1-2019

# Taking Data

Michael Pollack
*Benjamin N. Cardozo School of Law*, michael.pollack@yu.edu

# Taking Data

*Michael C. Pollack*†

*Technological development has created new forms of information, altered expectations of privacy, and given law enforcement more tools to examine that information and intrude on that privacy. One crucial facet of these changes involves internet service providers (ISPs): as people expose more of their lives to their ISPs—all the websites they visit, people they communicate with, emails they send, files they store, and more—law enforcement efforts to access that data become more and more common. But scholars and policymakers alike recognize that the existing statutory frameworks governing those efforts are based on obsolete technology and strike balances that are difficult to justify and that are both over- and underprotective of privacy.*

*This Article proposes a new approach to regulating government investigations of data that has been shared with ISPs—one that is inspired by a legal tool designed to achieve the very balance between public benefits and private burdens that has thus far proven elusive. This tool is the Takings Clause. Under the Takings Clause, the government can acquire private property, including intangible and intellectual property, but this wide-ranging power is disciplined by the requirement that the government pursue a public purpose and pay just compensation for the property it takes. This Article argues that adapting these features of the takings framework to govern the investigation of ISP-held data would be feasible, theoretically and doctrinally sound, and normatively desirable.*

*In making this argument, this Article addresses one of the primary problems with the various existing mechanisms by which government conducts investigations online, which is that the costs of diminished privacy fall on the civilian targets of those investigations. The result is that law enforcement does not adequately consider these costs when making investigation decisions. Acquiring information under a takings-inspired regime, by contrast, would trigger a requirement to compensate the person whose privacy has been diminished and thus impose a direct cost on the government entity conducting the investigation. This obligation to pay would force the investigating entity to be more thoughtful*

---

† Assistant Professor of Law, Benjamin N. Cardozo School of Law. I am grateful to Miriam Baer, William Baude, Maureen Brady, Christopher Buccafusco, David Carlson, Nestor Davidson, Myriam Gilles, Ben Grunwald, Daniel Hemel, Michael Herz, Orin Kerr, Timothy Mulvaney, Luke Norris, John Rappaport, Shelley Ross Saxer, Ric Simmons, Edward Stein, James Stern, Stewart Sterk, Lior Strahilevitz, Matthew Tokson, Felix Wu, Stephen Yelderman, and participants in the AALS New Voices in Property Law Workshop, Cardozo Junior Faculty Workshop, Law and Society Annual Meeting, Mid-Atlantic Junior Faculty Forum at the University of Richmond Law School, and Southeastern Association of Law Schools New Scholars Workshop for their guidance, suggestions, comments, and critiques. I thank the Stephen B. Siegel Program in Real Estate Law for research support.

*about which investigations are the highest priorities, most likely to yield valuable information, and most tailored to achieve their purposes.*



## INTRODUCTION

On February 16, 2016, a federal court ordered Apple to "assist law enforcement agents in enabling the search" of an iPhone that had been lawfully seized during the investigation into a mass shooting in San Bernardino, California.[1] Though this was not the first time that federal law enforcement had attempted to compel Apple to unlock an iPhone seized during the course of a criminal investigation, it was one of the first times that Apple resisted.[2] CEO Tim Cook took the matter public, issuing a statement that expressed Apple's opposition to the court's order and called for "public discussion" about the importance of data security.[3]

Sure enough, people started to pay attention.[4] Indeed, the incident fit into and catalyzed a broader conversation about the

---

1 Order Compelling Apple, Inc to Assist Agents in Search, *In re Search of an Apple iPhone Seized during Execution of a Search Warrant on a Black Lexus IS300, California License Plate 35KGD203*, No 15-0451, *1 (CD Cal filed Feb 16, 2016) (available on Westlaw at 2016 WL 618401).

2 See *In re Order Requiring Apple, Inc to Assist in the Execution of a Search Warrant Issued by This Court*, 149 F Supp 3d 341, 346–47 (EDNY 2016); Steven R. Morrison, *Breaking iPhones under CALEA and the All Writs Act: Why the Government Was (Mostly) Right*, 38 Cardozo L Rev 2039, 2041 (2017).

3 Tim Cook, *A Message to Our Customers* (Apple, Feb 16, 2016), archived at http://perma.cc/68X7-SDLL.

4 That is not to say that their positions, however sincerely taken, were entirely consistent. Public opinion polls showed differing levels of support for Apple's position

relationship among law enforcement, public safety, new technology, and privacy, all of which became front-page news.[5] One federal judge emphasized that the need for such a discussion "becomes more pressing daily, as the tide of technological advance flows ever farther past the boundaries of what seemed possible even a few decades ago."[6] Politicians and industry groups deployed, presidential candidates took positions, and even the United Nations High Commissioner for Human Rights weighed in.[7]

This larger effort to adapt privacy and law enforcement to new technology continues, but unfortunately in somewhat schizophrenic fashion. For example, in a "rare and remarkable display" of both bipartisanship and action, the House of Representatives has thrice passed the Email Privacy Act (EPA), a bill designed to increase the protection afforded to the content of emails stored by internet service providers (ISPs), with unanimous or near-unanimous support.[8] But the bill has never

---

and the government's efforts, and some polls even showed some irreconcilable beliefs—that Apple was right to resist the government but that the government should be able to look at cell phone data "to protect against terror threats." Philip Elmer-DeWitt, *Apple vs. FBI: What the Polls Are Saying—Updated* (Fortune, Feb 23, 2016), archived at http://perma.cc/NP9S-57GE.

5 See, for example, Michael D. Shear, *In Nod to Law Enforcement in Apple Case, Obama Ends Attempt to Straddle Privacy Divide* (NY Times, Feb 19, 2016), archived at http://perma.cc/PU7W-LJ4C; Todd C. Frankel and Ellen Nakashima, *Showdown over iPhone Reignites the Debate around Privacy* (Wash Post, Feb 19, 2016), archived at http://perma.cc/8PN7-YVWH. See also Bryan H. Choi, *For Whom the Data Tolls: A Reunified Theory of Fourth and Fifth Amendment Jurisprudence*, 37 Cardozo L Rev 185, 247 (2015).

6 *In re Order Requiring Apple, Inc to Assist*, 149 F Supp 3d at 376.

7 See, for example, Sam Thielman and Danny Yadron, *Crunch Time for Apple as It Prepares for Face-Off with FBI* (The Guardian, Feb 27, 2016), archived at http://perma.cc/DQK7-23BQ. For example, then-candidate Donald Trump called in February 2016 for a "[b]oycott [of] all Apple products until such time as Apple gives cell-phone info to authorities regarding radical Islamic terrorist couple from Cal." @realDonaldTrump (Twitter, Feb 19, 2016), archived at http://perma.cc/PZ69-SCUT. See also Press Release, United Nations Human Rights, Office of the High Commissioner, *Apple-FBI Case Could Have Serious Global Ramifications for Human Rights: Zeid* (United Nations Human Rights, Mar 4, 2016), archived at http://perma.cc/HLY5-4W2F.

8 Editorial, *The House Votes Unanimously to Strengthen Email Privacy* (NY Times, Apr 29, 2016), archived at http://perma.cc/732B-6LBQ. The first time the bill passed, in April 2016, it did so on a unanimous recorded vote. Email Privacy Act, HR 699, 114th Cong, 2d Sess, in 162 Cong Rec H 2035 (daily ed Apr 27, 2016). The second time the bill passed, in February 2017, it did so on a voice vote. Email Privacy Act, HR 387, 115th Cong, 1st Sess, in 163 Cong Rec H 992 (daily ed Feb 6, 2017). The third time the bill passed, in May 2018, it did so as an amendment to the annual National Defense Authorization Act (NDAA), Pub L No 115-232, 132 Stat 1636 (2018), which passed the

come to a vote in the Senate,[9] and in the wake of a different mass shooting in Orlando, the Senate actually considered (though ultimately rejected) a proposal to *decrease* the level of protection afforded to internet browsing history and information like email addresses with which a person has communicated.[10]

Of course, to recount examples like these is not to indict Congress for being torn—or, perhaps, even "paralyzed."[11] Indeed, as understandable as the impulse to protect privacy from new technology is, that impulse necessarily sits in tension with legitimate law enforcement and public safety considerations that have their own strong political salience.[12] But lurching between increasing and decreasing electronic privacy in response to whatever the latest headlines may prompt is a recipe for bad policy—in both directions.[13] These kinds of binary reactions are apt to result in a system that is both under- and overprotective of privacy relative to real law enforcement needs.[14] And yet it is "apparent to *everyone* involved" that our laws in this area are

---

House on a vote of 351 to 66. NDAA, HR 5515, 115th Cong, 2d Sess, in 164 Cong Rec H 4721 (daily ed May, 24, 2018).

9 On the demise of HR 699, see Erin Kelly, *Senate Derails Bill to Rein in Email Surveillance* (USA Today, June 9, 2016), archived at http://perma.cc/ZDG4-PHY2. HR 387 languishes in committee in the Senate. See *All Actions H.R.699—114th Congress (2015–2016)* (Library of Congress, Apr 28, 2016), archived at http://perma.cc/N3CB-ALSP. Finally, when the Senate took up the NDAA in 2018, it stripped out the language containing the Email Privacy Act. See NDAA, HR 5515, 115th Cong, 2d Sess, in 164 Cong Rec S 3961 (daily ed June 18, 2018).

10 See Karoun Demirjian, *After Orlando, Senate Rejects Plan to Allow FBI Web Searches without Court Order* (Wash Post, June 22, 2016), archived at http://perma.cc/UFJ7-UNEY.

11 Barry Friedman, *Unwarranted: Policing without Permission* 238 (Farrar, Straus, and Giroux 2017).

12 See id at 237. See also William Baude and James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 Harv L Rev 1821, 1857 (2016) ("[W]hat is notable about privacy is that it is also not obvious that it is an unalloyed good. And indeed sometimes it is affirmatively bad.").

13 See Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 Minn L Rev 577, 632–33 (2017) ("Legislative measures addressing perceived shortcomings in data privacy are almost universally perceived as outdated, incomplete, insufficiently rigorous, or some combination of the three. . . . Instead, when Congress has acted at all, it has done so piecemeal, through a series of narrowly targeted statutes.").

14 As President Barack Obama put it,

> You cannot take an absolutist view on [encryption]. If your view is strong encryption no matter what and we can and should create black boxes, that does not strike the balance that we've lived with for 200 or 300 years. And it's fetishizing our phones above every other value. That can't be the right answer.

Sam Machkovech, *Obama Weighs in on Apple v. FBI: "You Can't Take an Absolutist View"* (Ars Technica, Mar 11, 2016), archived at http://perma.cc/DB6K-PCUU.

obsolete or inadequate, and that how to update those statutes remains a crucial question in desperate need of an answer.[15]

This Article looks beyond these unsatisfactory either/or statutory proposals to identify and evaluate an underappreciated way in which government might be channeled when it seeks access to electronic data. This solution is not simply a variation on the usual themes of toggling protection up or down by requiring a warrant, eliminating an exception, creating a new exception, or the like. Instead, it is a statute inspired by an existing governmental power that has gone untapped in this arena—one that, in practice, contains features that are geared toward relatively more finely calibrated governmental action and that are designed to balance public benefits with private burdens: the power of eminent domain.[16] The Fifth Amendment's Takings Clause provides that government may "take[ ]" private property "for public use" so long as "just compensation" is rendered to the dispossessed former property owner.[17] While the most salient example of property subject to a taking is real property, the courts have made clear that personal property—including private papers, such as President Richard Nixon's White House papers[18]—and intellectual property are equally within the ambit of the Takings Clause.[19] This Article's argument is thus a simple one: if the government wants data stored on a server at Google, for example, it should be required to "take" it.[20]

First, as this Article argues in more detail below, a takings-inspired statute that authorized the government to acquire data

---

15 Friedman, *Unwarranted* at 238 (cited in note 11). See also Baude and Stern, 129 Harv L Rev at 1853 (cited in note 12); Fred H. Cate and Stephen A. Saltzburg, *Should Law Enforcement Have to Get a Warrant to Obtain Stored Emails?* (Wall St J, May 22, 2016), online at http://www.wsj.com/articles/should-law-enforcement-have-to-get-a-warrant-to-obtain-stored-emails-1463968801 (visited Oct 20, 2018) (Perma archive unavailable).

16 See *Armstrong v United States*, 364 US 40, 49 (1960) ("The Fifth Amendment's guarantee that private property shall not be taken for a public use without just compensation was designed to bar Government from forcing some people alone to bear public burdens which, in all fairness and justice, should be borne by the public as a whole.").

17 US Const Amend V.

18 See *Nixon v United States*, 978 F2d 1269, 1287 (DC Cir 1992).

19 See *Horne v Department of Agriculture*, 135 S Ct 2419, 2426 (2015) (holding that the Takings Clause "protects 'private property' without any distinction between different types," and explaining that "[t]he Government has a categorical duty to pay just compensation when it takes your car, just as when it takes your home"); *Ruckelshaus v Monsanto Co*, 467 US 986, 1003–04 (1984) (holding that trade secrets are protected by the Takings Clause).

20 The claim here is not that the Fifth Amendment presently requires the government to use its takings power in this context but rather that a statutory regime inspired by the takings power would be a feasible and beneficial innovation.

held by third parties like ISPs for law enforcement purposes would be both doctrinally and theoretically sound, doing little violence to the law of takings, the law of criminal procedure, and theories of property law more broadly.[21] Once guided by legislation, the government would do what it already does for ordinary takings for land acquisition, development, private sector regulation, and more: identify the property in question, file a declaration of a taking of that property in federal court, and pay the required compensation. In making this argument, this Article contributes a new perspective on how private data might be understood as property or property-like and demonstrates that the concerns raised by scholars who resist such property-based perspectives are either misplaced or avoidable.[22]

The second piece of the Article is more normative. For those who might accept a certain degree of propertizing with respect to private data, fears may linger about the implications of such a move in the law enforcement context. This Article shows not only that there is little to fear but that there is in fact much to be gained.[23] If the government were forced to investigate in accordance with a takings-style regime, it would have to pay for the data it wants, publicly account for those payments, and do so while embracing the exercise of one of the most politically unpopular governmental powers. Acquiring a warrant is often quite cheap; buying actual data can be costly.[24] And in this

---

21 See Part II.

22 See Part II.B.

23 In a 2004 article, Professor Paul Schwartz asserted in passing that "law enforcement access to personal data should not be structured through recourse to a propertized model" and that "the government's acquisition and use of personal data should not be subject to eminent domain or Takings Clause jurisprudence." Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 Harv L Rev 2056, 2096 (2004). I argue that there is little theoretical, doctrinal, or normative reason why either of these claims is right. See Part II.B (making theoretical and doctrinal arguments); Part III.A (making normative arguments).

