A Proposal to Adopt Data Discrimination Rather than Privacy as the Justification for Rolling Back Data Surveillance

Author(s): Benjamin W. Cramer

Source: *Journal of Information Policy*, Vol. 8 (2018), pp. 5-33
Published by: Penn State University Press
Stable URL: http://www.jstor.org/stable/10.5325/jinfopoli.8.2018.0005
Accessed: 04-06-2018 09:09 UTC

A PROPOSAL TO ADOPT DATA DISCRIMINATION RATHER THAN PRIVACY AS THE JUSTIFICATION FOR ROLLING BACK DATA SURVEILLANCE

Benjamin W. Cramer

ABSTRACT

Critics of data surveillance by government and businesses have used a legal strategy based on privacy, but have thus far been unsuccessful. This article suggests that civil libertarians should consider raising the specter of unfair data discrimination in legal arguments to roll back data surveillance, and they may find support from statutory and judicial precedents in which the American government fought to protect citizens from older types of discrimination. This may in turn support arguments that America is traditionally opposed to discrimination, and should be opposed to modern discrimination caused by data surveillance practices.

Keywords: surveillance, data tracking, privacy, discrimination, telecommunications

Since the Snowden revelations on data surveillance by the US government, civil libertarians have initiated legal actions attempting to roll back those surveillance programs, usually focusing on the Fourth Amendment. However, the government has perfected the rhetoric that surveillance protects the country from terrorism. Regardless of the evidence, this claim has immense argumentative power over lawmakers and the judiciary.

Privacy proponents have been equally frustrated in their attempts to achieve legislation to control personal data tracking by businesses. In this case, privacy rhetoric is not strong enough to overcome corporate claims of profitability, job creation, and innovation. Lawmakers have largely adopted this rhetoric, once again regardless of the evidence, and have been

Benjamin W. Cramer: Donald P. Bellisario College of Communications, Pennsylvania State University

JOURNAL OF INFORMATION POLICY, Volume 8, 2018

unmoved by the idea of privacy as a value to be preserved as companies monetize personal data.

This article argues that the privacy-based strategy to roll back data surveillance is untenable and should be scrapped in favor of one based on data discrimination. In light of emerging stories of discrimination enabled by big data, this article discusses historical legal justifications for protecting citizens from discrimination by both government and businesses. These protections have been achieved via more tenable constitutional arguments and have not been thwarted by rhetoric about national security or job creation.

Thus, this article suggests that civil libertarians should consider raising the specter of unfair data discrimination in legal arguments to roll back data surveillance, and they may find support from statutory and judicial precedents in which the American government fought to protect citizens from older types of discrimination. This may in turn support arguments that America is traditionally opposed to discrimination and should be opposed to modern discrimination caused by data surveillance practices.

This article is admittedly a position statement, encouraging an updated outlook on civil liberties that is untested and comes with no guarantee that it will be more successful than the previous outlook. Also, for purposes of brevity, the arguments in this article are based on American social and legal history; possible solutions to the problems of data surveillance may take different forms elsewhere, particularly in the European Union where data privacy laws are stronger. Nonetheless, for the United States at least, evidence indicates that the current privacy-based strategy is unlikely to succeed, so there is little initial harm in attempting a new argumentative technique. While privacy is a crucial American value, it may be more realistic to convince judges and politicians that a different American value, freedom from discrimination, is also at risk in the world of big data.

The State of Judicial and Legislative Privacy

Privacy is indeed a social value and democratic ideal for many Americans. In a 1965 ruling, Supreme Court Justice William O. Douglas made privacy bigger than even the Constitution when he noted, "We deal with a right of privacy older than the Bill of Rights, older than our political parties,

older than our school system."[1] The biggest privacy-oriented controversy of recent times, the American government's data surveillance regime, has inspired critics and civil libertarians to claim that such programs are violations of privacy. That argument has been mostly unsuccessful so far in the courts and the legislature; this is not because privacy is an unimportant value, but because as a value it lacks the rhetorical power to overcome opposing arguments that favor national security.

The state of privacy law in America indicates that privacy will remain a high-level ideal, but the authorities are unable or unwilling to enforce it at the practical level. With the advent of the information age, all data and communications are at risk of being tracked, but we are stuck with outdated and piecemeal privacy statutes that only protect limited categories of personal information. Examples include the Family Educational Rights and Privacy Act (FERPA, 1974), which prohibits schools and colleges from disclosing a student's educational records to anyone but the parents; the Health Insurance Portability and Accountability Act (HIPAA, 1996), which prohibits healthcare providers from disclosing personal health information without the patient's consent; or a variety of financial privacy laws targeting banks, such as the Bank Secrecy Act (1970) or the Right to Financial Privacy Act (1978).

These category-specific statutes are a result of America's preference for markets and private companies to address problems first, with laws only being enacted for specific problems in which the markets have failed to address citizen concerns. For privacy law, this pattern has resulted in a patchwork legal infrastructure with piecemeal statutes that addressed particular issues after they became problems.[2] But in the modern big data society, more and more sensitive information is stored online, including nearly all personal communications and business transactions of any purpose. This is far beyond categories like financial information, which are no longer unique in their sensitivity. The existing piecemeal privacy statutes are woefully inadequate in the era of big data and pervasive surveillance, leading civil libertarians to the higher rights embodied in the US Constitution.

In 2013, whistle-blower Edward Snowden revealed the extensive surveillance of Americans' telecommunications transmissions by the National

1. Griswold v. Connecticut, 486.
2. Radin, 218–19.

Security Agency (NSA) and other governmental bodies.[3] Many experts and commentators have claimed that the NSA's domestic surveillance program violates the Fourth Amendment, which secures the right of the American people against unreasonable searches and seizures by government without a warrant.[4] For example, this claim has been made by the National Constitution Center, a nonpartisan organization of eminent constitutional scholars that was established by Congress to educate the American people about their rights as citizens.[5] The American Civil Liberties Union has made the same claim in a lawsuit against then-Director of National Intelligence James Clapper[6]; as has libertarian politician Rand Paul in reaction to Clapper's much-criticized "least untruthful" testimony before Congress about the government's surveillance practices.[7]

The problem with this argument is that the Fourth Amendment is a right to demand that government investigators follow proper procedures when they search your personal effects, and that is a *type* of privacy, but the Amendment does not serve as a comprehensive right to privacy in all situations. There has been significant dispute over whether the modern surveillance regime should be evaluated under the Fourth Amendment at all, largely due to uncertainty over whether the collection of telecommunications records is actually a "search" under the Amendment (as opposed to mere compilation of data), plus arguments from surveillance proponents that the practice is necessary to protect national security and therefore is not "unreasonable" per the Amendment's language.[8]

A further weakness of the Fourth Amendment argument is the question of whether Americans actually have a *right* to privacy. This is a matter of a

---

3. This heavily reported event was first reported by journalist Glenn Greenwald; for a summary of his early reports, see Greenwald.

4. The text of the Fourth Amendment is as follows: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

5. Hafetz.

6. McVeigh. The lawsuit, ACLU v. Clapper, will be discussed in detail below.

7. Paul; In March 2013, 3 months before the Snowden revelations, Clapper testified before Congress and was asked by Sen. Ron Wyden, "does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Clapper's response was a direct "No, Sir." When it became known that the NSA did in fact conduct such surveillance, Clapper claimed in a news interview that "I responded in what I thought was the most truthful, or least untruthful manner, by saying no." His use of the bizarre term "least untruthful" attracted widespread criticism, particularly from surveillance critics in Congress. Kessler.

