact because it is typically viewed as applying to unpermitted uses strictly in advertising, not to more general commercial activities.[241]

Despite these limitations, the seeds of a solution to remedy certain harms from the use of one's data in prediction may yet be found in property theory. Property rights are politically and culturally compelling in today's market-solution-oriented milieu, because policy arguments with an economic rationale tend to fare better than constitutional rights to privacy when squared off against national security and public safety concerns.[242] There are two reasons property theory may ultimately work: a broader argument and a narrower, subtler one. Both, over time, will have the effect of lessening surveillance and information gathering by depriving predictive NSA and policing systems from many sources of commercial "feeder data."[243] The broad argument is that, as a society, individuals may restrict the use of their data by opting not to use services without a fair-value trade.[244] In other words, we should "raise our prices" and make data much more costly to gather.[245] This argument

---

237. *Id.* at 207.

238. *See id.* at 208.

239. *See id.* at 173–76.

240. *Id.* at 173.

241. *Id.* at 176–77 (noting that the Florida Supreme Court's narrow reading contravenes broader statutory language).

242. *See id.* at 245.

243. *See supra* note 48 and accompanying text.

244. *See* Josh Klein, *Privacy Isn't a Right*, SLATE (Nov. 7, 2013), http://www.slate.com/articles/technology/future_tense/2013/11/reputation_economics_privacy_isn_t_a_right_it_s_a_commodity.html.

> [A] better option might be to simply raise our prices. We can limit how our personal information is gathered and utilized, and in doing so we can demand that it be purchased at higher rates than just access to Instagram. It may not mean cold hard cash (at least not at first), but we can certainly expect more premium services, more discreet advertising, or even just better control over who gets our data and for what purposes.

Id.

245. *Id.*

stems not so much from property rights as from people voluntarily exercising their option not to participate in some online consumer transactions. The broad argument, then, is that the economic cost of obtaining data is proportional to the volume and depth of the privacy intrusion.

The narrower, subtler argument proposed here is that the use of personal data by companies in predictive simulations should be the prerogative of the owner, and something for which she is compensated. This prerogative stems from a recognized property right emerging from the significant commercial value of the data used in simulation by companies and government actors.[246] The prerogative circumscribes a person's right to use, exclude others from using, and profit from her data, creative contributions, movements, and behaviors—those aspects of personal autonomy that this Article terms a "virtual proxy." Those property rights naturally would include the actions of a person's virtual proxy in simulation to solving business or predictive marketing problems. The proxy or any subset of it may be "sold" by its owner under this right. The fundamental notion is supported by traditional property theory, in which ownership derives from the contribution of individual labor to a product or process.[247] In their seminal article on privacy, Warren and Brandeis argued that "living life itself" imbued one's personality and information with the labor necessary for a property right[248]—an even more direct, though often forgotten, link to the compensable value of the lived life.

The question of how society might rationally tie data gathered for the purposes of simulation to its commercial value is an interesting one that requires speculative thinking because it differs markedly from the model in place in today's information economy. Recently, critics have begun remarking on the "exhausting work of the technology user."[249] "Siren servers"[250] like Google, Facebook, Twitter, and Amazon aggregate the billions of tiny contributions made each day by users of their online services, aggregating user data, selling it, or otherwise monetizing their creative contributions.[251] According to one

246. *See id*.

247. MILLS, *supra* note 132, at 205.

248. *Id.* at 205–06.

249. Ian Bogost, *Hyperemployment, or the Exhausting Work of the Technology User*, ATLANTIC (Nov. 8, 2013), *available at* http://www.theatlantic.com/technology/archive/2013/11/hyperemployment-or-the-exhausting-work-of-the-technology-user/281149/ (last visited Feb. 19, 2014).

250. LANIER, WHO OWNS THE FUTURE?, *supra* note 116, at 55 ("Siren Servers gather data from the network, often without having to pay for it. The data is analyzed using the most powerful available computers, run by the very best available technical people. The results of the analysis are kept secret, but are used to manipulate the rest of the world to advantage.").

251. Bogost, *supra* note 249.

commentator, people have been "duped into contributing free value to technology companies," essentially working "unpaid jobs . . . hustling" for "unseen bosses."[252] The recent Digital Labor Conference notes the pervasiveness of these trends: "Every aspect of life drives the digital economy: sexual desire, boredom, friendship — and all becomes fodder for speculative profit. We are living in a total labor society and the way in which we are commoditized . . . is profoundly and disturbingly normalized."[253]

Unfortunately, these trends are the reverse of what technological productivity was supposed to bring. Left to play out, the current model will mean that a few individual "winners" who own siren servers will live well aggregating the tiny, free contributions of the vast swath of humanity, the totality of which is essential, but wherein each individual person is almost valueless.[254] Technology futurist Jaron Lanier remarked that "People are gradually making themselves poorer than they need to be. We're setting up a situation where better technology in *the long term just means more unemployment.*"[255]

However, the model we have chosen is not the only option. Lanier believes that a fundamentally new way of valuing personal information, creativity, and contribution will be imperative for a fair and functioning information society of the future.[256] Lanier proposes instead that the creative contributions of individuals be valued at reasonable prices driven by marketplace demands.[257] Each "access" of the creative content by others would elicit a micro-payment, and thus "personal expression would be valued."[258] The micropayment would offset the person's own consumption in the digital economy.[259] Such a system would require a different technical architecture than presently found on the Internet, as it demands that information "remember" its origin so that its creator can be compensated.[260] Obviously, it is by no means easy or quick to build, either from a policy or a technical standpoint.[261] It would likely require years of work, as well as societal assent to government oversight of the underlying tracking and valuation

252. *Id.* ("Today, everyone's a hustler. But now we're not even just hustling for ourselves or our bosses, but for so many other, unseen bosses . . . [for example,] for Twitter, which just converted years of tiny, aggregated work acts into $78 of fungible value per user.").