24 See Part III.B. Compare *Missouri v McNeely*, 569 US 141, 154–55 (2013) (observing that states have "streamline[d] the warrant process" and that technology also "allow[s] for the more expeditious processing of warrant applications" by remote means, including "telephonic or radio communication, electronic communication such as e-mail, and video conferencing"); FRCrP 41(d)(3) (providing that a magistrate judge may issue a warrant "based on information communicated by telephone or other reliable electronic means"); Friedman, *Unwarranted* at 138 (cited in note 11) (describing the ease of acquiring warrants via telephone or computer); Andrew H. Bean, *Swearing by New Technology: Strengthening the Fourth Amendment by Utilizing Modern Warrant Technology while Satisfying the Oath or Affirmation Clause*, 2014 BYU L Rev 927, 935–37 (observing that delays in the warrant procurement process have been drastically reduced by modern modes of communication), with Leslie R. Masterson and Jeremy R. Wallace, *The Manson*

context, making government bear those costs has the potential to substantially change government behavior.

As things stand now, the costs of diminished privacy fall on the civilian targets of investigations: the citizens or private entities whose privacy is intruded on. Those costs are significant,[25] but they are generally not borne by the government, which means that they are generally not considered by the government when it makes investigatory decisions. Employing a takings-based approach, by contrast, would house the task of balancing the costs and benefits of privacy invasions for law enforcement purposes within entities actually responsible for both bearing those costs and receiving those benefits. The government would thus be forced to internalize the real privacy-related externalities generated by its investigative efforts and to therefore be more thoughtful about prioritizing those efforts and tailoring their scope. Such an approach would also provide finer calibration, as I note above, because these judgments would be made at the retail level after consideration of the specific need for (and expected benefits of) a particular intrusion, rather than resolved in reactive, one-size-fits-all legislative enactments.

While scholars such as Professor Daryl Levinson have cast some doubt on the notion that government can be made to change its behavior in this manner,[26] this Article meets that

*Tapes: Evidence of Murder in Bankruptcy Court*, 36 Am Bankr Inst J 12, 13 (Nov 2017) (noting that tapes of an interview conducted with Charles Denton Watson, an associate of mass murderer Charles Manson, sold for $48,000); Jennifer R. Williams, *Beyond* Nixon*: The Application of the Takings Clause to the Papers of Constitutional Officeholders*, 71 Wash U L Q 871, 871 (1993) (noting that the Watergate tapes were valued at $2.5 million and that "prices for a relatively routine letter or memorandum from President Nixon's office range from $500 to $5,000"); Schwartz, 117 Harv L Rev at 2056 n 1 (cited in note 23) (noting that marketers are estimated to digest $75 billion of personal information each year). Of course, relative to *warrantless* searches, searches predicated on warrants are more costly for law enforcement officers. See Max Minzner, *Putting Probability Back into Probable Cause*, 87 Tex L Rev 913, 926 (2009) ("Searches pursuant to a warrant are more expensive for law enforcement than those without warrants."). See also Miriam H. Baer, *Pricing the Fourth Amendment*, 58 Wm & Mary L Rev 1103, 1134 (2017). My point is that, in absolute terms, the costs of procuring warrants are low and the costs of acquiring property are likely to be at least somewhat higher.

[25] See Friedman, *Unwarranted* at 142 (cited in note 11) (noting the lack of trust in the police and feelings of "anger," "fright," and "humiliation"). See also Orin S. Kerr, *An Economic Understanding of Search and Seizure Law*, 164 U Pa L Rev 591, 595 (2016) (noting that investigatory techniques "impose societal costs in the form of civil liberties violated, property destroyed, and peace and stability disrupted").

[26] Daryl J. Levinson, *Making Government Pay: Markets, Politics, and the Allocation of Constitutional Costs*, 67 U Chi L Rev 345, 359 (2000) (arguing that various barriers prevent government agents from responding to pecuniary incentives).

objection by drawing on evidence that law enforcement actors in fact are generally attuned to cost and by arguing that financial costs are particularly likely to translate into salient political and bureaucratic costs under the specific regime I propose.[27] So, far from handing the government the ability to blow a server-farm–sized hole in privacy, taking data has the potential to *decrease* the amount of data sought by the government and to consequently *increase* the data privacy enjoyed by American citizens.[28] At a minimum, this approach could better optimize the levels of both privacy and law enforcement intrusions.

This Article proceeds in three parts. Part I sets out the laws that presently shape the government's investigatory power in this arena—the Fourth Amendment,[29] the All Writs Act[30] (AWA), and the Stored Communications Act[31] (SCA)—as well as new proposals like the EPA.[32] It explores the ways in which each one is unequal to the moment, underprotective of privacy in favor of law enforcement, overprotective of privacy at the expense of law enforcement, or some combination of the three. Part II makes the doctrinal and theoretical case for taking data instead. It explains the operation of the Takings Clause, reveals how a takings-inspired approach could be employed in the law enforcement context, and fleshes out how private data may be thought of in property-like terms. To that end, it presents a model statutory framework that the government could use to acquire data in the possession of ISPs or other cloud computing

---

27 See Part III.A.

28 This proposal thus shares a common root with Professor Miriam Baer's recent proposal that local police departments pay a fee to a federal agency reflecting the volume and potential harm of their search activity. Baer, 58 Wm & Mary L Rev at 1137 (cited in note 24). It also fits with a piece of Professors Bernard Harcourt and Tracey Meares's randomized search proposal, in which people would be compensated for police encounters that are ultimately determined to be unreasonable. Bernard E. Harcourt and Tracey L. Meares, *Randomization and the Fourth Amendment*, 78 U Chi L Rev 809, 817, 868–70 (2011). Like these scholars, I think there is much potential in corrective pricing schemes, but this Article seeks to further develop this sort of intervention by drawing attention to property law's potential in this arena, and to the property-like nature of private data, by leveraging this distinct property-based framework and by proposing a scheme that can offer even more fine-grained pricing and thus achieve more fine-tuned outcomes. For another recent example of a property law contribution to the Fourth Amendment arena and Fourth Amendment doctrine, see generally Maureen E. Brady, *The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection*, 125 Yale L J 946 (2016).

29 US Const Amend IV.

30 28 USC § 1651.

31 Pub L No 99-508, 100 Stat 1848 (1986), codified as amended at 18 USC § 2701 et seq.

32 Email Privacy Act, HR 387, 115th Cong, 1st Sess, in 163 Cong Rec H 992 (daily ed Feb 6, 2017).

services like Google.[33] Part III evaluates that framework normatively, offers a more fulsome defense of it, and unpacks its potential as a viable way to balance privacy and security in a climate of rapidly transforming technology.

## I. THE EXISTING TOOLBOX FOR DATA SEARCHES

The government's ability to examine data held by ISPs presently comprises three basic pieces. The first piece consists of its traditional powers as cabined by the Fourth Amendment; the second, its abilities under the 1789 All Writs Act; and the third, its options under the 1986 Stored Communications Act. This Part sets out the metes and bounds of these three mechanisms, discusses their limitations, and closes by discussing some recent proposals for reforms and additions.

### A. The Fourth Amendment

The Fourth Amendment prohibits "unreasonable searches and seizures" of one's "person[ ], houses, papers, and effects" and provides that a warrant for such a search may be issued by a neutral magistrate upon a showing of "probable cause."[34] Current doctrine provides that the government conducts a "search" within the meaning of the Fourth Amendment if it violates a person's "reasonable expectation of privacy."[35] Data and electronic information are just as susceptible to this form of investigation as any other kind of evidence. Accordingly, if the government wishes to access a person's data, it may do so by getting a warrant supported by probable cause or by availing itself of one of the doctrinal exceptions to the warrant requirement.[36]

The ordinary regime for investigatory searches thus maps, at least as a first cut, onto the world of ISP-held data. But it does so in ways that are ultimately not particularly protective of privacy. This is largely because the Supreme Court has long held in a variety of contexts that a person has no "reasonable

---

[33] For ease of reference, this Article simply refers to ISPs as a catchall going forward.

[34] US Const Amend IV.

[35] *Katz v United States*, 389 US 347, 360 (1967) (Harlan concurring).

[36] See *Kentucky v King*, 563 US 452, 459 (2011) (noting that "a warrant must generally be secured" but that, because the "ultimate touchstone of the Fourth Amendment is 'reasonableness[,]' . . . the warrant requirement is subject to certain reasonable exceptions").

expectation of privacy" in information she "voluntarily convey[s]" to a third party.[37] As a result, under this "third-party doctrine," once information is shared with a third party—even when it is shared "on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed"—it is no longer protected by the terms of the Fourth Amendment.[38] To choose a case with some factual similarities to the problems this Article tackles, the Court held in *Smith v Maryland*[39] that a person has no reasonable expectation of privacy in the numbers he dials on his telephone because he voluntarily "convey[s] that number to the telephone company."[40] Similarly, it would appear that at least some information a person communicates to her ISP—her network address, sites visited, individuals emailed, and the like—is unprotected by the Fourth Amendment.[41] This is good news for the government, which accordingly does not need a warrant for such information, but potentially distressing news for some citizens. Giving voice to the latter view, Justice Sonia Sotomayor has cautioned that "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties"—precisely because, at least to her mind, "[t]his approach is ill suited to the

---

37 *United States v Miller*, 425 US 435, 442 (1976). See also *Smith v Maryland*, 442 US 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

38 *Miller*, 425 US at 443. See, for example, *California v Greenwood*, 486 US 35, 40–41 (1988) (finding no reasonable expectation of privacy in garbage left on the street and "readily accessible to animals, children, scavengers, snoops, and other members of the public") (citations omitted); *California v Ciraolo*, 476 US 207, 213–14 (1986); *Katz*, 389 US at 351.

39 442 US 735 (1979).

40 Id at 743.

41 See, for example, *United States v Christie*, 624 F3d 558, 573–74 (3d Cir 2010) (holding that an IP address is not protected); *United States v Forrester*, 512 F3d 500, 509–11 (9th Cir 2008) (sites visited and individuals emailed); *United States v Lifshitz*, 369 F3d 173, 190 (2d Cir 2004) (internet transmissions that have already arrived). Exactly where the line is drawn, particularly with respect to content information, has proven murky, though the weight of authority suggests that law enforcement needs a warrant to access the content of email communication. See, for example, *United States v Warshak*, 631 F3d 266, 288 (6th Cir 2010) (holding that the Fourth Amendment requires the government to obtain a warrant in order to access stored email content); Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo Wash L Rev 1208, 1210–11 (2004) ("It is too early to tell whether courts will adopt the same rationale for content information, such as e-mails. . . . Either way, it remains unclear today whether files held by ISPs on behalf of their users can retain a Fourth Amendment 'reasonable expectation of privacy.'").

digital age. . . . I for one doubt that people would accept without complaint the warrantless disclosure to the government of a list of every Web site they had visited in the last week, or month, or year."[42]

Even so, the Court has thus far declined invitations to revisit wholesale the third-party doctrine. In its recent decision in *Carpenter v United States*,[43] the Court considered whether records of cell-site location information in the possession of a wireless carrier were protected by the Fourth Amendment.[44] And while the Court held that they were so protected, it expressly did "not disturb" *Smith* and its third-party doctrine progeny.[45] Rather, it emphasized how "narrow" its conclusion was and how substantially that conclusion turned on the fact that cell-site location information is "unique" in terms of its power to reveal an "exhaustive chronicle" of a person's daily life and its intimate details.[46] There is a "world of difference," the Court said, between such information and everything else ordinarily—and still—subject to the third-party doctrine.[47] Accordingly, the privacy gap created by the third-party doctrine is likely to remain with us for some time—even if subject to ad hoc clawbacks, such as *Carpenter*, or other efforts to reshape it from time to time.[48]

---

42 *United States v Jones*, 565 US 400, 417–18 (2012) (Sotomayor concurring).

43 138 S Ct 2206 (2018).

44 Id at 2211.

45 Id at 2220.

46 Id at 2219, 2220. See also id at 2216 (calling cell-site records "qualitatively different" than run-of-the-mill information subject to the third-party doctrine); id at 2217 (emphasizing that time-stamped cell-site location information provides an especially "intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations'"), quoting *Jones*, 565 US at 415 (Sotomayor concurring); *Carpenter*, 138 S Ct at 2218 (pointing out that cell-site location information allows the government to "travel back in time to retrace a person's whereabouts"); id at 2220 (describing the power of cell-site location information to provide a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years"); id at 2222 (calling cell-site location information "an entirely different species" of record). Indeed, the Court was so taken with the distinct nature of cell-site location information that it used the word "chronicle" to illustrate that information's power five times in its relatively short opinion. Id at 2211, 2216, 2219, 2220.

47 *Carpenter*, 138 S Ct at 2219.