8. Since the Snowden revelations, this conundrum has been analyzed extensively by legal researchers. See, for example, Levinson-Waldman, 527–615; Kwoka, 103–65; Kerr, 285–329.

longstanding dispute; and it is important to note that the word "privacy" does not appear anywhere in the Constitution. Back in 1890, legal scholar and future Supreme Court Justice Louis Brandeis proposed that different parts of the Constitution could be cobbled together to form an indirect or implied right to privacy. Interestingly, Brandeis was reacting to that era's new surveillance technology for which the law was unprepared: cameras.[9] By the 1970s, the Supreme Court acknowledged Brandeis's reasoning by ruling that one could creatively interpret the First, Third, Fourth, Fifth, and (later) Fourteenth Amendments to conclude that Americans have an implied right to privacy.[10]

This conception of a right to privacy is already vague, and for critics of government surveillance, it is unlikely to work because of the procedural focus of the Fourth Amendment. The Fourth Amendment requires a *warrant* for a *search* of a citizen's effects. This indicates a procedure that must be followed by law enforcement and national security personnel, and not necessarily a right of the people to be shielded against an actual investigation that precipitates the government's enactment of that procedure. In short, if investigators have convinced a judge of probable cause to issue the warrant, then the Fourth Amendment has been satisfied. For modern NSA data surveillance, this procedure is carried out under the auspices of the Foreign Intelligence Surveillance Court (FISC), which approves warrants for NSA operations routinely. Thanks to the power of antiterrorism arguments, the FISC has issued the requested surveillance warrants at least 99 percent of the time.[11]

Until 2015, the FISC operated in near-absolute secrecy. Procedurally, national security officials would request a warrant to track a targeted person's communications from the court's sitting judges,[12] and only the government's side was represented.[13] For security reasons, the targeted individual was not informed that they were the subject of a warrant request, nor

9. Warren and Brandeis.

10. Griswold v. Connecticut; Roe v. Wade.

11. Various studies have concluded that the FISC approves search warrant requests from the security agencies as much as 99.97 percent of the time. See, for example, Clarke; Eichelberger; Cohen.

12. The Foreign Intelligence Surveillance Court consists of a committee of eleven (originally seven) judges selected from the Federal court system, who serve rotating 7-year terms. All member judges are appointed by the Chief Justice of the Supreme Court, with no additional confirmation by the Legislative Branch, while almost all of the court's activities involve processing search warrant requests made by Executive Branch security agencies. Lichtblau.

13. Note that there are slightly different procedures for foreign and domestic surveillance targets; see Greenwald and Ball.

was there anyone present to speak on behalf of this person or the public at large.[14] This procedure changed slightly with the USA Freedom Act of 2015, which added a requirement for the FISC to appoint at least five individuals to add arguments during warrant hearings in favor of privacy or civil liberties issues, thus serving somewhat as watchdogs on behalf of the general public, though there is still no representation for the targeted individual.[15] In fairness, the lack of proper representation can be justified by arguments that a national security investigation would be thwarted if the individual knows that he is being tracked. Regardless, this procedure of obtaining a warrant is consistent with the requirements of the Fourth Amendment, because a judge has been convinced that a search warrant is justified. Since the reforms of 2015, the security agencies' success rate in obtaining warrants has not changed appreciably.[16]

The term "unreasonable" in the text of the Fourth Amendment is also a problem for privacy proponents, because with the correct rhetorical strategy, security officials can easily overcome resistance by implying that it is reasonable to track communications in order to prevent terrorist attacks. This is a triumph of rhetoric that in turn creates a "ratchet effect" in which legal processes move in the direction of defeating an enemy and become tougher to scale back or repeal.[17] An example of this trend can be seen in the court case *Jewel v. NSA*: after being ordered by the judge to stop destroying evidence of its data collection activities, the NSA replied that "The impact of compliance with this Court's June 5 [2014] order on the NSA—on the national security of this country—would have immediate adverse consequences," and that "any decision that might impair NSA operation in this manner could immediately deprive the nation of this valuable tool and cause immediate and grave danger to the national security."[18] In another noteworthy court dispute on NSA surveillance, *Hepting v. AT&T*, the judge dismissed the citizen complaint for little reason beyond

14. Sprigman and Granick.

15. Poplin.

16. Martin.

17. For an analysis of the "ratchet effect" in general and its effects on surveillance law, see Givens.

18. Jewel v. National Security Agency, Opposition to Plaintiffs' Emergency Application to Enforce Court's Temporary Restraining Order, 2010 U.S. Dist. LEXIS 5110 (U.S. Dist., N.D. California, 2010), June 6, 2014, accessed September 2, 2017, https://www.eff.org/files/2014/06/06/govtopp6614.pdf, 11–12. The NSA was destroying records due to a procedural rule about only keeping the results of surveillance efforts for a limited time, while the complainants in the case demanded a particular set of records for discovery purposes.

the belief that the NSA surveillance program was "designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States"—with almost no discussion of whether the program was actually effective.[19]

The power of antiterrorism rhetoric, and its effectiveness against privacy or Fourth Amendment arguments, can be seen in a crucial split precedent. Two nearly identical district court cases, in which citizens sought damages for excessive government surveillance, resulted in opposite rulings because of how much the respective judges were swayed by antiterrorism rhetoric. In late 2013, Judge Richard Leon of the federal district court in the District of Columbia ruled in *Klayman v. Obama* that the NSA program is likely unconstitutional: "Surely, such a program infringes on 'that degree of privacy' that the founders enshrined in the Fourth Amendment." Rhetoric about the need to prevent terrorist attacks at all costs is almost entirely absent in Leon's ruling. He instead focused primarily on changing technologies and social uses of those technologies, concluding that it was time for old rules on the matter to be reconsidered.[20] According to Leon, modern telecommunications networks are pervasive, as is the ability of governments to track our usage of them, and this is a new phenomenon that deserves an updated Fourth Amendment analysis.

However, just days later a different district court judge, William Pauley of the Southern District of New York, ruled in *American Civil Liberties Union v. Clapper* that the NSA surveillance program did *not* violate the Fourth Amendment due to the reasonableness of national security investigations.[21] On appeal, the Second Circuit overturned this ruling but then remanded the case back to Pauley's court for procedural reasons, thus adding to the judicial confusion.[22] But more fundamentally, in his original ruling Pauley offered an interpretation that is nearly the opposite of Leon's in the *Klayman* case. Pauley said next to nothing about technology and based his opinion almost entirely on how NSA surveillance is justified by the need to prevent another terrorist attack like the one on September 11,

19. Hepting v. AT&T, In re: National Security Agency Telecommunications Records Litigation, 2006 U.S. Dist. LEXIS 41160 (U.S. Dist., N.D. California, 2006), June 3, 2009, accessed September 2, 2017, https://www.eff.org/files/filenode/att/orderhepting6309_0.pdf, 6.

20. Klayman v. Obama, 42. An appeal of this ruling by the government commenced at the District of Columbia Circuit Court of Appeals in November 2014 and is still being litigated at the time of writing.

21. American Civil Liberties Union v. Clapper, 749.

22. Stempel.

2001. Showing the power of the antiterrorism argument, Pauley also did not substantially discuss the Fourth Amendment or any right to privacy.[23]

These two parallel cases, leading to a split precedent, indicate the need for a higher appeals court to settle the Fourth Amendment question.[24] Also note that in both of these cases, and several others, the NSA and its defenders have claimed that "collection" of personal data is not the same as the "search" mentioned in the Fourth Amendment, while the "warrant" required by that Amendment is easily obtained from the secretive FISC.

Judge Leon in *Klayman v. Obama*, with his opinion that the NSA has violated the Fourth Amendment if one considers the issues raised by modern technologies, is clearly the outlier in this type of case. Otherwise, while the case history is still developing, so far the Fourth Amendment argument has not been successful in the courts. In addition to powerful government arguments on the need for security, the judiciary has also been constrained by a crucial pre-Internet Supreme Court precedent on what Americans should expect when they use telecommunications networks that collect their personal data.

Smith v. Maryland (1979)[25] involved a criminal defendant who had been suspected of making harassing phone calls to his victim. The police made use of a "pen register" at the phone company to determine that he was in fact calling the victim's number. A pen register has long been a popular tool with the law enforcement community for investigating criminal suspects via their telephone calling patterns. Early versions of this device recorded the audio pulses used by telephone systems to direct a call to the proper recipient; the pulses could be decoded to find the phone number that the customer was calling. This was done by the telephone company to compile called numbers for billing purposes, but the resulting records were also useful to the police.[26]

Mr. Smith argued that the police's use of phone company records of his calls was a search of his personal effects, and per the Fourth Amendment a warrant should have been obtained. The Supreme Court ruled that compiling information from the pen register is not a "search" under the Fourth Amendment because Smith "voluntarily conveyed numerical information to the telephone company." Furthermore, as a phone company customer,

23. American Civil Liberties Union v. Clapper. After a series of appeals and remands, this case is still being litigated at the time of writing.