253. *The Internet as Playground and Factory*, DIGITAL LABOR CONFERENCE, http://digitallabor.org/ (last visited Dec. 17, 2013).

254. LANIER, WHO OWNS THE FUTURE?, *supra* note 116, at 11.

255. *Id.* at 8.

256. *See id.* at 7–10.

257. *See id.*

258. LANIER, YOU ARE NOT A GADGET, *supra* note 107, at 100–01.

259. LANIER, WHO OWNS THE FUTURE?, *supra* note 116, at 240.

260. *See id.* at 226–27.

261. *See id.* at 233–35.

systems.[262]

Critics will no doubt argue that this outcome is implausible for at least two reasons. First, it is far-fetched to imbue a "virtual proxy" with real personhood in any non-entertainment sense. This Article makes no argument that this "proxy being" is a "real person" in any true sense, but copyright law suggests some interesting parallels. Although a person's persona (name, likeness, and attributes) is not copyrightable,[263] under copyright law authors get protection for sufficiently delineated fictional characters. [264] It will be difficult for supporters to argue that big data analytical models "predict behavior" without running an individual in sufficient simulation to meet the tests for copyrightability. In an interesting case from the Ninth Circuit illustrating both of these issues, the actors who portrayed the characters Norm and Cliff were able to sue Paramount studios for licensing animatronic robots to a national chain of bars that closely resembled their real appearances.[265] Might the "author" of one's virtual proxy have an intellectual property interest in it? The answer is unknown, but poses interesting questions.

In any case, supporters of predictive crime technology will have to walk a fine line in resisting the increasing economic plausibility of data as a property right. To both support the validity of predictive technology and resist property rights theory will put them between the horns of a dilemma. It will be difficult to argue that these systems have methodological validity in predicting criminal behavior or buying patterns, but have no commercial value to the primary human actor. A valid predictive model creates, in essence, a virtual person running in simulation. Are we to say that the human actor providing the attributes on which this simulation depends has no economic rights to it?

The second criticism is that the government may simply demand free access to the "proxy." Under a compensated data use system, however, commercial actors must reconceive the economic profitability of data-gathering models, and when they do so, large amounts of feeder data that predictive policing systems can pull from may become more expensive or even dry up altogether. Governments cannot force commercial entities to track and store information without compensation, even in our present environment.[266] In a future system

262. *See id.* at 344–45.

263. JULIE COHEN ET AL., COPYRIGHT IN A GLOBAL INFORMATION ECONOMY 265 (3d ed. 2010).

264. *See id.* at 257–65; *see, e.g.*, MGM, Inc. v. Am. Honda Motor Co., 900 F. Supp. 1287 (C.D. Cal. 1995) (holding that James Bond is a copyrightable character under either the Second Circuit or the Ninth Circuit test).

265. Wendt v. Host Int'l, Inc., 125 F.3d 806, 811 (9th Cir. 1997).

266. Robert Lenzner, *ATT, Verizon, Sprint Are Paid Cash By NSA For Your Private Communications*, FORBES (Sept. 23, 2013), http://www.forbes.com/sites/robertlenzner/2013/09/23/attverizonsprint-are-paid-cash-by-nsa-for-your-private-communications/ (noting that the

where personal data is costly and companies only record what they truly need, governmental interests would have to pay companies even more for data, demanding that these costs be exposed and rationalized within the state and national budgeting processes.

Regardless of the likelihood that Lanier's proposal will be implemented in the near future, it illustrates that technical visionaries recognize the limits of free access to personal data, and are cognizant that change will likely be necessary to accommodate different policy priorities. These changes, in turn, support the policy behind a property right for data. Over time, individuals possessing a property right to data may ultimately demand a higher price for its use, depriving much of the indiscriminate, inexpensive data gathering that occurs in today's today surveillance-prediction paradigm of its favorable cost-benefit ratio.

VI. CONCLUSION

"Knowledge invents the Secret."—Michel Foucault[267]

We now have the capacity to atomize human behaviors into gestures and biometric signals, and to dissect each thought into its constituent words, attributes, and hesitations as that thought forms. Our technologists believe that, with enough of this kind of atomization, higher-order selfhood can be modeled deterministically in advance. As a result, humans are in danger of becoming not only transparent, but also invisible and irrelevant.

> Both [governments and corporations] want access to everything that can be known about you, because who knows until later what may prove the crucial piece of information to uncover a terrorist network or lure in a new network of customers. They want everything, at least, that can be run through a system of massive computers and sorted into patterns of various potentially useful kinds. You are to be, in this sense, the transparent man or transparent woman. Your acts, your life patterns, your rights, your codes are to be an open book to them -- and increasingly a closed book to you. You are to be their secret. . . .[268]

In choosing to apply these principles to criminal prediction, our

---

NSA already compensates communications carriers for access to telephony metadata).

267. MICHEL FOUCAULT, THE BIRTH OF THE CLINIC 201 (1975).

268. Tom Englehardt, *Engelhardt*, *You Are Our Secret*, TOMDISPATCH.COM (June 16, 2013), http://www.tomdispatch.com/post/175713/tomgram%3A_engelhardt,_you_are_our_secret/.

society demonstrates that law and other institutions are in danger of "dehumanization"—in danger of forgetting that humans are even part of the equation. In this increasingly machine-mediated world, this form of justice, one choice among a wide spectrum of options, chooses us as consequence of our approach to technology.[269] With that choice comes consequences to our privacy and our capacity to create, and if unchecked represents the poorest possible policy, a total surveillance, mediated, and deterministic society that fails even to make its citizens safe.

269. HARCOURT, *supra* note 54, at 31–33.