48 See id at 2224, 2232 (Kennedy dissenting) (criticizing, on behalf of three justices, the Court's "illogical" line drawing around cell-site location information and arguing in favor of a straightforward application of *Smith* and the third-party doctrine rather than "category-by-category balancing"); Baude and Stern, 129 Harv L Rev at 1872 (cited in note 12) (arguing that "it is hard to imagine abandoning the third-party doctrine altogether"); Erin Murphy, *The Case against the Case for Third-Party Doctrine: A Response to Epstein and Kerr*, 24 Berkeley Tech L J 1239, 1252–53 (2009) (suggesting a "sliding

Moreover, under the umbrella of another exception to the warrant requirement, the government can sometimes access electronically transmitted and remotely stored information with just a subpoena served on the third-party possessor of that information (such as an ISP)[49] even though such subpoenas do not require probable cause and instead are evaluated under a much less searching standard akin to reasonableness.[50] The process of issuing a subpoena is also strikingly simple for the government and features few, if any, checks.[51] To take the example of a grand jury subpoena, a prosecutor drafts the subpoena herself;[52] can compel the production of any "books, papers, documents,

---

scale of protections" that could turn on a "hierarchy of disclosures" to third parties and on the disclosures' degrees of voluntariness). But see *Carpenter*, 138 S Ct at 2262–64 (Gorsuch dissenting) (criticizing the third-party doctrine as well as *Katz* itself).

49 See Friedman, *Unwarranted* at 234 (cited in note 11) ("If the government wants it, the Supreme Court says, it need only subpoena it from whoever happens to be holding it. No warrant is needed and no probable cause required, thank you very much."); Kerr, 72 Geo Wash L Rev at 1211–12 (cited in note 41):

> [T]he Fourth Amendment generally allows the government to issue a grand jury subpoena compelling the disclosure of information and property, even if it is protected by a Fourth Amendment "reasonable expectation of privacy." . . . [S]o long as the third party is in possession of the target's materials, the government may subpoena the materials from the third party without first obtaining a warrant based on probable cause.

In *Carpenter*, the Court arguably muddied the waters relating to the government's subpoena power, saying, on the one hand, that it "has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy" and, on the other, that "[t]he Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations." *Carpenter*, 138 S Ct at 2221, 2222. Time will tell how dramatic a shift this proves to be. See id at 2255 (Alito dissenting) (noting that the only reason the Court, in the majority's words, "has never held that the Government may subpoena third parties for records in which the suspect has a reasonable expectation of privacy" is that, until the *Carpenter* decision, "defendants categorically had no" protected interest in such records); Orin Kerr, *Does* Carpenter *Revolutionize the Law of Subpoenas?* (Lawfare, June 26, 2018), archived at http://perma.cc/C28R-UY27 (suggesting that *Carpenter* will ultimately not have a "major impact" on subpoenas).

50 See *United States v R. Enterprises, Inc*, 498 US 292, 297 (1991) ("[T]he Government cannot be required to justify the issuance of a grand jury subpoena by presenting evidence sufficient to establish probable cause because the very purpose of requesting the information is to ascertain whether probable cause exists."); *See v City of Seattle*, 387 US 541, 544–45 (1967) (holding that only "rather minimal limitations" are constitutionally required "in the case of investigative entry upon commercial establishments" and that an administrative agency may subpoena records consistent with the Fourth Amendment so long as the subpoena is "sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome").

51 Andrew E. Taslitz and Stephen E. Henderson, *Reforming the Grand Jury to Protect Privacy in Third Party Records*, 64 Am U L Rev 195, 199 (2014).

52 FRCrP 17(a).

data, or other objects" she designates;[53] and can do so "even just because [she] wants assurance that [the law] is not" being violated.[54] The recipient of such a subpoena—here, the ISP—generally has little standing to challenge that subpoena, and even the types of objections that a recipient is permitted to raise usually fail.[55]

Finally, in addition to these exceptions to the protection offered by the Fourth Amendment, the fact remains that the Fourth Amendment—even when it does apply—is not particularly effective at disciplining law enforcement or protecting privacy. This is because there are often no real penalties attached to its violation. The central penalty is the exclusion from trial of evidence unlawfully collected, but even when that penalty applies, its efficacy as a deterrent for law enforcement agencies or for individual officers is, as many scholars have long argued, highly questionable.[56] Moreover, the exclusionary rule is riddled

---

53 FRCrP 17(c)(1).

54 *United States v Morton Salt Co*, 338 US 632, 643 (1950). See also *R. Enterprises*, 498 US at 297 (explaining that the purpose of a subpoena is to permit a grand jury "to inquire into all information that might possibly bear on its investigation until it has identified an offense or has satisfied itself that none has occurred").

55 See *United States v Calandra*, 414 US 338, 345 (1974) (stating that a grand jury witness "is not entitled to urge objections of incompetency or irrelevancy . . . to challenge the authority of the court or of the grand jury or to set limits to the investigation that the grand jury may conduct"), quoting *Blair v United States*, 250 US 273, 282 (1919) (quotation marks omitted); Christopher Slobogin, *Subpoenas and Privacy*, 54 DePaul L Rev 805, 811 (2005).

56 See, for example, Oren Bar-Gill and Barry Friedman, *Taking Warrants Seriously*, 106 Nw U L Rev 1609, 1622 (2012) ("To say that the exclusionary rule is a failure is to risk hyperbole and understatement at the same time."); id at 1625:

> The issue is straightforward: the ostensible purpose of the exclusionary rule is to deter police misconduct, but the mechanism is a lost conviction. The evidence and the literature suggest that convictions are low on the list of things police are rewarded or punished for. Police care about arrests, not convictions.

See also Dallin H. Oaks, *Studying the Exclusionary Rule in Search and Seizure*, 37 U Chi L Rev 665, 755 (1970):

> As a device for directly deterring illegal searches and seizures by the police, the exclusionary rule is a failure. There is no reason to expect the rule to have any direct effect on the overwhelming majority of police conduct that is not meant to result in prosecutions, and there is hardly any evidence that the rule exerts any deterrent effect on the small fraction of law enforcement activity that is aimed at prosecution.

See also Christopher Slobogin, *Why Liberals Should Chuck the Exclusionary Rule*, 1999 U Ill L Rev 363, 369, 381 (noting that "virtually all the studies [ ] suggest that, for many police officers, concern over the [exclusionary] rule is not a significant influence when contemplating a search or seizure," and likewise concluding that "exclusion is not a strong behavior-shaping mechanism in the typical search and seizure setting"); id at

with exceptions of its own that further erode its disciplinary potential.[57] But even if the exclusionary rule were more solid, it would offer no protection in circumstances in which the target of the investigation is never brought to trial.[58] In that circumstance, an aggrieved individual has resort only to a civil lawsuit, but the doctrine of qualified immunity provides law enforcement with a robust defense in all but the most egregious cases featuring known breaches of whatever protections the Fourth Amendment does provide.[59] And even when a plaintiff does

391–92 (discussing police surveys revealing that exclusion "is an ephemeral punishment" at best); Randy E. Barnett, *Resolving the Dilemma of the Exclusionary Rule: An Application of Restitutive Principles of Justice*, 32 Emory L J 937, 953, 974 (1983) (observing that "[o]fficers who testify in suppression hearings may not be present in court when the judge gives his ruling and even if they are informed of the outcome, they may not be told of the judge's rationale" and that, because "there is no formal mechanism by which a police department learns of the suppression of evidence because of the misconduct of its officers[,] . . . it becomes extremely difficult, if not impossible, to discipline those officers whose actions most frequently result in the suppression of evidence"); Oaks, 37 U Chi L Rev at 667 (presenting empirical evidence that offers "little support for the proposition that the exclusionary rule discourages illegal searches and seizures, but [that] falls short of establishing that it does not"); id at 706–09 (offering evidence that suggests the exclusionary rule is ineffective).

57 See *Davis v United States*, 564 US 229, 238–39 (2011) (discussing the application of the "good-faith" exception to the exclusionary rule). See also Slobogin, 1999 U Ill L Rev at 375–76 & n 39 (cited in note 56) (describing "today's swiss cheese exclusionary rule").

58 See Slobogin, 1999 U Ill L Rev at 374–75 (cited in note 56) (citations omitted):

> In a large number of cases involving questionable stops and searches, the police do not make an arrest, either because they never intended to do so or because they find nothing, so the exclusionary rule never has a chance to come into play. Even when an arrest occurs, the search issue frequently is not litigated because the police don't pursue the case, or because the case is resolved through a plea or in some other fashion that avoids or undermines a hearing on the Fourth Amendment issue. The number of cases in the latter category is enormous; plea bargains dispose of ninety to ninety-five percent of all criminal actions.

59 See *White v Pauly*, 137 S Ct 548, 551 (2017) ("[Qualified] immunity protects 'all but the plainly incompetent or those who knowingly violate the law.'"), quoting *Mullenix v Luna*, 136 S Ct 305, 308 (2015). See also *Kisela v Hughes*, 138 S Ct 1148, 1162 (2018) (Sotomayor dissenting) ("[The Court's] one-sided approach to qualified immunity transforms the doctrine into an absolute shield for law enforcement officers, gutting the deterrent effect of the Fourth Amendment."); Stephen R. Reinhardt, *The Demise of Habeas Corpus and the Rise of Qualified Immunity: The Court's Ever Increasing Limitations on the Development and Enforcement of Constitutional Rights and Some Particularly Unfortunate Consequences*, 113 Mich L Rev 1219, 1245 (2015) (observing that the Supreme Court's qualified immunity decisions have "created such powerful shields for law enforcement that people whose rights are violated, even in egregious ways, often lack any means of enforcing those rights"). Convicted individuals seeking civil damages face another hurdle: the *Heck v Humphrey* bar further insulates investigators from liability by prohibiting convicted individuals from filing civil suits complaining of, among other

manage to subject law enforcement to liability, the evidence suggests that the prospective disciplinary effect of that liability on law enforcement behavior tends to be scant and unreliable.[60]

For all of these reasons, it is "difficult for robust Fourth Amendment protections to apply online."[61] Though the Fourth Amendment's warrant requirement is popularly understood to be the *ne plus ultra* of privacy protection, the rules surrounding searches and subpoenas—and the remedies available for their violation—make it a weak check on government intrusion, particularly in the context of electronically transmitted and ISP-stored data.[62] And while that ought to distress privacy advocates first and foremost, even those sympathetic to the government's interests might concede that the existing doctrine is, as Justice Sotomayor observed, poorly tailored to the current era.[63]

### B. The All Writs Act

Existing statutory frameworks are likewise becoming flawed or even obsolete as a result of the march of time and technology. For some of those statutes, such obsolescence can hardly be called a surprise. One of the major statutes at play in this arena is the AWA, initially enacted as part of the Judiciary Act of 1789 and barely amended since then. Despite predating the advent of the telephone by nearly a century, to say nothing of the internet, the AWA has played a major role in the government's attempts to secure judicial orders commanding technology companies to unlock devices like the iPhone seized in the course of investigating the San Bernardino shooting.[64] The

---

things, unlawful searches that would "necessarily imply the invalidity of [their] conviction or sentence." *Heck v Humphrey*, 512 US 477, 487 (1994).

60 See Joanna C. Schwartz, *Myths and Mechanics of Deterrence: The Role of Lawsuits in Law Enforcement Decisionmaking*, 57 UCLA L Rev 1023, 1067 (2010) ("[M]any law enforcement agencies do not gather information about past lawsuits. And without information about past suits, law enforcement can hardly make the types of informed decisions presupposed by judicial and scholarly theories of deterrence.").

61 Kerr, 72 Geo Wash L Rev at 1212 (cited in note 41). See also *Carpenter*, 138 S Ct at 2262 (Gorsuch dissenting) (asking, in light of the third-party doctrine and the fact that "we use the Internet to do most everything," "What's left of the Fourth Amendment?").

62 See Friedman, *Unwarranted* at 120, 122 (cited in note 11) ("[T]he Supreme Court has taken a cavalier, if not outright dismissive, attitude toward [the warrant requirement]," riddling it with "exception after exception.").

63 See *Jones*, 565 US at 417–18 (Sotomayor concurring).

64 See *All Writs Act Orders for Assistance from Tech Companies* (American Civil Liberties Union, 2016), archived at http://perma.cc/C633-8KLU (collecting cases).

AWA could even be called on to coerce ISPs with regard to other information stored by or produced by customers.

The AWA provides that federal courts have the power to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[65] This might include, for example, orders compelling third parties like ISPs to produce certain information relevant to an ongoing investigation or outstanding court order. Indeed, to hear the government tell it, the AWA is a "venerable" and "vital part of our legal system," compared to which "few laws are more vital."[66] But the AWA has also been described by the Supreme Court as "a *residual* source of authority,"[67] and by some judges as a "gap filler" statute—a "source of interstitial authority" that merely relieves Congress of the obligation to anticipate and provide every possible writ or tool that a federal court might need in service of the proper exercise of its jurisdiction.[68]

However one thinks of the AWA, it cannot plausibly be held out as a skeleton key for every possible need and every possible aim. So while the AWA has doubtless been applied "flexibly" in view of its aims,[69] the words of the statute must mean *something*.[70] This implies that there is some limit on what is "necessary or appropriate in aid" of a court's jurisdiction and what is "agreeable to the usages and principles of law."[71] Indeed, an expansive reading of these provisions might run afoul of the canon that Congress does not "hide elephants in mouseholes,"[72]

---

65 28 USC § 1651(a).

66 Government's Reply in Support of Motion to Compel and Opposition to Apple Inc's Motion to Vacate Order, *In re Search of an Apple iPhone*, No 16-10, *3 (CD Cal filed Mar 10, 2016).

67 *Pennsylvania Bureau of Correction v United States Marshals Service*, 474 US 34, 43 (1985) (emphasis added).

68 *In re Order Requiring Apple, Inc to Assist in the Execution of a Search Warrant Issued by This Court*, 149 F Supp 3d 341, 353 (EDNY 2016). See also *Michael v Immigration and Naturalization Service*, 48 F3d 657, 669 (2d Cir 1995) ("[T]he scope of the all writs provision confine[s] it to filling the interstices of federal judicial power when these gaps threaten[ ] to thwart the otherwise proper exercise of federal courts' jurisdiction."), quoting *Pennsylvania Bureau of Correction*, 474 US at 41. See also Morrison, 38 Cardozo L Rev at 2046 (cited in note 2) (describing the AWA as "[d]esigned to fill in the gaps of federal judicial power").

69 *United States v New York Telephone Co*, 434 US 159, 173 (1977).

70 See *Duncan v Walker*, 533 US 167, 174 (2001) ("It is our duty to give effect, if possible, to every clause and word of a statute."), quoting *United States v Menasche*, 348 US 528, 538–39 (1955) (quotation marks omitted).