24. Schmitt.

25. Smith v. Maryland, 442 U.S. 735 (U.S. Supreme Court, 1979).

26. Strange.

Smith should have known that the network would need to know this information in order to function properly as it connected his calls. Thus, he did not have a reason to expect his calling information to be private.[27]

Smith v. Maryland was the Supreme Court's first notable acknowledgement of the "Third Party Doctrine"—the idea that the Fourth Amendment applies when government authorities search you and your possessions directly, but *not* when they search information that you have given to a third party (such as a telecommunications network company) voluntarily.[28] The ruling was also a key development in the doctrine of "reasonable expectation of privacy"—the idea that you should not expect privacy for information that you have voluntarily exposed to the public, with telecommunications networks now being considered "public" for purposes of this argument.[29]

And finally, *Smith v. Maryland* established the precedent that a person's use of a telecommunications network is completely voluntary, which may have been a viable conclusion for landline telephones in 1979, but which may no longer be tenable in modern times when it is becoming less and less possible to live one's life offline.[30] Also note that the modern digital equivalents of the old pen register device can record the routing information *and* the content of telecommunications transmissions; the latter of these is a development of the modern information age. The ongoing difficulties of the *Smith v. Maryland* precedent are evident in the conflicting *Klayman* and *Clapper* cases described earlier: Judge Leon in *Klayman* contributed lengthy dicta on why the precedent needs to be overturned due to modern technological realities, but Judge Pauley in *Clapper* used that same precedent as direct justification for NSA surveillance because we use networks voluntarily.

Judges in more recent cases on modern surveillance techniques in law enforcement have exhibited some acknowledgement of the questions

27. Smith v. Maryland, 743.

28. Solove, 102–10.

29. This is related to the previously established notion that you have no privacy from devices like cameras when you voluntarily walk around in public. The ruling in Smith v. Maryland stated that the information used by telecommunications networks, especially phone numbers, is visible to the public so this makes a network "public" under this discussion.

Note that this conception of a "public" network does not apply to who built the network, resulting in a contradiction with other areas of law. If a telecommunications network was built by a private company with private capital, it is considered a "private" network in contract law and corporate law, but it is likely to be considered "public" in the realm of Fourth Amendment law. Michel and Gattuso.

30. Nissenbaum, 559–96.

raised by new technologies, especially the power of metadata (data in a communications transmission other than the actual content of the message, such as routing information, global positioning system [GPS] location data, etc.), but surveillance in itself will probably continue to be upheld. In *U.S. v. Jones* (2012), police officers placed a GPS tracking device on a suspect's car and tracked his movements for nearly a month, but had neglected to obtain a warrant for that extended time period. In its ruling, the Supreme Court noted that the resulting collection of personal data was a possible intrusion into the most intimate details of the individual's private life, but merely concluded that the data collection was indeed a "search" under the Fourth Amendment and that the police officers should have simply followed the proper warrant procedures.[31] In *U.S. v. Davis* (2014), the Eleventh Circuit Court of Appeals made a similar point about police collection of a suspect's cellular phone location data, which can be considered an intrusion into one's private life, but this court also ruled that the typical procedure to obtain a warrant is sufficient to overcome Fourth Amendment concerns.[32]

This section has argued that regardless of its merits as an American value, arguments in favor of personal privacy (via the Fourth Amendment or otherwise) have been unsuccessful in court cases or political arguments challenging the American government's pervasive tracking of telecommunications transmissions. This is because judges and politicians are likely to be swayed by the power of antiterrorism rhetoric. The next section argues that the corporate sector, which has its own reasons for tracking personal telecommunications data, has its own powerful rhetoric that easily defeats value-based privacy arguments.

Corporate Disregard for Privacy

While the Snowden revelations of governmental data surveillance ignited a political controversy in 2013, the data tracking practices of the corporate sector had already been known for years. While some privacy activists had criticized such practices previously, the public became more concerned about corporate data tracking in tandem with the NSA controversy, with some political leaders following apace.[33]

31. U.S. v. Jones.
32. U.S. v. Davis.
33. Lyon, 1–13.

According to communications scholar Tim Wu, the media industry has used three business models regularly since the late nineteenth century: selling content, selling advertising space, or both in tandem. The book and movie industries, for example, sell content directly to the media consumer. The broadcast television industry is free for viewers and sells airtime (advertising space) through which companies can reach those viewers. Cable television and magazines do both. This industry structure was mostly static until the late 1990s, when Internet firms pioneered a fourth business model that combines the older ones with a new technological twist: giving a service like e-mail or social networking to consumers for free while collecting their personal information, which is then sold to advertisers.[34]

Data tracking by websites and Internet service providers (ISPs) is nearly as old as the World Wide Web, and companies have traditionally tracked users' browsing and searching activities in order to find patterns of personal behavior that could be of interest to advertisers. Most of the leading web companies, like Google, provide services for free and thus are dependent upon advertising revenues, while advertisers crave precise user data for the creation of targeted and efficient ads.[35]

The privacy practices (or lack thereof) inherent to Internet advertising have been under the purview of the Federal Trade Commission (FTC) since a personal data tracking complaint against GeoCities in 1998.[36] Political concerns have escalated into calls for enforced "Do Not Track" options for Internet users, which would also be under the purview of the FTC.[37] Consumer advocacy groups first advanced this idea to the FTC in 2007,[38] and the commission first proposed an enforced requirement for Do Not Track options in web browsers in 2010.[39]

In discussions of data tracking by businesses, economic arguments (almost always featuring the terms "jobs" and "innovation") play the role performed by antiterrorism arguments when government is the tracker.[40]

---

34. Wu.

35. Madrigal.

36. Federal Trade Commission, "In the Matter of GeoCities"; Federal Trade Commission, "Internet Site Agrees to Settle."

37. The FTC has been involved in general consumer privacy issues since it was given the responsibility for enforcing the Fair Credit Reporting Act of 1970. Federal Trade Commission, "Protecting Consumer Privacy," A-3.

38. Brookman.

39. Angwin and Valentino-DeVries.

40. The upcoming discussion uses notable examples of industry statements and media reports in which the "jobs" and "innovation" arguments were used in a fashion that contradicts privacy-based counterarguments.

Government has mastered the art of claiming to protect national security; the corporate sector has mastered the art of claiming to protect the economy. During FTC hearings in 2010, Time Warner Cable Executive Vice President Joan Gillman stated that "Do-not-track could hinder job creation within the advertising industry and by websites that rely on advertising revenue."[41] The power of this type of argument is captured in the following quote from former US Commerce Secretary Gary Locke: "America needs a robust privacy framework that preserves consumer trust in the evolving Internet economy while ensuring the Web remains a platform for innovation, jobs, and economic growth."[42] Despite the brief allusion to privacy concerns, note that this statement does not question whether data tracking really does foster those economic ideals: this is taken as a given.

Some legislators have attempted to resist these arguments with a focus on privacy as the primary value to be achieved. Representative Jackie Speier (D-CA) introduced the Do Not Track Me Online Act in 2011, which would have authorized the FTC to enforce regulations regarding the collection and use of information about any individual obtained via online tracking. Reactions to the bill fell into a dichotomy of business benefits versus consumer privacy, with everyone claiming to have the public's interests at heart.

The advertising industry's stance was represented by a lawyer for the Digital Advertising Alliance who framed the bill in terms of what consumers supposedly desire: "There is no consumer product in the world right now that people love more than the stuff that's going on in the Internet. And that requires the free flow of information [among Internet companies]."[43] Time Warner Cable stated that "do-not-track could hinder job creation within the advertising industry and by Web sites that rely on advertising revenues," as well as "inhibit innovation and the development of new services."[44] Neither of the media outlets that published these quotations investigated whether they were accurate or based on rigorous public opinion research and economic data.

Speier's bill died in committee, possibly because the majority of her colleagues subscribed to the economic ideal rather than the privacy ideal. Meanwhile, the White House weighed in with a 2012 report that

41. Gross.
42. Quoted in Vega.
43. Davis.
44. Wyatt.

attempted to counteract the trend with a focus on consumer privacy. In his introduction to the report, President Barack Obama was compelled to make a brief reference to the pro-business point of view, stating that "the Internet has enabled . . . an explosion of commerce and innovation creating jobs of the future. Much of this innovation is enabled by novel uses of personal information." But otherwise the President claimed that "we must reject the conclusion that privacy is an outmoded value. It has been at the heart of our democracy from its inception, and we need it now more than ever."[45]

Bills to protect consumer privacy online were still being promoted by the President in 2015, despite a lack of action in Congress. An updated White House proposal released that year reflected (according to some critics) the Obama Administration's recent and severe loss of credibility among privacy advocates, thanks to the Snowden revelations.[46] Pro-business think tanks repeated the standard arguments based on jobs and innovation: a researcher with the Mercatus Center stated that "No matter how well-intentioned this proposal may be, it is vital to recognize that restrictions on data collection could negatively impact innovation, consumer choice, and the competitiveness of America's digital economy."[47] The Technology Policy Institute noted that "The Administration has repeatedly failed to demonstrate that privacy legislation is needed to address concrete harms or that such legislation would improve consumer welfare . . . it [the proposed legislation] is likely to harm innovation and ultimately make consumers worse off."[48] Note that this pro-industry statement, in which the government is criticized for failing to provide evidence that its privacy goals are necessary, neglected to do the same thing for its own arguments on innovation. During research for this article, no notable instances were found of anyone in the government or media questioning this contradiction, once again showing the power of economic rhetoric.