71 28 USC § 1651(a).

72 *Whitman v American Trucking Associations, Inc*, 531 US 457, 468 (2001).

threaten the separation of powers,[73] or intend consequences that may well be absurd.[74]

But even if one could avoid those problems, the lack of clarity in the doctrine surrounding the AWA makes it so unreliable that even the government (to say nothing of the rest of us) ought to prefer something better tailored.[75] When deciding whether to issue an order under the AWA, courts are to consider how "far removed" the subject of the order is "from the underlying controversy," how "unreasonable [a] burden[ ]" the order would place on the subject, and how "necessary" the subject's assistance is to addressing the underlying controversy.[76] These are fuzzy concepts; indeed, by their terms, they aren't even binary questions ("Is assistance necessary?") but rather questions of degree ("How necessary is assistance?") that then must be balanced in some indeterminate fashion that risks ad hoc judgment calls and arbitrary distinctions.

To be sure, the AWA might be made to work in a nonabsurd, relatively predictable fashion that does not threaten the separation of powers. The point is simply that doing so is difficult and would mean MacGyvering the statute in ways that lack clear limiting principles. At best, then, the AWA is an inferior way of governing law enforcement's valid interests in an increasingly complex technological world.

### C. The Stored Communications Act

The difficulties plaguing the application of the AWA are mirrored even in much more contemporary efforts to address the problem of investigation in the digital age. The SCA, enacted as part of the Electronic Communications Privacy Act of 1986,[77] set

---

73 See *In re Order Requiring Apple, Inc to Assist*, 149 F Supp 3d at 361. See also *Plum Creek Lumber Co v Hutton*, 608 F2d 1283, 1290 (9th Cir 1979) (warning that adopting such an interpretation "would be to usurp the legislative function and to improperly extend the limited federal court jurisdiction").

74 See *In re Order Requiring Apple, Inc to Assist*, 149 F Supp 3d at 367 n 33 (considering whether the AWA permits a court to compel a drug company to produce the drugs necessary for a court-ordered execution). The government had no answer to this hypothetical when it was raised at oral argument. Id at 372–73.

75 See *United States v Hardage*, 58 F3d 569, 574 (10th Cir 1995) ("Unfortunately, there is an extreme dearth of case law interpreting the substantive parameters of the All Writs Act."); Morrison, 38 Cardozo L Rev at 2057 (cited in note 2) ("The best that can be said is that AWA jurisprudence does not appear to be the model of consistency.").

76 *New York Telephone Co*, 434 US at 172–75.

77 Pub L No 99-508, 100 Stat 1848 (1986), codified as amended in various sections of Title 18.

out the primary statutory framework by which ISPs can be compelled to disclose to the government communications and transactional records in their custody. The statute is notably "dense and confusing,"[78] but a short overview will suffice for present purposes.

The SCA regulates the government's ability to access both content data, which is the actual content of emails held by ISPs, and noncontent data, which is essentially all the rest of the data that ISPs hold. As for content data, the SCA draws distinctions based on whether the email has been opened and based on its age. For unopened emails in electronic storage on the server of an ISP for fewer than 180 days, the government needs a search warrant supported by probable cause in order to compel the ISP to turn over the email.[79] But for unopened email in such storage for *more* than 180 days and for opened email, the government needs only an administrative or grand jury subpoena or a judicial order based on "reasonable grounds to believe" that the contents of the email "are relevant and material to an ongoing criminal investigation."[80] Subpoenas of this type must be accompanied by notice to the user,[81] unless a "supervisory official" certifies that "there is reason to believe" that such notice will have an "adverse result."[82] Adverse results include the endangerment of life or physical safety, flight from prosecution, destruction of or tampering with evidence, intimidation of potential witnesses, or anything that would "otherwise seriously jeopardiz[e] an investigation or unduly delay[ ] a trial."[83] Judicial orders of the type just outlined also must be accompanied by notice unless the issuing court concludes there is "reason to believe" that such notice will have one of these "adverse result[s]."[84] When these circumstances exist, notice may be delayed for a period "not to exceed ninety days," and the government is

78 Kerr, 72 Geo Wash L Rev at 1208 (cited in note 41).

79 18 USC § 2703(a).

80 18 USC § 2703(d). See also 18 USC § 2703(b)(1)(B) (authorizing such orders or subpoenas for emails in storage for longer than 180 days); Kerr, 72 Geo Wash L Rev at 1216, 1223 (cited in note 41) (discussing the different treatment of opened and unopened emails).

81 18 USC § 2703(b)(1)(B).

82 18 USC § 2705(a)(1)(B).

83 18 USC § 2705(a)(2).

84 18 USC § 2705(a)(1)(A).

entitled to further extensions "of up to ninety days each" upon further certification or order.[85]

The bottom line is that, to access the content of unopened email that is six months old or younger, the government needs a warrant. But to access the content of older unopened email *or opened email*, the SCA says the government can get away with as little as an administrative subpoena.[86] And while notice to the user is technically required, the government can simply certify and recertify that such notice might have adverse results and thereby delay that notice indefinitely. If the Fourth Amendment protects the content of emails regardless of their age,[87] this aspect of the SCA addressing content data is arguably unconstitutional, as the government may have recently conceded.[88] If not, the stuff with which the SCA fills the gap—a subpoena without notice—is exceptionally weak.[89]

A large part of why it is so weak is that the SCA "freez[es] into the law the understandings of computer network use" at the time it was enacted in 1986, and it divides the computing world into providers of "electronic communication service" (ECS) and providers of "remote computing service" (RCS).[90] Simplifying greatly, ECS is basically short-term communication and "temporary, intermediate storage . . . incidental to" the transmitted communication, whereas RCS is long-term storage.[91] Nowadays, ISPs usually offer users both ECS and RCS without any practical distinction[92]—certainly not one that users contemplate—but the SCA prescribes different rules for the two types of services. The result is that the statute considers new, unopened email to be part of ECS (with its warrant

---

85 18 USC § 2705(a)(1)(A), (a)(1)(B), (a)(4). At the end of the delay period, however extended, the government must serve the user with a notice that states the nature of the law enforcement inquiry and informs the user that her information was supplied to an identified government authority on an identified date. 18 USC § 2705(a)(5).

86 See Friedman, *Unwarranted* at 246 (cited in note 11) (calling it a "strange loophole").

87 See note 41.

88 See Transcript of Oral Argument, *Carpenter v United States*, No 16-402, *45 (US filed Nov 29, 2017).

89 See Kerr, 72 Geo Wash L Rev at 1234 (cited in note 41) (observing that "the government can often compel all opened e-mails from an ISP with a mere subpoena and without meaningful notice"); id at 1220 n 80 (noting that § 2703(b) might be unconstitutional).

90 Id at 1214. See also Friedman, *Unwarranted* at 246 (cited in note 11).

91 18 USC § 2510(17)(A) (ECS); 18 USC § 2510(17)(B) (RCS). See also Kerr, 72 Geo Wash L Rev at 1214–16 (cited in note 41) (explaining the distinction in greater detail).

92 See Kerr, 72 Geo Wash L Rev at 1215 (cited in note 41).

requirement), but it considers opened email or older unopened email to be part of RCS (with its substantially weaker privacy protections).[93]

In addition to governing the handling of the kind of content data discussed so far, the SCA also covers noncontent data—essentially everything besides the content of communications.[94] The statute divides noncontent data into two groups. Information like a user's name, address, telephone number, or network address; the length of the user's service contract with the provider; the user's payment information; and the user's connection records and "records of session times and durations" fall into one group.[95] The SCA provides that the government can access such information with merely an administrative or grand jury subpoena and without any obligation to provide notice to the user.[96] All other noncontent data—addresses emailed, sites visited, etc.[97]—whether considered ECS or RCS, falls into another group. To access that kind of information, the government needs either a warrant supported by probable cause *or* the kind of court order supported by "reasonable grounds to believe" that the data "are relevant and material to an ongoing criminal investigation" discussed above in the context of content data.[98] (The government still need not provide notice to the user.[99]) Note that, for this latter group of noncontent data, while a grand jury or administrative subpoena will not suffice, a court order issued at a standard that "falls well short" of probable cause still will.[100]

As even this short summary ought to demonstrate, the SCA is a thoroughly complex statute that is rooted in an outdated conception of the relevant technology, that provides "surprisingly weak" protection for a wide swath of content in-

---

93 See id at 1216.

94 It is important not to underestimate the meaningfulness of noncontent data. Particularly when compiled, it can be "just as revealing of our lives as content information." Friedman, *Unwarranted* at 254 (cited in note 11).

95 18 USC § 2703(c). See Kerr, 72 Geo Wash L Rev at 1219 (cited in note 41) (explaining that Congress deemed this enumerated list "less private than other records").

96 18 USC § 2703(c)(2), (3).

97 See Kerr, 72 Geo Wash L Rev at 1228 (cited in note 41) (explaining what noncontent data includes).

98 18 USC § 2703(d). See also 18 USC § 2703(c)(1)(A), (B). The government can also compel the disclosure of noncontent records with the consent of the user. 18 USC § 2703(c)(1)(C).

99 18 USC § 2703(c)(3).

100 *Carpenter*, 138 S Ct at 2210.

formation,[101] and that strikes a puzzling balance in the protection it offers to noncontent information. Perhaps even more than the AWA, it is being asked to do a job that it was not designed to do in a context it was not designed to fit.[102]

### D. Recent Proposals

Recognizing some of these anachronisms and inadequacies, legislators and scholars have set to work crafting possible replacements or additions to the government's toolkit. The one that has come closest to becoming law is the EPA. This bill, which has been thrice passed in the House and thrice left on the cutting room floor in the Senate, would leave the rules for noncontent data unchanged but would require a warrant supported by probable cause for *all* content data—whether ECS or RCS, and regardless of its age or opened/unopened status.[103] This reform would simplify the SCA while also substantially raising the level of protection afforded to content data: administrative subpoenas and "reason to believe" court orders would no longer suffice.[104] At the same time, however, the EPA would double the notice delay period from 90 to 180 days, again subject to "one or more extensions," without amending the standard under which such delays would be authorized.[105]

The EPA's across-the-board warrant requirement for content information is certainly a boon to privacy advocates, who could perhaps live with the fact that it comes with an expanded notice delay period. After all, the warrant requirement means that the underlying search will have undergone a more rigorous review in the first instance. But the protection of much sensitive noncontent data would remain relatively low. Moreover, the EPA might well overcorrect the SCA's privacy flaws.[106] For ex-

---

101 Kerr, 72 Geo Wash L Rev at 1233 (cited in note 41).

102 See id at 1214 ("The SCA is not a catch-all statute designed to protect the privacy of stored Internet communications; instead it is narrowly tailored to provide a set of Fourth Amendment-like protections for computer networks.").

103 See, for example, Email Privacy Act § 3, HR 699, 114th Cong, 2d Sess, in 162 Cong Rec H 2022 (daily ed Apr 27, 2016). See also notes 8–9 (discussing the fate of these bills).

104 18 USC § 2703(b)(1)(B), (d).

105 Compare HR 699 § 2705(c) (cited in note 8), with 18 USC § 2705(a).

106 See Christopher Slobogin, *Policing, Databases, and Surveillance: Five Regulatory Categories* *4, 8 (Vanderbilt Law Research Paper No 17-23, Apr 2017), archived at http://perma.cc/WZ49-PB78 (noting that a broad warrant requirement "has problems of its own": it "overprotects the interests at stake" by sweeping up "a large number of

ample, not all agencies that conduct investigations—and from whose investigations society benefits—have the power to seek and execute warrants. As Mary Jo White, then the chair of the Securities and Exchange Commission (SEC), explained, the fact that civil law enforcement agencies like the SEC (as well as the Federal Trade Commission and the Commodity Futures Trading Commission) cannot obtain warrants means that the EPA would prevent those agencies "from getting *any* electronic communications from Internet service providers, regardless of the circumstances."[107] The EPA would thus hamstring civil investigations into Ponzi schemes and insider trading by creating an "unprecedented digital shelter . . . that does not exist for paper materials . . . [and] that would enable wrongdoers to conceal evidence."[108] It is perhaps for reasons like these that the Senate has consistently declined to consider the bill.[109] Or, perhaps, there is simply insufficient support in the Senate for such an increase in privacy protection.[110]

Other reforms might entail more modest adjustments. For example, rather than require a warrant, a new statute could address concerns like White's by requiring that the government get some other court order for the data it seeks, governed by a sub–warrant standard like "reasonable grounds to believe."[111] A new amendment might also reduce the period for which notice can be delayed.[112] These might be reasonable "middle ground" improvements,[113] and perhaps they might attract political support in ways that the EPA has not.

Indeed, tweaking timelines and modulating burdens of proof might well be the best our politics can handle, and the search for the perfect ought not be the enemy of the good. But we can do better. Just like the EPA, and like the SCA before it, these adjustments are either/or, on/off solutions. They risk being reactive

---

situations" that "do not merit the full protection of a judicial probable-cause finding," and it "handcuff[s] legitimate government efforts to nab terrorists and criminals").

107 Mary Jo White, *Privacy Rules Shouldn't Handcuff the S.E.C.* (NY Times, May 12, 2016), online at http://www.nytimes.com/2016/05/13/opinion/privacy-rules-shouldnt-handcuff-the-sec.html (visited Oct 22, 2018) (Perma archive unavailable).

108 Id.

109 See note 9 and accompanying text.

110 See note 10 and accompanying text.

111 18 USC § 2703(d) (indicating the standard for court-ordered disclosure of electronic information). See also Kerr, 72 Geo Wash L Rev at 1234–35 (cited in note 41) (making such a suggestion).

112 See Kerr, 72 Geo Wash L Rev at 1235 (cited in note 41).

113 Id at 1234.

to the latest headlines, they are not a recipe for precise calibration of public investigatory need and private interests in privacy, and they avoid deeper questions about how investigations should be governed in the digital age.[114] And the hazier the test that will apply when the protection is "on," the more confusion and unpredictability will plague the courts, investigating entities, and American citizens. The bottom line is that there is only so much that can be done by coloring inside the old lines and offering variations on the SCA's themes.[115]

The balance of this Article colors outside those lines and offers a different replacement inspired by an underappreciated source: the government's takings power. Part II sets out what the approach might look like and defends the analogy. Part III grapples with its normative implications.