This recent history shows that when it comes to discussions of data tracking by the corporate sector, legislators and regulators are unlikely to place personal privacy at the top of their list of concerns. The argument that companies must collect personal data in the interests of the economy has emerged victorious. Meanwhile, a lesser known business trend adds further pressure on companies (in a plethora of different industries) to

45. The White House.
46. Wilhelm.
47. Eggerton.
48. Ibid.

collect as much data from their customers as possible. Business owners are under increasing pressure to collect and monetize consumer data—from actual usage of websites, to data collected from loyalty and discount cards, to social media commentary that is simply about the company in question. Shareholders are placing more and more pressure on companies to increase revenues via the sale of such data to advertisers.[49]

Thus, the Internet industry is unlikely to believe or even acknowledge claims that users' privacy is violated by data tracking practices, and even if they did, the economic benefits are apparently so powerful that furnishing proof of their existence is hardly necessary. The majority of representatives in Congress have adopted this position.[50]

The apotheosis of this trend might be the data tracking legislation passed early in the Trump Administration. Shortly after Trump took office, he signed legislation that repealed a rule from the previous administration that prohibited ISPs from selling the personal data of their customers; these rules were stricter than those applied to websites like Google or Facebook, prompting accusations of unequal treatment.[51]

The Trump Administration, including present FCC Chairman Ajit Pai, has concluded that ISPs will protect the privacy of their customers, with no evidence given for this conclusion except for lobbying statements by the ISPs themselves. The administration has also missed the fact that companies like Google and Facebook collect and sell personal data in return for free consumer services, while ISPs already make money by charging customers for network access—hence, the previously differentiated privacy rules. Now ISPs can charge their customers for access *and* make money off those customers a second time by selling their personal data.[52]

The Specter of Data Discrimination

While privacy advocates and like-minded civil libertarians can and should charge that modern data surveillance by government and corporations is an invasion of privacy, we have seen that this argument faces

49. Laney.
50. Davis.
51. Fung.
52. This practice is called "double dipping" in the industry. Frieden.

severe handicaps in the judiciary and in the halls of Congress. Beyond court precedents and political trends as described herein, it is also very difficult for an individual person to prove that his or her privacy has been directly violated by mass surveillance.[53] This same problem is an admitted weakness of the present article, which offers a shortage of actual examples of data discrimination due to the fact that such practices are either classified (government) or proprietary trade secrets (corporate).[54] Meanwhile, surveillance proponents often make the "nothing to hide" argument, trying to assure you that if your personal details are mundane and boring, with no evidence of treachery, then they will be unnoticed by whoever is watching.[55] That argument can be tough to refute without evidence of actual harm. These are the myriad weaknesses of the pro-privacy strategy against data tracking and surveillance, and this article contends that the strategy is unlikely to overcome emotional and patriotic calls for greater national security, or similarly powerful economic arguments on behalf of jobs and innovation, no matter how hollow or unsupported those arguments might be. On the other hand, the specter of discrimination is easier to actualize and may serve as a stronger civil liberties argument.

Due to the classified and secretive operations of the national security establishment, there have been relatively few reports of actual data discrimination by government thus far; while the inscrutable and untraceable operations of data brokers[56] has led to the same result in the private sector. However, journalists and civil libertarians have found some instances of data discrimination in both sectors, resulting in true hardship for people

53. The inability of an individual to find evidence that he or she was *directly* impacted by data surveillance was an important reason for citizen losses in the aforementioned court cases Jewel v. NSA and Hepting v. AT&T.

54. There have been some attempts by researchers to compile cases of data discrimination, finding evidence that individuals were truly disadvantaged by such practices. Research is gaining traction among critics of the use of big data by the criminal justice system in particular. See, for example, Wexler.

55. This assumption, while common, is a fallacy at many different levels, ranging from the fact that you may be concerned about revealing personal details that have nothing to do with crime or terrorism, to the fact that you do not know who is watching beyond vague categories of "advertisers" or "government officials." This fallacy has been broken down and refuted at length in Solove, 21–32.

56. Boutin.

whose data was appropriated without their consent and possibly even misinterpreted.[57]

In government, accusations of data-driven misinterpretations and discrimination have often been directed at the secretive No Fly List, which was created after the 2001 terrorist attacks to prevent suspicious persons from boarding planes.[58] As of 2013 (the date of the most recent leaked documents), the No Fly List includes more than 47,000 names.[59] A sitting US Congressman, Tom McClintock (R-CA), found himself on this list and could obtain no information on why he was included, finally finding after months of taxpayer-funded investigation that he was mistakenly listed due to having the same name as a member of the Irish Republican Army.[60] On several occasions, the late Senator Ted Kennedy (D-MA) ran afoul of the No Fly List because an unnamed federal agency included an undefined "T. Kennedy" on its list of possible terrorists. Several ordinary American citizens, many of whom are of Middle Eastern descent and have fairly common Islamic names that are likely to belong to other people too, have been placed on the No Fly List with no due process investigation and few possibilities for getting themselves removed from it.[61]

Journalists have found that a person can be placed on the No Fly List for reasons of pure data-driven discrimination and misinterpretation of possible terrorist connections, with little or no actual investigation or vetting. For example, in addition to simply having a name similar to that of an actual known terrorist, one could be placed on the list for a non-terrorism-related arrest record, for having traveled to a country that is believed to harbor terrorists, online statements about terrorism or the politics of

57. This article uses the term "misinterpretation" for the possibility that your personal data will be compiled into a profile that reaches incorrect conclusions about your interests and demographic characteristics. For example, you may have performed online research on depression for a school project, and then an advertiser uses your web usage data to conclude incorrectly that you actually suffer from that illness. This process is also known as "causal inference" in the computer science literature.

There have been some arguments that this problem can be rectified with more data, which could conceivably overcome the weaknesses of the lesser amount of data from which inferences were drawn. However, data experts have found that one cannot assume that more data is better, because it may contain the same "noise" and omissions as the original data set. See, for example, Amatriain.

58. Siegel.

59. Lipsey.

60. Wegmann.

61. Bonner.

fighting it, or even plain old clerical errors.[62] Due to the opaque process of compiling the list, the absence of any mandated appeals procedure for a person to contest their inclusion, or the absence of any means for a worried citizen to even find out if and why they are on it, a federal judge declared the No Fly List and its procedures to be unconstitutional in 2014.[63]

Data-driven discrimination has also been detected in a program used in conjunction by governments and the banking industry. After large banks in the United States and other countries were criticized for (knowingly or unknowingly) handling the accounts of terrorist organizations, the banks turned to a database called World-Check, operated by Thompson Reuters, and endeavored to refuse service to anyone listed therein. The database contains more than two million listings of what it calls "politically exposed persons" and is also used by a wide variety of government security agencies.[64] In 2016, leaked documents revealed that World-Check listed not just individuals but also charities and religious institutions as "terrorists." Thompson Reuters has refused to divulge its process for placing people and organizations in the database under the rationale that it is a proprietary technology, beyond stating that it uses official sources to identify who is a "terrorist." Nevertheless, the leaked documents revealed that individuals and organizations had been labeled as "terrorist" in the database if any unnamed government agency listed them as possible suspects, or even if they had been called "terrorist" online by critics and pundits in social media.[65]

Outside of the United States, evidence indicates that thousands of people and groups have been denied banking services due to being listed in the World-Check database, with no procedure for learning that they were listed or to appeal the listing. Thus far it is unknown if government agencies have discriminated against persons or groups in this database, although the evidence for private-sector discrimination is strong, particularly in banking.[66]

Evidence of data-driven discrimination or misinterpretation outside of government security agencies continues to be revealed, with

62. Lipsey. In one well-reported case, a Stanford University doctoral student was placed on the No Fly List for an unexplained reason, and endured 7 years of legal action against the government before finding that an FBI agent had accidentally checked the wrong box on a form.

63. Latif v. Holder; see also American Civil Liberties Union.

64. Shabibi and Bryant.

65. Pauli.

66. "Why Did HSBC Shut Down Bank Accounts?"

real ramifications for the persons involved. The case of Stacy Snyder is instructive. At age 25, Snyder was about to receive a teaching certificate when her educational institution located a Facebook photo in which she posed with a cup of beer at a party. Even though she was of legal drinking age at the time the photo was taken, and had received no demerits while working toward her teaching degree, officials at Millersville University of Pennsylvania revoked the certification, with only "unprofessional" behavior given as a reason.[67]

Then there is the unnamed young woman in a widely reported story about possibly unethical (or at least insensitive) data interpretation involving Target retail stores. While compiling data on shopping patterns for baby-related items at the online Target store and social media posts about visiting doctors for consultation on pregnancy issues, the Target website calculated that the young woman was either pregnant or likely to be so in the near future due to her interest in the topic. The website then automatically sent promotions and coupons for baby care items to everyone in her contact list, complete with a congratulatory message on the upcoming birth. Unfortunately, the young woman was underage and had not yet revealed the pregnancy to her family; Target's supposedly benign coupon offering caused great family strife while exposing the highly private incident of an underage pregnancy.[68]

Most news headlines on this story trumpeted that Target looked at some detached data snippets and decided for itself that the young woman was pregnant. According to data analytics experts, what really happened was that an algorithm calculated that she was statistically likely to be pregnant and that her social contacts were equally statistically likely to be interested in buying baby-related gifts for her.[69] This distinction may be notable for technicians, but their argument has inadvertently shed a harsh light on the problem because obscure programming code created social and personal impacts with no human intervention. This indicates the new challenges of discrimination in the modern big data society, with real people being affected by opaque technological processes that are shielded by claims of trade secrets (corporate) or classification (government). It might be time to form a new legal outlook on these precise new manifestations of data-driven discrimination.

67. Rosen.
68. Hill.
69. Piatetsky.

A Possible Legislative Movement to Curtail Data Discrimination

Social movements fighting against discrimination have given us some of the most memorable moments of American history. The most obvious example is the civil rights movement inspired by powerful leaders like Martin Luther King, which convinced most of the American political establishment that personal discrimination is unacceptable in a democratic society. King himself often cited the ideals of democracy and the American Constitution to justify an end to discrimination: for example, "Now is the time to make real the promises of democracy. Now is the time to rise from the dark and desolate valley of segregation to the sunlit path of racial justice."[70] King also advocated "bringing our whole nation back to those great wells of democracy which were dug deep by the founding fathers in the formulation of the Constitution and the Declaration of Independence."[71]

Perhaps the greatest legislative achievement of the civil rights movement was the passage of the Civil Rights Act of 1964, which prohibited discrimination in schools, employment, and public accommodations (restaurants, hotels, etc.) based on race, religion, or gender. Crucially for this article's arguments, Congress found, in the Constitution, justifications for exercising its power to illegalize these types of discrimination. The Act was justified via the Fourteenth Amendment right to equal protection under the law; and the Commerce Clause, which allows government regulation of companies that engage in interstate commerce.

The Fourteenth Amendment, particularly its "equal protection" clause, has been used by the American legislature and judiciary to justify rules that prohibit discrimination by government.[72] This is true of the Civil Rights Act of 1964 in particular. As a legal ideal, equal protection means that a law that protects citizens from certain harms should be applied to all citizens equally, while *not* treating everyone equally under the law is itself a form of discrimination. In the words of legal scholar Robert Bork, "The purpose

70. From the speech by Martin Luther King at the Lincoln Memorial in Washington, DC, August 28, 1963.

71. From "Letter from Birmingham Jail" by Martin Luther King, April 16, 1963.

72. The relevant provision is in Section 1 of the Fourteenth Amendment, which reads as follows: "All persons born or naturalized in the United States, and subject to the jurisdiction thereof, are citizens of the United States and of the State wherein they reside. No State shall make or enforce any law which shall abridge the privileges or immunities of citizens of the United States; nor shall any State deprive any person of life, liberty, or property, without due process of law; nor deny to any person within its jurisdiction the equal protection of the laws."

that brought the Fourteenth Amendment into being was equality before the law, and equality, not separation, was written into the law."[73]

The use of the Commerce Clause to prohibit discrimination against individuals by private businesses is lesser-known but surprisingly powerful when put into effect. Federal use of this strategy dates as far back as 1948: when a private business owner in Michigan refused to serve African Americans and claimed that government rules against such practices were unconstitutional, the US Supreme Court ruled that they were indeed constitutional because the Commerce Clause enabled federal regulation of his business across state lines, in turn justifying federal rules that prohibited his discriminatory practices.[74]

These two constitutional rationales—equal protection under the Fourteenth Amendment and federal regulation of interstate business under the Commerce Clause—have been used to support further topical statutes combating discrimination in certain realms by both government and businesses. In either the statutory text or later court rulings, equal protection under the Fourteenth Amendment has served as justification for the Voting Rights Act of 1965 (which prohibits racial discrimination against voters in elections at any level of American government),[75] and Title IX of the Education Amendments of 1972 (which prohibits gender discrimination by colleges that receive federal funding, and are therefore governmental entities).[76]

The Fourteenth Amendment and/or the Commerce Clause have also supported further statutes that prohibit discrimination by private businesses, such as the Fair Housing Act of 1968 (targeted at realtors and landlords),[77] the Equal Credit Opportunity Act of 1974 (targeted at banks and creditors),[78] and the Americans with Disabilities Act of 1990 (applicable to all businesses).[79] Notably for this article's arguments, the Equal Employment Opportunity Commission already makes efforts to find if job applicants have faced rejection for seemingly benign reasons inferred from their personal information; these efforts were inspired by complaints

73. Bork, 82. Here Bork was discussing the seminal Supreme Court precedent on equality before the law: Brown v. Board of Education.

74. Bob-Lo Excursion Company v. Michigan.

75. Note that the right to vote has its own direct protection in the Fifteenth Amendment, while the Fourteenth Amendment prohibits purposefully discriminatory election procedures. Karlan, 8.

76. Lamar, 1111–65.

77. Dubofsky, 152.

78. Gates, 421.

79. Mikochik, 619.

that employers rejected applicants because they lacked vague qualifications like "language skills" after inferring from other sources that they were of a certain race or national origin.[80] While fiendishly difficult to prove, this is the type of data-driven discrimination that is on the increase in the big data society, as piecemeal snippets of personal data are used to compile possibly inaccurate conclusions about a person's characteristics.

All of these antidiscrimination statutes and regulations were arguably inspired by the civil rights movement of the 1960s, as the techniques pioneered by African Americans in their fight against institutional discrimination were picked up by later movements working on behalf of women, disabled persons, and other underrepresented groups. These statutes have also been targeted at discrimination both by the government and by the private sector, indicating the rhetorical power of arguments that discrimination from any source is a problem that America is willing to fight legislatively and judicially. Social movements of the past have achieved new legal protections for previously underrepresented populations, or prohibitions of institutionalized behaviors that could no longer be justified in a democratic society.[81] If and when Americans decide they have had enough of the perceived or actual discrimination caused by pervasive data surveillance, a new social movement focused on a modern conception of equality may lead to similar results.

Conclusion: Future Options

It would be naïve to think that the social movements described in the previous section, and the new laws they achieved, eliminated discrimination altogether. Less-enlightened individuals will continue to treat their fellow citizens unfairly, sometimes with support from laws and regulations (a perennial challenge currently faced by the lesbian, gay, bisexual, and transgender [LGBT] community in particular),[82] and legislation targeting that problem

80. Such inferences are called "proxy criteria" in employment law. Cox, 27, 44. The EEOC does not have precise regulations that illegalize such activity *ex ante*, but performs an evaluation after an individual files a complaint, to determine if such discrimination took place. Ibid., 81–86.