## II. TAKING DATA

As the foregoing discussion illustrates, resolution of the tension between privacy and law enforcement in the digital arena has proven elusive. Even the legislative solutions that have emerged are not durable enough to adapt to new technology and new needs. Part of the reason why answers seem so hard to find is no doubt that the question being asked is nearly impossible to answer in general terms. We want the police to have the right incentives to investigate when and where they should be investigating so as to protect the public, and we want them to respect our privacy by not investigating when the intrusion is too great relative to the benefits the investigation would generate.[116] But because it is hard to make this call at the level of wholesale legislation, traditional tools and rules of criminal procedure that speak either in bright-line rules or in hazy tests will consistently fail to resolve this tension.

Property law, by contrast, offers a tool that is designed to strike precisely the kind of retail-level balance between public benefits and private burdens that we are looking for: the power

---

[114] See notes 11–14 and accompanying text.

[115] See Berman, 102 Minn L Rev at 632–33 (cited in note 13) (noting the inadequacy of the current legislative frameworks, which lack any "overarching, unified information protection regime").

[116] See Friedman, *Unwarranted* at 237 (cited in note 11) ("That's the tension: protect the information, and law enforcement says it can't go after some bad guys; weaken protections, and we all can say adios to any shard of security from government prying.").

of eminent domain.[117] And it is a tool that can potentially do the same in the investigatory sphere. Indeed, the Takings Clause has a number of features that can be readily adapted to govern the investigation of ISP-held data. Moreover, the analogy would be both doctrinally and theoretically sound, doing little violence to the law of takings, theories of property, or the law of criminal procedure.

### A. A Data Takings Act

To see how this might work, consider the terms and operation of the Takings Clause. It provides that government may not use its power of eminent domain to "take[ ]" private property, except if it does so "for public use" and renders "just compensation" to the former property owner.[118] While this provision is phrased by way of restriction, it necessarily implies the power of the government to act when the conditions are satisfied. In other words, the government *may* exercise its power of eminent domain to take private property so long as it does so for public use and with just compensation—that is, by paying fair market value, measured at the time of the taking, to the

---

[117] Another way of framing this turn is by understanding the existing regime—in which information is, say, either subject to a warrant requirement or not—as either protecting a privacy entitlement with a property rule (absent a warrant, law enforcement can gain access only in a voluntary transaction with the target) or providing no privacy entitlement at all. See Guido Calabresi and A. Douglas Melamed, *Property Rules, Liability Rules, and Inalienability: One View of the Cathedral*, 85 Harv L Rev 1089, 1105 (1972). Proposals such as the EPA can be characterized similarly. See text accompanying notes 103–10. This is problematic for the same reason that property-rule protection often risks being problematic: negotiated bargains or even breaches of the protection that would be socially desirable may not occur because of holdout problems and other high transaction costs. See Calabresi and Melamed, 85 Harv L Rev at 1118–19. In this context, these risks are quite likely to emerge: targets who have broken the law obviously face very high stakes and will resist voluntary disclosure at any cost, but even innocent people who simply wish to keep their information confidential from law enforcement may not be so inclined to provide access to it upon request even if that disclosure would be beneficial for society. A takings-based regime, by contrast, would protect privacy with a liability rule: privacy would be protected against government intrusion *unless* the government paid compensation at a collectively determined value to the person whose privacy was intruded upon. See id at 1092. (Indeed, eminent domain is a classic example of liability rule protection. Id at 1108.) This solves the problem created by property-rule protection by permitting efficient breaches of the entitlement while removing from the entitlement holder the power to hold out. The primary objection to liability rules is that they are often too difficult to administer when the costs of assessing value are high. See id at 1119, 1125. But as discussed at greater length in Part III.B, that objection can be adequately met here. I am grateful to Lior Strahilevitz and Maureen Brady for noting this lens.

[118] US Const Amend V.

now former owner of the property in question.[119] And while real property is perhaps the most common subject of eminent domain, the power sweeps wider.[120] Personal property, and even intangible property, may be taken by eminent domain.[121]

Note that the "public use" requirement does not embrace only those takings in which the public will actually be permitted to *use* or have access to the property in question. Rather, the question is whether the taking has a "public purpose."[122] The Supreme Court has held that alleviating blight,[123] reducing the concentration of land ownership,[124] and promoting economic development[125] are all public purposes that can justify taking private property. This pattern reflects a judgment on the part of the Court that it ought to "eschew[ ] rigid formulas and intrusive scrutiny" and instead "afford[ ] legislatures broad latitude in determining what public needs justify the use of the takings power."[126] In fact, a taking may be justified as being for a public use even if the government hands the property over to another private party that will make what the government believes to be a better use of it.[127] All that matters is "the taking's purpose, and not its mechanics," and courts will not lightly unsettle a legislature's identification of a public purpose.[128]

---

119 See *Horne*, 135 S Ct at 2432, quoting *United States v 50 Acres of Land*, 469 US 24, 29 (1984). See also *Palazzolo v Rhode Island*, 533 US 606, 625 (2001); *United States v Miller*, 317 US 369, 373–74 (1943).

120 See *City of Oakland v Oakland Raiders*, 646 P2d 835, 838 (Cal 1982) ("No constitutional restriction, federal or state, purports to limit the nature of the property that may be taken by eminent domain."); Roberta Rosenthal Kwall, *Governmental Use of Copyrighted Property: The Sovereign's Prerogative*, 67 Tex L Rev 685, 694 (1989) ("[A]ny type of property, tangible or intangible, is subject to the exercise of eminent domain.").

121 See *Horne*, 135 S Ct at 2425–28 (holding that personal property is subject to the Takings Clause); *Monsanto*, 467 US at 1003–04 (holding that trade secrets are protected by the Takings Clause); *Kimball Laundry Co v United States*, 338 US 1, 16 (1949) (holding that the government owed just compensation under the Fifth Amendment for having taken a laundry company's trade routes); *James v Campbell*, 104 US 356, 357–58 (1881) (holding that patents are protected by the Takings Clause); *West River Bridge Co v Dix*, 47 US (6 How) 507, 534 (1848) (explaining that the distinction for purposes of the Takings Clause between "property which is corporeal" and property which is not, like a franchise, "has no foundation in reason").

122 *Kelo v City of New London*, 545 US 469, 479–80 (2005) (collecting cases).

123 *Berman v Parker*, 348 US 26, 33–35 (1954).

124 *Hawaii Housing Authority v Midkiff*, 467 US 229, 241–42 (1984).

125 *Kelo*, 545 US at 483–84.

126 Id at 483.

127 See *Midkiff*, 467 US at 243–44 ("The mere fact that property taken outright by eminent domain is transferred in the first instance to private beneficiaries does not condemn that taking as having only a private purpose."). See also *Kelo*, 545 US at 485–87.

128 *Midkiff*, 467 US at 244.

Finally, as a matter of statute, the federal government must comply with the process set out in the Declaration of Taking Act.[129] Specifically, a governmental entity seeking to take property on behalf of the United States must first file a declaration in the district court in which the property is located containing a statement of the authority under which the taking is being made, the public use for which the property is to be taken, a description of the property sufficient to identify it, the interests in the property that are being acquired, a plan showing the land taken, and an estimate of just compensation.[130] Upon the filing of this declaration and, crucially, the depositing of a bond in the amount of the estimated compensation, title to the property vests in the government and the right to just compensation vests in the former owners.[131] Litigation may then proceed if necessary regarding the actual amount of compensation and the lawfulness of the taking itself.[132]

A Data Takings Act (DTA) would take a similar form. It is not my aim here to offer a definitive legislative proposal with nonnegotiable operational details but rather to provide enough of a starting point to enable discussion about the normative and practical implications. After all, those implications might point the way toward further desirable features or suggest necessary safeguards. Moreover, while this proposal is aimed at the federal level—in the interest of promoting uniformity and because the relevant existing statutes and notable disputes are federal and involve federal law enforcement actors—it could also function in principle as a model for states and localities to enact with respect to their own investigating entities, though there may be additional complexities at the state and local levels.[133]

As a first step, the DTA would provide that, in order to access ISP-held data like sites visited and persons emailed for

---

129 46 Stat 1421 (1931), codified as amended in various sections of Title 40.

130 40 USC § 3114(a).

131 40 USC § 3114(b). See, for example, *United States v Sid-Mars Restaurant & Lounge, Inc*, 644 F3d 270, 272 (5th Cir 2011); *United States v 21.54 Acres of Land, More or Less, in Marshall County*, 491 F2d 301, 304 (4th Cir 1973).

132 See FRCP 71.1 (providing rules to govern takings proceedings for "real and personal property"); *Anatomy of a Condemnation Case* (US Department of Justice, May 15, 2015), archived at http://perma.cc/K7J6-AJ5E.

133 One meaningful source of complexity is that states and localities may react differently to budgetary pressures than agencies of the federal government, may be more constrained by such pressures, and indeed may perceive different pressures altogether.

some or all law enforcement purposes,[134] the government would be obligated to employ a takings-based process (rather than any other investigative tool) to acquire that data. Just as with the ordinary takings process, the DTA would require a law enforcement agency seeking to acquire ISP-held data for investigatory purposes to file a declaration in district court and to pay a bond for the estimated compensation.[135]

Some additional details would be necessary, however. First, the DTA would allocate to the holder of an email account or to the creator of ISP-held data—the person whose privacy is implicated—a quasi-property right in that data reflecting the private nature of the information in question.[136] This would be a limited right only for the purposes of enabling this takings-based regime to function and directing the payment of compensation.[137] It

---

[134] Because this Article is meant to prompt a discussion about the possibilities of a law of this type, a precise definition of the set of investigations covered by the DTA is not strictly necessary. For example, Congress could narrow the idea and limit it to only, say, terrorism investigations. If it does that, it might opt to call the statute the Data Anti-Terrorism Acquisition Act or Deter Acts of Terrorism by Acquisition Act, which, while somewhat clumsy, reduce to an attractive acronym: DATA Act. See Mary Whisner, *What's in a Statute Name?*, 97 L Library J 169, 179–82 (2005) (cataloging Congress's penchant for employing clever acronyms in statute titles). Where appropriate in the balance of the Article, I point out the implications of certain scoping choices as well as the choices one might make in light of particular implementation concerns.

[135] See notes 130–32 and accompanying text.

[136] See note 150 and accompanying text (noting that the government can create property rights). This allocation to the user, rather than to the ISP for example, is designed to reflect the privacy interests at issue—interests that the ISP does not have. See *Carpenter*, 138 S Ct at 2272 (Gorsuch dissenting) (suggesting that it is "entirely possible a person's cell-site data could qualify as *his* papers or effects" because "customers have substantial legal interests in this information, including at least some right to include, exclude, and control its use"). In making this allocation, the statute would be operating on a relatively clean slate because determining, for example, who owns an email as a matter of existing law has proven difficult. Some of the most sustained attention to this question has arisen regarding what happens to emails and social media accounts upon the death of the account holder, but answers remain stubbornly elusive for now. See Orin Kerr, *Who Can Access Your E-mails after You Die?* (Wash Post, Oct 17, 2017), online at http://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/10/17/who-can-access-your-e-mails-after-you-die/?utm_term=.86b7ed7c9dfc (visited Oct 21, 2018) (Perma archive unavailable); Jonathan J. Darrow and Gerald R. Ferrera, *Who Owns a Decedent's E-mails: Inheritable Probate Assets or Property of the Network?*, 10 NYU J Legis & Pub Pol 281 (2007) (discussing the open question and the impact of ISP terms of service, and suggesting that email be thought of as a bailment). Indeed, the Supreme Court recently denied certiorari in a case implicating the question. See *Ajemian v Yahoo!, Inc*, 84 NE3d 766 (Mass 2017), cert denied, 138 S Ct 1327 (2018).

[137] One might object to a scheme in which suspected criminals are paid for their data. But even guilty people—to say nothing of merely possibly guilty people—value their privacy. When the government intrudes upon that privacy, those people experience a loss all the same as innocent people. Compensating them for that intrusion is therefore

would not, for reasons I discuss below, create a right to sell this private data to any willing buyer; rather, it would give structure to the process by which one and only one buyer—namely, the government—could purchase that data at its own election.[138] Accordingly, when the government acquires the data, it would not acquire anything that had ever been further alienable to others, and that limitation would run with the data.[139] The government would therefore not be able to resell the data it took. The statute could even expressly prohibit the government from doing so to make this doubly clear.

Second, the DTA would give authority to make an investigatory taking of this information to both criminal investigatory entities (like the FBI) and civil investigatory entities (like the SEC, to address Mary Jo White's concerns[140]), and it would require such entities to use that authority and associated process rather than traditional tools like warrants or subpoenas. The entity would have to identify in its declaration precisely the property it seeks to take and establish the safety- or welfare-protecting public use that the taking would serve. A declaration devoid of any reason why acquiring the data in question would advance these goals by furthering an investigation would be inadequate.[141] The agency would also have to include in its declaration an estimate of the compensation owed and pay a bond in that amount. Finally, for reasons I discuss in more detail below, the DTA would require

---

not equivalent to "rewarding" them for their (suspected) criminal activity, at least not any more than is affording them due process or any of the other rights and privileges extended to the accused. But if one were concerned nonetheless, one solution might be to put the compensation in escrow and use it to pay for the defense to which the accused is constitutionally entitled.

138 See notes 155–88 and accompanying text (discussing arguments against marketable rights in data and the contours of restrictions on alienability).

139 See notes 155–88. The resulting limitation on the government's ability to resell follows from the rule of *nemo dat quod non habet*, which means that one may not give what one does not have; in other words, one cannot sell any better title than he owns. *Mitchell v Hawley*, 83 US 544, 550 (1872).