81. Cole, 1–13.

82. For example, Indiana and Arkansas have enacted statutes that protect businesses from claims of discrimination against gay and lesbian customers, justified by the idea that treating such people equally is against the accused business owner's religion. Davey. Also note recent efforts in North Carolina to regulate the use of public restrooms by transgender persons, which adds additional hardship to such people's personal lives. Berman and Phillips.

cannot guarantee that an act of discrimination can be proven and prosecuted. For example, a bank can say that it refused to offer a loan to a woman for legitimate financial reasons, as opposed to outright gender discrimination, and this can be difficult to prove or disprove.[83] But the antidiscrimination statutes inspired by the civil rights movement have at least provided citizens with a way to check institutionalized abuses, and the existence of such laws can create social pressure to prevent abuses before they happen.

In terms of the surveillance and privacy issues discussed throughout this article, the shortage of victories experienced by civil libertarians so far may not be permanent, because legal principles change over time. A variety of Supreme Court Justices—the quintessential authorities on this matter—have said so many times. For example, Felix Frankfurter stated that "If facts are changing, law cannot be static."[84] This is an obvious argument in favor of new legal interpretations necessitated by technological developments (the Internet), political trends (antiterrorism), or business practices (monetization of personal data). Frankfurter's Supreme Court contemporary, William O. Douglas, bluntly proclaimed that "The Constitution is not neutral. It was designed to take the government off the backs of people."[85] Perhaps government is still on our backs in the form of pervasive data surveillance; Douglas would recommend that the Constitution be less neutral on this topic.

Convincing the judiciary and political representatives to relaunch the old antidiscrimination efforts of the 1960s may require an equally robust and committed social movement that remains focused on the task for years, but this may be more practical in light of the inflexible rhetoric and judicial precedents in the realm of privacy as described in this article. It will be a long process, but such movements have been successful many times in American history.[86] In fact, there is already an emerging "data justice" effort in the academic community to draw attention to the larger social issues caused by data discrimination,[87] and perhaps these works could inspire a wide social movement.

---

83. In recent years, some data analytics experts have theorized that human beings are the most discriminatory toward their fellows, and data collection algorithms could be designed to be *less* discriminatory and to avoid human pitfalls. This idea is still in its theoretical infancy, but for interesting examples, see Montoya; Miller.

84. Frankfurter, 6.

85. Douglas, *The Court Years*, 8.

86. Cole, 223–25.

87. See, for example, Dencik et al., 1–12; Taylor; Heeks and Renken, 1–13.

Meanwhile, civil libertarians who continue arguing that data surveillance violates the Fourth Amendment will be saddled by the *Smith v. Maryland* precedent for the foreseeable future. Little did the Supreme Court know in 1979 how this ruling, based on police techniques to find the numbers called by a person using a landline phone, would decades later impede efforts to restrict government and corporate surveillance of practically all personal communications via far more advanced technologies. Some legal scholars have called for the abolishment of the legal doctrines given to us by *Smith v. Maryland*, including the Third Party Doctrine (stating that the Fourth Amendment only applies when the government searches your effects directly, and *not* when it obtains your personal data from companies to which you gave it voluntarily), and the antiquated idea that we use telecommunications services completely voluntarily and therefore have no reasonable expectation of privacy toward the resulting personal data.[88]

Like Judge Richard Leon in *Klayman v. Obama*, this article argues that these doctrines have become outdated and untenable due to modern technological developments and new behaviors by businesses and government officials. Perhaps Judge Leon's resistance to the pull of *Smith v. Maryland* can become the first step in overturning the precedent as no longer viable, which has happened with other Supreme Court precedents in American history. The most noteworthy example of this is the odious "separate but equal" doctrine from *Plessy v. Ferguson*.[89] That doctrine may have been socially and politically acceptable in 1896, but it had become so heavily condemned by civil rights activists and the general public, while enabling institutionalized discrimination with far-reaching social and economic consequences, that the Supreme Court finally (and unanimously) overturned it via *Brown v. Board of Education* in 1954.[90]

This article does not seek to elevate potential data discrimination in the near future to the same level of repugnance as racial injustice in the mid-twentieth century, but there is indeed evidence that changing social perceptions and political trends can lead to the rejection of an existing Supreme Court precedent that had stood for decades. If this could happen with the severe institutionalized discrimination engendered by *Plessy*

88. See, for example, Baker; Issacharoff and Wirshba, 987–1049; Fakhoury.

89. Plessy v. Ferguson. The "separate but equal" doctrine claimed that it was acceptable to require white and black citizens to use separate civic facilities, such as schools and hospitals, as long as those facilities were of equal quality. Poor enforcement of the "equal quality" side of this equation arguably led to the doctrine being overturned 58 years later.

90. Brown v. Board of Education.

v. Ferguson, it is not beyond the realm of possibility that changing perceptions of technology (and how it can be abused by government and businesses) could inspire the judiciary to toss *Smith v. Maryland* into the dustbin of history too.

The *Brown* ruling also cited equal protection under the Fourteenth Amendment to justify the prohibition of racial segregation in public schools, which was now considered an unacceptable form of discrimination by governmental entities. As described in the previous section, that doctrine and the Commerce Clause have been used to justify anti-discrimination laws that seek to eliminate other types of institutionalized discrimination as practiced by both government and the corporate sector. A movement to frame data-driven discrimination and misrepresentation as violations of the Fourteenth Amendment (government) and the Commerce Clause (businesses) might be a viable strategy to achieve new statutes that roll back modern data surveillance practices.

While this is merely a suggestion with no guarantee of future success, it may be time to accept the fact that the privacy argument against data surveillance is not working, and there is plenty of evidence for that. But concerned citizens should not give up because the government and corporate sectors thus far have little incentive to scale back their use of modern technologies to collect our personal data for their own benefit. Our old friend William O. Douglas was eerily prescient on this too: "Big Brother in the form of an increasingly powerful government and in an increasingly powerful private sector will pile the records high with reasons why privacy should give way to national security, to law and order, to efficiency of operation, to scientific advancement and the like."[91] Tools to scale back such behavior by both government and businesses will be necessary, and they have been achieved before when American citizens framed the problem as a matter of discrimination.

This article has argued that a focus on privacy is unlikely to be a successful strategy for civil libertarians and other critics of the American government's surveillance programs or the data tracking practices of private businesses. This is not because privacy is an unimportant value, but because as a value it lacks the rhetorical power to overcome arguments in favor of national security or the profitability of corporations. This article recommends instead that civil libertarians should position freedom from discrimination as a value with more affinity for lawmakers and the

91. Douglas, *Points of Rebellion*, 29.

judiciary, possibly convincing them that the surveillance regime indeed violates American ideals.

BIBLIOGRAPHY

Amatriain, Xavier. "In Machine Learning, What Is Better: More Data or Better Algorithms." *KD Nuggets*, June 2015. Accessed September 2, 2017. http://www.kdnuggets.com/2015/06/machine-learning-more-data-better-algorithms.html.

American Civil Liberties Union. "Court Rules No Fly List Process Is Unconstitutional and Must Be Reformed." Press release, June 24, 2014. Accessed May 10, 2017. http://aclu-or.org/nofly.

Angwin, Julia and Jennifer Valentino-DeVries. "FTC Backs Do-Not-Track System for Web." *Wall Street Journal*, December 2, 2010. Accessed May 2, 2017. http://www.wsj.com/articles/SB10001424052748704594804575648670826747094.

Baker, Stewart. "Drawing a Line on the Third-Party Doctrine." *Washington Post*, May 4, 2014. Accessed May 11, 2017. https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/05/04/drawing-a-line-on-the-third-party-doctrine/?utm_term=.fde295d8c276.

Berman, Mark and Amber Phillips. "North Carolina Governor Signs Bill Repealing and Replacing Transgender Bathroom Law amid Criticism." *Washington Post*, March 30, 2017. Accessed June 19, 2017. https://www.washingtonpost.com/news/post-nation/wp/2017/03/30/north-carolina-lawmakers-say-theyve-agreed-on-a-deal-to-repeal-the-bathroom-bill/?utm_term=.93f22c64cbd4.

Bonner, Raymond. "No-Fly List Riddled with Errors, Impossible to Get Off of." *Informed Comment*, December 16, 2015. Accessed May 10, 2017. https://www.juancole.com/2015/12/riddled-errors-impossible.html.

Bork, Robert H. *The Tempting of America: The Political Seduction of the Law*. New York: Touchstone, 1990.

Boutin, Paul. "The Secretive World of Selling Data about You," *Newsweek*, May 30, 2016. Accessed May 10, 2017. http://www.newsweek.com/secretive-world-selling-data-about-you-464789.