140 See note 107 and accompanying text.

141 A suspicionless investigative taking would likely not pass muster under the "public use" requirement, but the DTA could make that clear as a matter of statutory text. See notes 122–28 and accompanying text; notes 189–93 and accompanying text (exploring the application of the "public use" requirement to the context of data takings).

that a politically appointed official within the agency sign off on the taking.[142]

Third, to address some of the unique concerns applicable to this context, which Part III further explains, the DTA would also mandate that the funding for the required compensation payments come from the investigating entity's own budget.[143] As a failsafe, the DTA could also incorporate considerations for exigent circumstances[144] and could provide that an agency that runs out of money, but believes it still needs particular ISP-held data, can seek a court order excusing it from the terms of the statute and issuing it a traditional warrant upon a showing of both probable cause and exceptional need. Further, while takings compensation is generally set at the fair market value of the property taken measured at the time of the taking,[145] and while this Article discusses below how that measure would translate to the realm of the DTA, the statute could even clarify how this valuation would be made.[146] Finally, the DTA could retain the SCA's delayed notification regime,[147] but it would also require each agency to publicly issue a quarterly report to Congress indicating the number of takings made, the price of each, and whether and how the applicable investigation was materially advanced by the data that was purchased.[148]

While the fact that the DTA I sketch out does not contain a warrant requirement and instead builds an entirely distinct investigatory framework might seem problematic, that is precisely what the SCA already does. It is also what the EPA would continue to do for noncontent information. But instead of drawing the kinds of blunt, arbitrary, and potentially complex lines that

---

142 See notes 218–60 (discussing ways in which accountability and other political dynamics would join with the requirement that compensation be paid to generate behavioral changes on the part of investigators).

143 See notes 231–32 and accompanying text (discussing the import of this requirement).

144 See *King*, 563 US at 460 (discussing the exigent circumstances exceptions to the warrant requirement and their justifications).

145 See note 119 and accompanying text (noting the fair-market-value standard). The fact that value is assessed at the time of the taking would prevent gamesmanship in which the government retroactively adjusts its valuation once it sees the data it acquires.

146 See Part III.B (discussing the valuation aspect of implementing the DTA).

147 See 18 USC § 2705(a). The payment of compensation would not jeopardize secrecy (in the event the court authorized a disclosure delay) because the government's bond could simply be paid in escrow to the court.

148 See notes 233–39 and accompanying text (revealing the import of this reporting requirement).

these existing statutes and proposals do—lines that are destined to become obsolete as technology advances—the DTA would draw inspiration from the government's takings power and offer a more neutral and resilient mechanism designed to achieve retail-level balancing of private burdens and public benefits. And rather than just add it to the mix of options for the government, the DTA would demand that this particular tool be used in the relevant set of investigations and would set up a structure within which it would be used. By channeling the government in this way, the DTA could bring coherence, predictability, and balance to an area of law and policy that sorely needs it.

### B. The Property Analogy

Before exploring those benefits in earnest, and before engaging with related implementation questions, it is worth pausing to examine the theoretical and doctrinal bases on which this property analogy rests. After all, if the world of data investigations bears no similarity to the world of property and eminent domain, a regime for the former inspired by the latter—even if otherwise attractive—might make little sense. In fact, however, there are serious connections between the two.

The first possible pivot point has to do with whether private data and rights of access to such data could be conceived of as akin to the types of property subject to eminent domain. To be sure, the law does not presently recognize a property right in a particular piece of data,[149] but the government "clearly [has] power to create property rights," and creating a species of property right with respect to ISP-held data is conceptually sound.[150]

---

[149] See Pamela Samuelson, *Privacy as Intellectual Property?*, 52 Stan L Rev 1125, 1131 (2000) ("Indeed, the traditional view in American law has been that information as such cannot be owned by any person."). See also *Moore v Regents of the University of California*, 793 P2d 479, 493 (Cal 1990) (holding that a person does not have a property right in her genetic information).

[150] Samuelson, 52 Stan L Rev at 1134 (cited in note 149). See also Lawrence Lessig, *The Architecture of Privacy*, 1 Vand J Ent L & Prac 56, 63 (1999); Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 Georgetown L J 2381, 2383–84 (1996). At least one member of the current Supreme Court evidently agrees that electronic communications data can be conceived of as property. See *Carpenter*, 138 S Ct at 2270 (Gorsuch dissenting) (observing that "[s]tate (or sometimes federal) law often creates rights in both tangible and intangible things" and suggesting that treating "digital record[s]" as "property" may be sound); *United States v Ackerman*, 831 F3d 1292, 1307–08 (10th Cir 2016) (Gorsuch) (applying a property-based trespass theory of the Fourth Amendment to find that a search occurred when a government agent examined an email). And while there are disputes as to which

After all, at the heart of what property rights are meant to protect is the right to exclude others and to control access.[151] This same interest in exclusion and control is precisely why people value the private nature of their data in the first place: when people create data and store it in a place to which they can limit access, like a password-protected email account, they have memorialized a piece of private personal information over which they hope and expect to retain control.[152] In this way, one's interest in, say, her email address book is all at once one of privacy *and* one of exclusion, as the Supreme Court has recently recognized.[153] The two are deeply intertwined, and the latter is fundamentally a form of property interest. Conceiving of one's

---

governments can create property rights for which purposes, there is little reason why the power to create property rights for the purposes of a federal law, like this Article's proposal, cannot reside (even if nonexclusively) in the federal government. See Orin Kerr, *Can the Federal Government Define "Property" for Purposes of Federal Law?* (The Volokh Conspiracy, Mar 28, 2013), archived at http://perma.cc/G9JQ-TA7K. See also Part II.A (noting that this proposal may also be a model for states).

[151] See *Loretto v Teleprompter Manhattan CATV Corp*, 458 US 419, 435–36 (1982) (identifying these rights as constituting the "bundle" of property rights); *Kaiser Aetna v United States*, 444 US 164, 179–80 (1979) (describing the right to exclude as "so universally held to be a fundamental element of the property right"); *International News Service v The Associated Press*, 248 US 215, 250 (1918) (Brandeis dissenting) ("An essential element of individual property is the legal right to exclude others from enjoying it."); Lior Jacob Strahilevitz, *Information Asymmetries and the Rights to Exclude*, 104 Mich L Rev 1835, 1836 (2006) ("American courts and commentators have deemed the 'right to exclude' foremost among the property rights."); Thomas W. Merrill, *Property and the Right to Exclude*, 77 Neb L Rev 730, 752 (1998) (calling the right to exclude the "sine qua non" of property). I do not intend here to wade into the robust debate about "the centrality of the right to exclude to the definition of property." Jonathan Klick and Gideon Parchomovsky, *The Value of the Right to Exclude: An Empirical Assessment*, 165 U Pa L Rev 917, 935 (2017). Rather, it suffices for present purposes to note that even many of those who would not call the right to exclude the sole characteristic of property nonetheless recognize that it is among the important characteristics of property. See, for example, Gregory S. Alexander, *The Complex Core of Property*, 94 Cornell L Rev 1063, 1066 (2009) ("[A]lthough the right to exclude is part of the core of ownership, the core is more complex than exclusion alone."); Felix S. Cohen, *Dialogue on Private Property*, 9 Rutgers L Rev 357, 370–71 (1954) (arguing that, while property may involve other rights, it "must at least involve a right to exclude").

[152] See *Thyroff v Nationwide Mutual Insurance Co*, 864 NE2d 1272, 1278 (NY 2007) (holding that a claim for conversion of electronic data is cognizable because "it generally is not the physical nature of a document that determines its worth, it is the information memorialized in the document that has intrinsic value").

[153] See *Byrd v United States*, 138 S Ct 1518, 1527 (2018) (linking privacy and exclusion by noting that "'[o]ne of the main rights attaching to property is the right to exclude others,' and, in the main, 'one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of the right to exclude'"), quoting *Rakas v Illinois*, 439 US 128, 143 n 12 (1978); *Byrd*, 138 S Ct at 1528 (referring to "the expectation of privacy that comes from lawful possession and control *and the attendant right to exclude*") (emphasis added).

interest in that data as property-like thus reflects the very feature that makes the data valuable to its creator—its exclusive and private nature—as well as the primary threat to that data's value, namely its becoming nonprivate and nonexcludable.[154]

At the same time, however, many scholars have argued that personal data should not be considered a form of property.[155] Their primary concern is a consequentialist one: they fear that treating data like property will erode the privacy protection it is afforded. This is either because propertizing data will "encourage[ ] transactions in data that most of us would prefer be discouraged"[156] or because information asymmetries and collective action problems will lead people to sign away too much of their personal data.[157] But these critiques are raised in the context of contemplating a wide and open market for personal data.[158] And while at least something of a market in some personal data has already come to fruition,[159] expanding or endorsing such a market is neither this Article's aim nor a necessary consequence of recognizing *any* property interest in personal data.[160] Instead, this Article contemplates a sui generis regime governing law enforcement's access to ISP-held data for investigatory purposes, in which private data is conceived of as a form of property *within that regime*.

Of course, it is fair to ask whether these critiques apply all the same within a framework like this Article's, which is based

---

[154] See James Y. Stern, *Intellectual Property and the Myth of Nonrivalry* *61–62 (unpublished manuscript, 2018) (on file with author):

> [O]btaining access is clearly injury in itself, even if others' access is otherwise undiminished. It isn't hard to imagine that someone doesn't remember what they wrote in an email two years ago and wouldn't really care if the email were permanently erased but might very much care whether someone else gets to read the message.

[155] See, for example, Schwartz, 117 Harv L Rev at 2057 (cited in note 23) ("Legal scholars interested in protecting information privacy [ ] have been suspicious of treating personal data as a form of property.").

[156] Jessica Litman, *Information Privacy/Information Property*, 52 Stan L Rev 1283, 1303 (2000).

[157] See Mark A. Lemley, *Private Property*, 52 Stan L Rev 1545, 1551 (2000); Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan L Rev 1373, 1391–92 (2000); Samuelson, 52 Stan L Rev at 1145 (cited in note 149).

[158] See Cohen, 52 Stan L Rev at 1391 (cited in note 157) (equating "[p]roperty talk about data privacy" with "enabling . . . trade"). See also Schwartz, 117 Harv L Rev at 2076 (cited in note 23) (framing these objections as objections to "data trade").

[159] See note 264 and accompanying text.

[160] See Jesse Dukeminier, et al, *Property* 177 (Wolters Kluwer 9th ed 2017) (discussing severing the recognition of a property interest in a thing from the recognition of the interest-holder's ability to sell that thing in a market transaction).

on the Takings Clause, but the answer on that score is no. This is because, unlike a large-scale free market in data, takings are a decidedly nonmarket framework. By definition, these transactions are nonconsensual, monopsony-like transactions: there is only one buyer that can exercise the power (the government), and that buyer exercises its power without the agreement of the target owner. There is no mechanism by which a data owner can put her information up for sale, nor is there a mechanism by which an array of potential buyers can make offers. Embracing a takings analogy is therefore not likely to lead to a robust data trade—with the attendant concerns about privacy erosion that many have—because nothing about the exercise of eminent domain enables trade.

There is a related concern that propertizing data would make privacy dependent on socioeconomic status. The wealthy would be able to maintain privacy, the concern goes, because they could afford not to sell access to their private data, while those less well-off would find themselves coerced by circumstance (or education level, or predatory practices, etc.) to give up their privacy. As Professor Pamela Samuelson has put it, "If information privacy is a civil liberty, it may make no more sense to propertize personal data than to commodify voting rights."[161] Accepting the premise of the argument for the moment, this distributional concern carries substantially less weight than it might elsewhere in a nonmarket, takings-based context in which everyone is a priori equally coerced and, by definition, takings are nonconsensual, coercive transfers of property rights.[162] Moreover, the danger that some people will feel obligated by circumstance to volunteer their information to a buyer does not arise within a takings framework because the transfers occur only upon the request of the government. Finally, however, there is a deeper problem with the premise of this concern. The idea that propertizing data necessarily risks commodifying civil liberties elides an important distinction between a thing and an associated right or liberty. Things (like data) are distinct from rights (like voting rights or even privacy rights) even if commodifying the thing has consequences for the exercise of the associated right. For example, books, pamphlets, and other written texts are things, and the fact that those texts are commodities

---

[161] Samuelson, 52 Stan L Rev at 1143 (cited in note 149).

[162] In fact, this risk-spreading is one of the virtues of an eminent domain approach, particularly as applied to the law enforcement context. See note 233 and accompanying text.

has consequences for the ease with which people can exercise their rights to speak freely. But it is not the case that speech rights *themselves* are commodified because books are, nor can it seriously be suggested that we ought not commodify books lest we risk commodifying speech rights.[163] The same is true with respect to personal data. But even if one rejects this thing/rights distinction, the rights-commodification concern remains, as I note above, largely mitigated in the context at issue here.

Another leading objection to considering data as property is more theoretical. It begins by arguing that, even if it were practically possible to prevent the development of a large market in propertized personal data (and to prevent the consequences that would follow), coherently doing so, even in a sui generis fashion, would require embracing features of ownership that are fundamentally inconsistent with what it means to call something property.[164] Those who take this view begin from the premise that "property connotes free alienability" and argue that, once one starts down the road of propertizing data, one is either accepting that a market will arise or, in the interest of avoiding that result, proposing limitations on data ownership that lead to a type of property that is not truly property.[165] This objection needs to be taken seriously, not only because it goes to the heart of what propertized data could conceivably look like but also because it applies to the takings-based approach this Article proposes, which imagines a form of property that is not freely alienable but that is instead alienable only to a government buyer upon the demand of that buyer. Moreover, the specific proposal here implicates, as I indicate above, some of its own additional restrictions on alienation.[166]

---

[163] Indeed, because rights have their own protections in the Constitution, we need not avoid propertizing certain things merely to protect associated rights. For example, while books are property that the government can generally acquire through the exercise of eminent domain, an effort to do so for the purpose of stifling speech would very likely violate the First Amendment.

[164] See Schwartz, 117 Harv L Rev at 2091 (cited in note 23) (describing one "anti-propertization argument" as "rest[ing] on the very idea of free alienability, which is considered by many to be an inevitable aspect of property"). See also Margaret Jane Radin, *Contested Commodities* 18 (Harvard 1996) ("Many would say that the question of inalienable property is a contradiction in terms.").

[165] Schwartz, 117 Harv L Rev at 2090 (cited in note 23) ("In their view, once information is propertized, it will be difficult to limit an individual's right to sign away this interest."). See Samuelson, 52 Stan L Rev at 1138–40, 1171 (cited in note 149) (arguing that a primary difficulty with a property rights system for information privacy is how to "limit[ ] transferability" within a system based on alienability).

[166] See notes 136–39 and accompanying text.

The problem with conceiving of property as being inherently about free alienability is that it is just not true, at least not when framed in such stark terms.[167] As Professor Paul Schwartz has explained in the context of information property, "the idea that free alienability is an inexorable aspect" of property is "a problematic cartoon" that obscures a more complex reality in which one possesses property rights in some things without the complete ability to alienate those things.[168] To take just a few examples, consider that rights of first refusal are common and enforceable under many circumstances even though they require that a property owner permit an identified party (rather than anyone else) to buy her property if the party so chooses.[169] Conditions like these thus restrict the owner's ability to sell her property to whomever she wishes, yet they easily coexist with calling the property in question "property."[170] Conservation easements and historic preservation laws can likewise function as restraints on alienability, but it is not suggested that property burdened by such restrictions is no longer "property."[171] Similar restrictions on alienation arise on the intellectual property side as well. For example, copyright law provides that a grant of copyright is incompletely alienable and is instead

---

167 A leading property casebook puts it succinctly: "On most occasions you may sell or give away what you own, but not always. . . . Notwithstanding, we still talk about what you own as your 'property.'" Dukeminier, *Property* at 177 (cited in note 160). See also Jennifer E. Rothman, *The Right of Publicity: Privacy Reimagined for a Public World* 125, 131–32, 139 (Harvard 2018) (noting that "[l]imits can be, and have been, placed on the alienability of property in various contexts," particularly "when fundamental rights are at stake, the underlying property is one we wish not to commodify, or if transfers of the property are likely to be inefficient or even impossible," and offering as examples blood, historic buildings, human organs, military services, endangered species, and alcohol); Susan Rose-Ackerman, *Inalienability and the Theory of Property Rights*, 85 Colum L Rev 931, 931 (1985) (arguing that, when "defined as any restriction on the transferability, ownership, or use of an entitlement," "inalienability is pervasive in modern, developed societies, in developing nations, and in the historical past").

168 Schwartz, 117 Harv L Rev at 2093 (cited in note 23). See also *Moore*, 793 P2d at 509 (Mosk dissenting) (observing that "the same bundle of rights does not attach to all forms of property" and that, "[f]or a variety of policy reasons, the law limits or even forbids the exercise of certain rights over certain forms of property").

169 See Restatement (Third) of Property: Servitudes § 3.4, cmt f at 445 (2000).

170 Of course, there are circumstances under which the terms of a right of first refusal will be held to be an *unreasonable* restraint on alienation. See id. But recognizing the existence of a reasonable restraint on alienation means accepting that conceiving of property as necessarily about free alienability is too simplistic. See *Moore*, 793 P2d at 510 n 8 (Mosk dissenting) (using rights of first refusal as a similar example).

171 Restatement (Third) of Property: Servitudes § 3.4, cmt f at 445 (cited in note 169). See also Rothman, *The Right of Publicity* at 125 (cited in note 167) (observing that historic buildings have limitations placed on their alienability).

subject to an author's own inalienable right to terminate prior transfers within a particular period of time.[172] It also limits the subsequent alienability of certain nonexclusive licenses.[173] And statutes like the Video Privacy Protection Act of 1988[174] (VPPA), the Driver's Privacy Protection Act of 1994[175] (DPPA), and the Gramm-Leach-Bliley Act of 1999[176] (GLBA) either prohibit entities from transferring the information they possess in their files or impose conditions on the circumstances under which transfers can occur and on those to whom such information can be transferred.[177]

What these examples demonstrate is that "property is an artifact, a human creation that can be, and has been, modified in accordance with human needs and values."[178] And once we recognize that something can be thought of as property even if it is less than fully alienable, the idea of propertizing data ought to be less theoretically objectionable.[179] It also ought to be "less menacing to privacy" because it means that it is plausible to establish privacy-protecting limitations with respect to the transfers of data even if that data is conceived of as property.[180]

For all these reasons, there is a solid theoretical foundation for thinking of private data as property, or at least as sufficiently property-like. There is also therefore a basis for

---

172 See 17 USC §§ 203(a), 304(c). See also Schwartz, 117 Harv L Rev at 2092 (cited in note 23), citing *Marvel Characters, Inc v Simon*, 310 F3d 280, 282 (2d Cir 2002).

173 See Peter S. Menell, *Bankruptcy Treatment of Intellectual Property Assets: An Economic Analysis*, 22 Berkeley Tech L J 733, 800 (2007).

174 Pub L No 100-618, 102 Stat 3195 (1988), codified at 18 USC § 2710.

175 Pub L No 103-322, 108 Stat 2099 (1994), codified at 18 USC § 2721.

176 Pub L No 106-102, 113 Stat 1338 (1999).

177 See Schwartz, 117 Harv L Rev at 2099–2101 (cited in note 23); 18 USC § 2710(b) (VPPA); 18 USC § 2721 (DPPA); 15 USC § 6802 (GLBA).

178 Hanoch Dagan, *The Craft of Property*, 91 Cal L Rev 1517, 1532 (2003). See also Schwartz, 117 Harv L Rev at 2092 (cited in note 23) ("Property can also take the form of incomplete interests and, just as importantly, can serve to structure social relationships. . . . The role of alienability in property has always been more complex than [the rigid focus on alienability] implies.").

179 Schwartz, 117 Harv L Rev at 2126 (cited in note 23) ("[T]he inability to place restrictions on one's ability to trade personal data is an inevitable aspect neither of property in general nor of a particular property interest in personal information.").

180 Id at 2094. Even more, as Schwartz observes, insisting upon a conception in which personal information is either freely alienable property or not property at all "may encourage advocacy of only rearguard policies" that "at best merely lock[ ] in the current level of information privacy in the United States"—a level that privacy advocates generally view as "inadequate." Id at 2093. As this Article demonstrates, embracing propertized data, within limits, can break out of this cycle and improve the level of information privacy enjoyed by Americans. See Part III.A.

understanding the investigatory acquisition of that data—and the attendant intrusion upon privacy—as similar to the taking of a property right that requires compensation. And in fact, this connection between investigatory intrusions and property rights like the right to exclude has doctrinal roots too. As the Supreme Court has explained, such "property concepts" are instructive in "determining the presence or absence of the privacy interests protected by [the Fourth] Amendment."[181] After all, the text of the Fourth Amendment refers to types of property—"houses, papers, and effects"[182]—and thus reflects the Amendment's historically "close connection to property."[183] The British common law at the time the Fourth Amendment was adopted likewise expressed the concept of a search as one in which an unconsented entry onto property occurred.[184] Of course, the Court held in *Katz v United States*[185] that a search for Fourth Amendment purposes also occurs whenever the government violates a person's "reasonable expectation of privacy,"[186] but the Court has also consistently cautioned that the *Katz* test "supplements, rather than displaces," the traditional property-based tests.[187] Accordingly, principles of property law remain quite relevant in assessing and governing the kinds of investigatory activity in which the government may engage.[188]

For both doctrinal and conceptual reasons, then, it is fair to conceive of government access to ISP-held data as a form of property intrusion. Two further hurdles warrant brief attention at this stage.

---

181 *Byrd*, 138 S Ct at 1526, quoting *Rakas*, 439 US at 143 n 12.

182 *Jones*, 565 US at 404, quoting US Const Amend IV.

183 *Jones*, 565 US at 405. See also *Florida v Jardines*, 569 US 1, 11 (2013) (discussing favorably the "traditional property-based understanding of the Fourth Amendment" and "the Fourth Amendment's property-rights baseline").

184 See *Jones*, 565 US at 404–05, citing *Entick v Carrington*, 95 Eng Rep 807, 817 (CP 1765).

185 389 US 347 (1967).

186 Id at 360 (Harlan concurring).

187 *Byrd*, 138 S Ct at 1526. See also *Jones*, 565 US at 409; *Jardines*, 569 US at 10–11; id at 12 (Kagan concurring); *Rakas*, 439 US at 143 n 12 ("[B]y focusing on legitimate expectations of privacy in Fourth Amendment jurisprudence, the Court has not altogether abandoned use of property concepts in determining the presence or absence of the privacy interests protected by that Amendment.").

188 See *Rakas*, 439 US at 143 n 12 ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society."). See also *Carpenter*, 138 S Ct at 2272 (Gorsuch dissenting) (encouraging litigants to make such property law arguments).

One has to do with whether a taking of data for law enforcement reasons could be analogous to a taking for a "public use," consistent with the limitations of the Takings Clause. This is relevant, not strictly for doctrinal purposes but also for fleshing out the conceptual basis and justification for the analogy. Here, too, the fit is a reasonable one.[189] To start, recall that the Court has held that legislatures possess "broad latitude" to determine what uses justify takings.[190] But even beyond the deference owed to legislative judgments in this arena, understanding a taking of data for law enforcement purposes as analogous to a public use fits with other purposes that qualify as public uses. Indeed, the Court has held that "[p]ublic safety" and "law and order" are among "the more conspicuous examples" of the governmental aims and public purposes that can be pursued by the exercise of eminent domain.[191] For example, when the Court concluded that blight reduction constituted a public use, it approvingly cited the legislature's determination that the neighborhood in question had become "injurious to the public [ ] safety."[192] Likewise, when it concluded that reducing the concentration of land ownership was a public use, it again approvingly referenced the fact that the status quo had been "injuring the public tranquility and welfare."[193]

Still, it bears noting here that courts have held that "[p]roperty seized and retained pursuant to the police power is not taken for a 'public use' in the context of the Takings Clause," with the result that law enforcement does not regularly owe compensation when it seizes property in the course of a criminal investigation.[194] But this is not because law enforcement is not a "public use" as a constitutional matter. Rather, it is because "[t]he government may not be required to compensate an owner for property which it has already lawfully acquired under the exercise of governmental authority other than the power of

---

189 See *Haig v Agee*, 453 US 280, 307 (1981) ("It is 'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation."), quoting *Aptheker v Secretary of State*, 378 US 500, 509 (1964).

190 See *Kelo*, 545 US at 483; note 126 and accompanying text.

191 *Berman*, 348 US at 32.

192 Id at 28.

193 *Midkiff*, 467 US at 232.

194 *AmeriSource Corp v United States*, 525 F3d 1149, 1153 (Fed Cir 2008). See also Brian Angelo Lee, *Emergency Takings*, 114 Mich L Rev 391, 399 (2015) (observing that property losses resulting from certain police activities are generally noncompensable, and criticizing that principle).

eminent domain."[195] In other words, if the government's source of authority is outside of the realm of eminent domain, then its action is not a taking. But as I discuss above, the proposal here would root the government's power to acquire ISP-held data firmly in a takings-based regime and remove it from any other source.[196] From a doctrinal standpoint, then, there is little difficulty. Conceptually, one might nonetheless query why ISP-held data ought to be treated differently than any other information and property seized by law enforcement, but the foregoing discussion illustrates how this sort of information presents unique challenges for which the tools and limits employed in ordinary investigations have proven particularly unsatisfying and which may therefore necessitate unique solutions.[197]

The other hurdle is the concern that a takings approach to government investigation of ISP-held data would amount to an end-run around the Fourth Amendment's protections. But as I discuss above, this type of data is ultimately not well-protected by the Fourth Amendment because of the third-party doctrine and the rules surrounding administrative subpoenas.[198] Of course, if the Supreme Court were to dramatically alter either or both of these rules, a takings-inspired approach would face distinct obstacles. But unless and until that happens, the Fourth Amendment is essentially out of the picture for much ISP-held data. Accordingly, the path is cleared for a regime that borrows instead from the principles of property law that animate the Takings Clause.

---

[195] *Bennis v Michigan*, 516 US 442, 452 (1996). See also *AmeriSource Corp*, 525 F3d at 1153–54.

[196] See text accompanying notes 133–48.

[197] See notes 49–63, 69–76, 90–93, 116, and accompanying text. Of course, if there are other investigatory contexts in which a similar takings-inspired regime proved appropriate, it would be worth exploring the adaptability of this sort of regime. And indeed, given the renewed attention to an orthogonal but related issue—the validity and limits of asset forfeiture laws—there may well be some broader rethinking of the rules surrounding law enforcement acquisition of property and the compensation owed for it in the coming years. See, for example, *Indiana v Timbs*, 84 NE3d 1179, 1182–84 (Ind 2017) (describing the constitutionality of civil forfeiture laws under the Eighth Amendment), cert granted, 138 S Ct 2650 (2018).

[198] See notes 38–55 and accompanying text (observing the gaps in Fourth Amendment protection resulting from the third-party doctrine and the administrative search exception).

* * *

The final Part of this Article further fleshes out the potential upsides of such a regime, engages more deeply with potential downsides and implementation questions surrounding valuation, and concludes that, while the devil may be in the details, the Takings Clause may offer a promising and practical model for a statute that can guide the exercise of the government's power and cabin its discretion in this arena. The details of a statute like the DTA, and the idea as a whole, therefore warrant serious consideration.

## III. THE PRIVACY UPSIDE

The normative argument against a statute like the DTA—against taking data—is fairly straightforward: if the government can simply purchase access to ISP-held information, it will do so whenever it wants, for whatever ends it wants, largely free of restraint or review. Moreover, even if commodifying data is not the same as commodifying privacy,[199] there is still arguably something expressively unsavory about a regime that reduces privacy to something the government can pay to overcome. It may even risk demeaning privacy and further eroding society's respect for privacy outside the law enforcement context. After all, if government teaches by its example that privacy matters only insofar as government chooses not to pay an access fee, subjective expectations of privacy may decrease in ways that corporations, or even friends and neighbors, might exploit.[200]

---

[199] See notes 161–63 and accompanying text.