Brookman, Justin. "At Last, Some Progress on Do Not Track." Center for Democracy & Technology, April 24, 2014. Accessed May 2, 2017. https://cdt.org/blog/at-last-some-progress-on-do-not-track/.

Clarke, Conor. "Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?" Essay, *Standard Law Review*, February 2014. Accessed May 10, 2017. https://www.stanfordlawreview.org/online/is-the-foreign-intelligence-surveillance-court-really-a-rubber-stamp/.

Cohen, Gage. "FISA Surveillance Requests Are Almost Never Rejected." *The Daily Caller*, March 6, 2017. Accessed May 10, 2017. http://dailycaller.com/2017/03/06/fisa-surveillance-requests-are-almost-never-rejected/.

Cole, David. *Engines of Liberty: The Power of Citizen Activists to Make Constitutional Law*. New York: Basic Books, 2016.

Cox, Paul N. "Substance and Process in Employment Discrimination Law: One View of the Swamp." *Valparaiso University Law Review* 18 (1983): 21–118.

Davey, Monica, Campbell Robertson, and Richard Perez-Pena. "Indiana and Arkansas Revise Rights Bills, Seeking to Remove Divisive Parts." *New York Times*, April 2, 2015. Accessed June 19, 2017. https://www.nytimes.com/2015/04/03/us/indiana-arkansas-religious-freedom-bill.html.

Davis, Wendy. "Privacy 'Track' Bill Draws Key Support." *Media Post*, February 11, 2011. Accessed May 2, 2017. http://www.mediapost.com/publications/article/144858/.

Dencik, Lina, Arne Hintz, and Jonathan Cable. "Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism." *Big Data & Society*, July–December (2016): 1–12.

Douglas, William O. *The Court Years, 1939–1975: The Autobiography of William O. Douglas*. New York: Vintage Books, 1981.

———. *Points of Rebellion*. New York: Random House, 1970.

Dubofsky, Jean Eberhart. "Fair Housing: A Legislative History and a Perspective." *Washburn Law Journal* 8 (1968): 149–66.

Eggerton, John. "Privacy Bill Followers Don't Keep Their Feelings Private." *Broadcasting & Cable*, February 27, 2015. Accessed May 2, 2017. http://www.broadcastingcable.com/news/washington/privacy-bill-followers-dont-keep-their-feelings-private/138396.

Eichelberger, Erika. "FISA Court Has Rejected .03 Percent of All Government Surveillance Requests." *Mother Jones*, June 10, 2013. Accessed May 10, 2017. http://www.motherjones.com/mojo/2013/06/fisa-court-nsa-spying-opinion-reject-request.

Fakhoury, Hanni. "Smith v. Maryland Turns 35, But Its Health Is Declining." *Electronic Frontier Foundation*, June 24, 2014. Accessed May 11, 2017. https://www.eff.org/deeplinks/2014/06/smith-v-maryland-turns-35-its-healths-declining.

Federal Trade Commission. *In the Matter of GeoCities*, Decision and Order, Docket No. C-3850, February 5, 1999. Accessed May 2, 2017. https://www.ftc.gov/sites/default/files/documents/cases/1999/02/9823015.do_.htm.

———. "Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case." Press release, August 13, 1998. Accessed May 2, 2017. https://www.ftc.gov/news-events/press-releases/1998/08/internet-site-agrees-settle-ftc-charges-deceptively-collecting.

———. *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers*. Report, March 2012. Accessed May 2, 2017. https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Frankfurter, Felix. *Law and Politics: Occasional Papers by Felix Frankfurter*. Edited by Archibald MacLeish and E. F. Prichard, Jr. Gloucester, MA: P. Smith, 1939.

Frieden, Robert. "FCC's Ajit Pai too Focused on Deregulation." *The Hill*, May 9, 2017. Accessed May 10, 2017. http://thehill.com/blogs/pundits-blog/technology/332503-ajit-pai-too-focused-on-deregulation.

Fung, Brian. "Trump Has Signed Repeal of FCC's Internet Privacy Rule. Here's What Happens Next." *Los Angeles Times*, April 4, 2017. Accessed May 10, 2017. http://www.latimes.com/business/la-fi-internet-privacy-fcc-20170404-story.html.

Gates, Margaret J. "Credit Discrimination Against Women: Causes and Solutions," *Vanderbilt Law Review* 27 (1974): 409–41.

Givens, Austen D. "The NSA Surveillance Controversy: How the Ratchet Effect Can Impact Anti-Terrorism Laws." *Harvard Law School National Security Journal*, July 2, 2013. Accessed May 10, 2017. http://harvardnsj.org/2013/07/the-nsa-surveillance-controversy-how-the-ratchet-effect-can-impact-anti-terrorism-laws/.

Greenwald, Glenn. *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. New York: Metropolitan/Henry Holt, 2014.

Greenwald, Glenn and James Ball. "The Top Secret Rules that Allow NSA to Use US Data without a Warrant." *The* Guardian, June 20, 2013. Accessed June 19, 2017. https://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant.

Gross, Grant. "Lawmakers, Companies Question Online Do-Not-Track Proposal." *PCWorld*, December 2, 2010. Accessed May 2, 2017. http://www.pcworld.com/article/212260/article.html.

Hafetz, Jonathan. "How NSA Surveillance Activity Endangers the Fourth Amendment." National Constitution Center, August 13, 2013. Accessed May 5, 2017. http://blog.constitutioncenter.org/2013/08/how-nsa-surveillance-endangers-the-fourth-amendment/.

Heeks, Richard and Jaco Renken. "Data Justice for Development: What Would It Mean?" *Information Development* (2016): 1–13.

Hill, Kashmir. "How Target Figured out a Teen Girl Was Pregnant Before Her Father Did." *Forbes*, February 16, 2012. Accessed May 10, 2017. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#2d08bbac6668.

Issacharoff, Lucas and Kyle Wirshba. "Restoring Reason to the Third Party Doctrine." *Minnesota Law Review* 100 (2016): 987–1049

Karlan, Pamela S. "Section 5 Squared: Congressional Power to Extend and Amend the Voting Rights Act." *Houston Law Review* 44 (2007): 1–31.

Kerr, Orin S. "The Fourth Amendment and the Global Internet." *Stanford Law Review* 67 (2015): 285–329.

Kessler, Glenn. "James Clapper's 'Least Untruthful' Statement to the Senate." *Washington Post*, June 12, 2013. Accessed May 9, 2017. https://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html?utm_term=.490595392940.

Kwoka, Margaret B. "The Procedural Exceptionalism of National Security Secrecy." *Boston University Law Review* 97 (2017): 103–65.

Lamar, Patricia Werner. "The Expansion of Constitutional and Statutory Remedies for Sex Segregation in Education: The Fourteenth Amendment and Title IX of the Education Amendments of 1972." *Emory Law Journal* 32 (1983): 1111–65.

Laney, Douglas. "The Hidden Shareholder Boost from Information Assets." *Forbes*, July 21, 2014. Accessed May 10, 2017. https://www.forbes.com/sites/gartnergroup/2014/07/21/the-hidden-shareholder-boost-from-information-assets/#3ec9e1387628.

Levinson-Waldman, Rachel. "Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public." *Emory Law Journal* 66 (2017): 527–615.

Lichtblau, Eric. "In Secret, Court Vastly Broadens Power of N.S.A." *New York Times*, July 6, 2013. Accessed May 10, 2017. http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.

Lipsey, Sid. "8 Ways You Can End Up On the No-Fly List." *Mental Floss*, September 1, 2015. Accessed May 10, 2017. http://mentalfloss.com/article/68073/8-ways-you-can-end-no-fly-list.

Lyon, David. "Surveillance, Snowden, and Big Data: Capacities, Consequences, Critique." *Big Data & Society* 1, no. 2 (2014): 1–13.

Madrigal, Alexis C. "I'm Being Followed: How Google—and 104 Other Companies—Are Tracking Me on the Web." *The Atlantic*, February 29, 2012. Accessed May 2, 2017. http://www.theatlantic.com/technology/archive/2012/02/im-being-followed-how-google-151-and-104-other-companies-151-are-tracking-me-on-the-web/253758/.

Martin, Alexander J. "US Surveillance Court Declined Less than 2 per cent of Applications." *The Register*, April 21, 2017. Accessed May 10, 2017. https://www.theregister.co.uk/2017/04/21/us_surveillance_court_declined_less_than_2_per_cent_of_applications/.

McVeigh, Karen. "NSA Surveillance Program Violates the Constitution, ACLU Says." *The Guardian*, August 27, 2013. Accessed May 5, 2017. http://www.theguardian.com/world/2013/aug/27/nsa-surveillance-program-illegal-aclu-lawsuit.

Michel, Norbert and James Gattuso. "Are U.S. Telecom Networks Public Property?" The Heritage Foundation, April 8, 2004. Accessed May 10, 2017. http://www.heritage.org/technology/report/are-us-telecom-networks-public-property.

Mikochik, Stephen L. "The Constitution and the Americans with Disabilities Act: Some First Impressions." *Temple Law Review* 64 (1991): 619–28.

Miller, Claire Cain. "Can an Algorithm Hire Better Than a Human?" *New York Times*, June 25, 2015. Accessed September 2, 2017. https://www.nytimes.com/2015/06/26/upshot/can-an-algorithm-hire-better-than-a-human.html?mcubz=1.

Montoya, Carlos. "Algorithms and Discrimination: 'People Discriminate More Than Algorithms Do'/" Blog post, January 26, 2016. Accessed September 2, 2017. http://employers.stellaremploy.com/algorithms-and-discrimination-people-discriminate-more-than-algorithms-do/.

Nissenbaum, Helen. "Protecting Privacy in an Information Age: The Problem of Privacy in Public." *Law and Philosophy* 17, no. 5 (1998): 559–96.

Paul, Rand. "The NSA Is Still Violating Our Rights, Despite What James Clapper Says." *The Guardian*, February 20, 2014. Accessed May 5, 2017. http://www.theguardian.com/commentisfree/2014/feb/20/nsa-violating-american-rights-rand-paul.

Pauli, Darren. "Global 'Terror Database' World-Check Leaked." *The Register*, June 29, 2016. Accessed May 10, 2017. https://www.theregister.co.uk/2016/06/29/global_terror_database_worldcheck_leaked_online/.

Piatetsky, Gregory. "Did Target Really Predict a Teen's Pregnancy? The Inside Story." *Predictive Analytic Times*, May 9, 2014. Accessed May 11, 2017. http://www.predictiveanalyticsworld.com/patimes/target-really-predict-teens-pregnancy-inside-story/3566/.

Poplin, Cody M. "Amici Curiae for FISC Announced." *Lawfare*, December 1, 2015. Accessed May 10, 2017. https://www.lawfareblog.com/amici-curiae-fisc-announced.

Radin, Margaret Jane. *Boilerplate: The Fine Print, Vanishing Rights, and the Rule of Law*. Princeton, NJ: Princeton University Press, 2013.

Rosen, Jeffrey. "The Web Means the End of Forgetting." *New York Times*, July 21, 2010. Accessed May 2, 2017. http://www.nytimes.com/2010/07/25/magazine/25privacy-t2.html?pagewanted=all.

Schmitt, Gary. "A Tale of Two Judges: The NSA on Trial." *The Weekly Standard*, January 13, 2014. Accessed May 5, 2017. http://www.weeklystandard.com/articles/tale-two-judges_773264.html?page=1.

Shabibi, Namir and Ben Bryant. "VICE News Reveals the Terrorism Blacklist Secretly Wielding Power over the Lives of Millions." *Vice*, February 4, 2016. Accessed May 10, 2017. https://news.vice.com/article/vice-news-reveals-the-terrorism-blacklist-secretly-wielding-power-over-the-lives-of-millions.

Siegel, Josh. "Gun Control and the No-Fly List: All You Need to Know." *Newsweek*, December 11, 2015. Accessed May 10, 2017. http://www.newsweek.com/gun-control-and-no-fly-list-all-you-need-know-403821.

Solove, Daniel J. *Nothing to Hide: The False Tradeoff between Privacy and Security*. New Haven, CT: Yale University Press, 2011.

Sprigman, Christopher and Jennifer Granick. "The Secret FISA Court Must Go." *Daily Beast*, July 24, 2013. Accessed May 10, 2017. http://www.thedailybeast.com/articles/2013/07/24/the-secret-fisa-court-must-go.

Stempel, Jonathan. "NSA's Phone Spying Program Ruled Illegal by Appeals Court." *Reuters*, May 7, 2015. Accessed May 5, 2017. http://www.reuters.com/article/2015/05/07/us-usa-security-nsa-idUSKBN0NS1IN20150507.

Strange, Jeff. "A Primer on Wiretaps, Pen Registers, and Trap and Trace Devices." Texas District & County Attorneys Association (2009). http://www.tdcaa.com/node/4813 (last visited May 10, 2017).

Taylor, Linnet. "What Is Data Justice? The Case for Connecting Digital Rights and Freedoms Globally." *Draft Paper* (2017). Accessed September 2, 2017. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2918779.

Vega, Tanzina. "A Call for a Federal Office to Guide Online Privacy." *New York Times*, December 16, 2010. Accessed May 2, 2017. http://www.nytimes.com/2010/12/17/business/media/17privacy.html.

"Why Did HSBC Shut Down Bank Accounts?" *BBC News*, July 28, 2015. Accessed May 10, 2017. http://www.bbc.com/news/magazine-33677946.

Warren, Samuel and Louis Brandeis. "The Right to Privacy." *Harvard Law Review* 4, no. 5: 193–220. (December 15, 1890).

Wegmann, Philip. "Big Mistake: The FBI Flagged this Congressman as a Terrorist." *The National Interest*, July 4, 2016. Accessed May 10, 2017. http://nationalinterest.org/blog/the-buzz/big-mistake-the-fbi-flagged-congressman-terrorist-16841.

Wexler, Rebecca. "When a Computer Program Keeps You in Jail." *New York Times*, June 13, 2017. Accessed June 19, 2017. https://www.nytimes.com/2017/06/13/opinion/how-computers-are-harming-criminal-justice.html.

The White House. "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy." Policy proposal, February 2012. Accessed May 2, 2017. http://itlaw.wikia.com/wiki/Consumer_Data_Privacy_in_a_Networked_World:_A_Framework_for_Protecting_Privacy_and_Promoting_Innovation_in_the_Global_Digital_Economy.

Wilhelm, Alex. "White House Drops 'Consumer Privacy Bill Of Rights Act' Draft." *Tech Crunch*, February 27, 2015. Accessed May 2, 2017. http://techcrunch.com/2015/02/27/white-house-drops-consumer-privacy-bill-of-rights-act-draft/.

Wu, Tim. "Facebook Should Pay All of Us." *The New Yorker*, August 14, 2015. Accessed May 2, 2017. http://www.newyorker.com/business/currency/facebook-should-pay-all-of-us.

Wyatt, Edward. "Legislators Support Internet Privacy, but Question How to Achieve It." *New York Times*, December 2, 2010. Accessed May 2, 2017. http://www.nytimes.com/2010/12/03/technology/03privacy.html.

COURT CASES

American Civil Liberties Union v. Clapper, 959 F.Supp.2d 724 (U.S. Dist., S.D.N.Y, 2013).

Bob-Lo Excursion Company v. Michigan, 333 U.S. 28 (U.S. Supreme Court, 1948).

Brown v. Board of Education, 347 U.S. 483 (U.S. Supreme Court, 1954).

Griswold v. Connecticut, 381 U.S. 479 (U.S. Supreme Court, 1965).

Hepting v. AT&T, 2006 U.S. Dist. LEXIS 41160 (U.S. Dist., N.D. California, 2006).

Jewel v. National Security Agency, 2010 U.S. Dist. LEXIS 5110; Case No. C-08-4373-JSW (U.S. Dist., N.D. California, 2014).

Klayman v. Obama, 957 F. Supp. 2d 1 (U.S. Dist., D.C., 2013).

Latif v. Holder, 969 F. Supp. 2d 1293 (U.S. Dist., Oregon, 2013).

Plessy v. Ferguson, 163 U.S. 537 (U.S. Supreme Court, 1896).

Roe v. Wade, 410 U.S. 959 (U.S. Supreme Court, 1973).

Smith v. Maryland, 442 U.S. 735 (U.S. Supreme Court, 1979).

U.S. v. Davis, 754 F.3d 1205 (11th Circuit, 2014).

U.S. v. Jones, 565 U.S. 400 (U.S. Supreme Court, 2012).