[200] See *Olmstead v United States*, 277 US 438, 485 (1928) (Brandeis dissenting) ("Our government is the potent, the omnipresent teacher. For good or for ill, it teaches the whole people by its example."). See also Craig Konnoth, *An Expressive Theory of Privacy Intrusions*, 102 Iowa L Rev 1533, 1535 (2017) ("[T]he very act of intrusion sends a message about the values society holds dear and the status that particular individuals have in society. Thus, certain searches . . . are harmful even if no damning information is found."). That said, this particular ship may have already sailed with respect to the commodification of data privacy. See Schwartz, 117 Harv L Rev at 2125 (cited in note 23) ("A strong conception of personal data as a commodity is emerging in the United States, and individual Americans are already participating in the commodification of their personal data."). Moreover, there is at least some reason to question whether what the law permits and what the government does, in fact, alter what people think about privacy and the values that are associated with it. Indeed, subjective expectations of privacy have been shown to be remarkably resistant to doctrinal shifts in Fourth Amendment law. See Matthew B. Kugler and Lior Jacob Strahilevitz, *The Myth of Fourth Amendment Circularity*, 84 U Chi L Rev 1747, 1750 (2017) (finding that, "[t]hough expectations move a little right after a major Supreme Court decision

That certainly sounds bad. And if you think it is bad, then the message of this Article is not simply that we should refrain from enacting a statute like the DTA but rather that there are yet additional reasons not to propertize data—reasons that do not turn on the specter of a full-fledged market in personal data but that arise from the consequences of even a more modest, single-purpose intervention.[201] Another message might be that the potential for government takings of ISP-held information is an additional reason for the Supreme Court to overrule or further limit its prior decisions with respect to the third-party doctrine, the rules surrounding subpoenas, and/or the remedies available for violations of the Fourth Amendment.[202]

But this last Part explores why this negative reaction is incomplete and why taking data may in fact represent a promising improvement on the status quo—one that could offer greater protection for privacy while satisfying law enforcement's need to conduct effective investigations that protect the public.

### A. Compensation's Effect

To see how the DTA may better achieve this balance, recall the SCA's current regime. With respect to unopened email that is six months old or younger, the statute's privacy protection is as strong as can be: the government needs a warrant. Assuming that the Constitution does not require such protection because that data has been revealed to a third party, the SCA's protection exceeds the constitutional floor.[203] Replacing the SCA with the DTA would therefore, at first glance, make it marginally easier for the government to access this information: instead of needing to get a warrant from a judge based on a showing of probable cause, the government would need only to make a

---

substantially changes Fourth Amendment law, within a span of months expectations snap right back to where they were beforehand and they remain stable thereafter").

[201] See notes 155–60 and accompanying text (exploring consequences of markets in personal data).

[202] See Part I.A. There are, of course, many who question the third-party doctrine on other, related bases. See notes 41–48 and accompanying text. See also, for example, Friedman, *Unwarranted* at 234–58 (cited in note 11); Baude and Stern, 129 Harv L Rev at 1872 (cited in note 12); Choi, 37 Cardozo L Rev at 217 n 166 (cited in note 5). But see generally Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 Mich L Rev 561 (2009) (arguing that the third-party doctrine prevents criminals from hiding their activities and clarifies the extent of Fourth Amendment protection).

[203] See notes 38–41 and accompanying text.

declaration of public use and pay compensation before taking data held by an ISP.[204]

Before turning to why things are more complex than that first glance, recall that *all the rest of the ISP-held information*—the content of unopened email more than six months old; the content of opened email of any age; and noncontent data like a user's name, address, connection and usage records, phone number, network address, service contract, payment information, sites visited, and addresses emailed—is offered little protection by the SCA.[205] At most, the government needs only to give a judge reason to believe that the information is relevant to an investigation; for some of this data, the government can even access it with a mere administrative subpoena.[206] With this low baseline, the worst-case scenario for the DTA is that it swaps one largely unprotective regime with another.

Of course, if the DTA makes no improvement to the protection afforded to a wide swath of ISP-held data and actually risks eroding the protection afforded to the rest of it, it is hard to see any upside. But that diagnosis assumes that taking such data under the DTA creates a merely procedural hurdle—the filing of a declaration of public use and the rest of the process set out in the statute. Not so. Rather, taking ISP-held data under the DTA would add two important substantive hurdles: the agency would have to pay for the data out of its budget, and the agency would have to report to congressional appropriators and to the public about precisely how much data it purchased and what investigatory and law enforcement benefits those purchases yielded.[207]

Together, the obligations to pay for investigatory searches of ISP-held data and to justify those purchases to Congress would do more to force agencies to internalize and consider the privacy-related costs of their activities than administrative subpoenas do—and perhaps even more than warrants do. Even warrants place nearly all the costs of the privacy intrusion on the person whose privacy is being intruded on. Besides the costs attendant to the applicable judicial processes, which are generally low, the

---

[204] Of course, if the Fourth Amendment does require a warrant for such content data, see notes 41 and 89, the DTA would not apply to that data and would instead apply only to the data that is outside the scope of the Fourth Amendment's protection.

[205] But see note 88 and accompanying text (noting doubts as to the constitutionality of the SCA's sub–warrant requirements for content data).

[206] See notes 80–86 and 96–100 and accompanying text.

[207] See notes 136–45 and accompanying text.

government faces no costs at all.[208] It matters not at all whether the investigation yields useful information, and thanks to the doctrine of qualified immunity, as I discuss above, nearly any defects in the government's investigatory process will result in no penalty beyond any evidence acquired being excluded at trial.[209] And even if exclusion were a meaningful cost for the government—which is far from clear—the good faith exception means that defects in a warrant or subpoena might not even result in exclusion.[210] Accordingly, the government perceives significant benefits from its investigatory activities when its efforts lead to convictions or thwarted criminal activity and, at worst, fairly neutral outcomes when they do not.[211] The result familiar to basic law and economics scholarship is that the government will overinvestigate relative to an efficient baseline.[212]

The innovation of the DTA would be to change all of this and force investigatory agencies to pay—and to pay up front—in terms of money for the costs of the information they seek to acquire from ISPs, and in terms of political capital when that money is perceived by legislative overseers and by the public to have been wasted. Moreover, because the costs faced by the agencies would reflect the fair market value of the particular

---

[208] See note 24 (describing the ease with which government agencies may acquire warrants). Professors Max Minzner and Christopher Anderson have demonstrated that law enforcement officers are sensitive to costs when conducting warranted wiretaps, but wiretaps are a particularly expensive type of search. Max Minzner and Christopher M. Anderson, *Do Warrants Matter?*, 9 Rev L & Econ 169, 191–92 (2013). As they explain, the Wiretap Act requires that recorded calls be

> "minimized," or continuously monitored in real time so that monitoring of a particular transmission can be stopped once it is determined to not relate to criminal activity. As a result, any time that a call is recorded by law enforcement, agents must be available to simultaneously listen to the call as it occurs.

Id at 172 (citation omitted). Needless to say, execution of an ordinary search warrant is far less labor intensive than that and, accordingly, far less costly. Note as well that I am assuming a certain baseline of fixed labor costs that the government will invest, more or less, in a particular investigation regardless of the method or form of legal authorization for that investigation. My focus is on the marginal costs that particular threshold authorizations—warrant, subpoena, taking, etc.—add to the mix.

[209] See note 59 and accompanying text.

[210] See notes 55–57 and accompanying text.

[211] As Professor Barry Friedman put it, law enforcement presently gets to "writ[e] its own blank checks," secure in the knowledge that other people bear the burdens. Friedman, *Unwarranted* at 257 (cited in note 11).

[212] See, for example, Richard A. Posner, *Economic Analysis of Law* 56–57 (Wolters Kluwer 9th ed 2014) (exploring the socially inefficient consequences of government not internalizing the costs of its behavior).

information being acquired,[213] those costs would necessarily be set at the retail level by the market rather than, as they effectively are now, at the wholesale level by Congress. In contrast to the inherent difficulties that arise when a legislature tries to draw lines in this context, the DTA would entail little risk of categorical over- or underprotection of privacy.[214] Instead, the costs faced by law enforcement would reflect, at a more finely calibrated level, the privacy actually intruded on by law enforcement activity. The decisions that law enforcement would make based on those costs would accordingly be better tailored and would strike a superior balance, having emerged from a more accurate accounting of the costs and benefits in a given circumstance. In sum, we would have (more) economically rational decision-making, (more) transparency, and (more) democratic accountability: the very things policing has been said to be missing.[215]

If the result were a complete internalization of the precise privacy costs of these agencies' activities at a case-by-case level, agencies would engage in an efficient level of privacy-intrusive investigations. But even if the DTA would not lead agencies to perfectly internalize *all* of the costs of their data-related investigatory activities—a likely impossible goal—it would do so at least to some degree. We would thus expect to see at least a marginal reduction in the amount of overinvestigation and therefore a marginal improvement in the protection of privacy both quantitatively and qualitatively—not only relative to the SCA's regime but, again, even relative to a warrant requirement.

This account is well rooted in the standard efficiency rationale for compensating takings in the ordinary context—takings involving condemnations of land for the creation of parks and the like. As former Judge Richard Posner and Professors Frank Michelman, Michael Heller, James Krier, and many others have argued, if the government did not have to

---

[213] See note 119 and accompanying text.

[214] See notes 13–15, 114–15 and accompanying text (discussing inadequacies of either/or privacy protection legislation).

[215] Friedman, *Unwarranted* at 46 (cited in note 11) (explaining that one of the biggest challenges in regulating policing, especially with respect to new technology, is that far too much of it is "shrouded in secrecy to a degree that is often difficult to comprehend" and arguing that transparency is "essential"); id at 71 (emphasizing that cost-benefit analysis is "one of the primary tools of good government" that is sorely lacking in policing).

compensate property owners for land taken by eminent domain, the government would take whatever property and whatever resources maximized its own benefits, regardless of the costs to the dispossessed property owners and regardless of the costs to society at large.[216] In other words, government "would not feel incentives, created by the price system, to use those resources efficiently."[217] The Takings Clause's compensation requirement is thus understood to lead government to make efficient takings decisions—to take property only when the public benefits of the taking outweigh the burdens and costs on the private owner.

That, as promised, is how a significant tool of property law strikes the kind of balance that has proven elusive when it comes to investigations of ISP-held data. Adapting that tool to transform searches of ISP-held data into endeavors that must be similarly compensated should be expected to have the same result: government would make efficient investigatory takings decisions that take proper account of the privacy interests in a given circumstance. At a minimum, government would make decisions that are *more* efficient and *more* conscious of the privacy costs than those it currently makes under the SCA or the Fourth Amendment in the absence of a compensation requirement.

This line of argument was, however, called into question in a seminal article by Professor Levinson, which argued that government does not internalize costs like a private firm does, as would be necessary for the standard account to hold.[218] Levinson

---

[216] See, for example, Posner, *Economic Analysis of Law* at 56–57 (cited in note 212); Michael A. Heller and James E. Krier, *Deterrence and Distribution in the Law of Takings*, 112 Harv L Rev 997, 1001 (1999); Thomas W. Merrill, Dolan v. City of Tigard*: Constitutional Rights as Public Goods*, 72 Denver U L Rev 859, 882–83 (1995); Robert C. Ellickson, *Suburban Growth Controls: An Economic and Legal Analysis*, 86 Yale L J 385, 420 (1977); Frank I. Michelman, *Property, Utility, and Fairness: Comments on the Ethical Foundations of "Just Compensation" Law*, 80 Harv L Rev 1165, 1218 (1967). To be clear, however, I do not mean to suggest that law enforcement responds *only* to budgetary constraints. See Ronit Levine-Schnur and Gideon Parchomovsky, *Is the Government Fiscally Blind? An Empirical Examination of the Effect of the Compensation Requirement on Eminent-Domain Exercises*, 45 J Legal Stud 437, 463 (2016) (providing data that "call[s] into question" the theory that officials "are exclusively motivated by budgetary constraints" when making takings decisions). In fact, I do not mean to imply any single explanation for government action. Rather, I simply mean to suggest that law enforcement in fact responds to budgetary constraints, as well as related accountability constraints, and that a regime that leverages those constraints would ultimately be, for lack of a better word, marginally more constraining.

[217] Heller and Krier, 112 Harv L Rev at 999 (cited in note 216).

[218] Levinson, 67 U Chi L Rev at 359 (cited in note 26).

explained that the very incentive effects just set out rely on the assumptions that, first, "government will not take full account of the costs of takings unless it is forced to pay money from the treasury,"[219] and second, that forcing government to pay in such a manner would in fact force government to internalize the costs of its takings and to make "socially optimal choices" with respect to takings.[220] These assumptions, Levinson argued, are fundamentally flawed because government does not care about financial outflows or inflows *qua* financial outflows and inflows. Rather, government responds only to political incentives, and while those political incentives may be "causally connected to social costs and benefits, [ ] they are not the same thing."[221] And more damning still, Levinson showed that that causal connection is indeed quite complex and indeterminate.[222]

It is no understatement to say that Levinson's argument "revolutionized" the standard account of government cost-internalization and has led scholars to rethink the doctrines surrounding compensation for both constitutional torts and takings.[223] But, for four reasons, Levinson's quite fair observations do not ultimately undermine the argument that a takings-based regime for law enforcement acquisition of ISP-held data, under the circumstances I outline here, could result in an increased degree of privacy protection and a step toward a more efficient level of data searches.

First, much of what Levinson had to say is about the incentives felt by elected officials, not heads of administrative agencies and certainly not more junior bureaucrats constrained by their departments' budgets. At times, he said as much outright.[224] At other times, the limitation was baked into the argument. For example, Levinson accurately undermined the analogy between private firms and elected officials by explaining that, because investors in a private firm have largely

---

219 Id at 349.

220 Id at 347.

221 Id at 357.

222 Levinson, 67 U Chi L Rev at 357 (cited in note 26).

223 Lawrence Rosenthal, *A Theory of Governmental Damages Liability: Torts, Constitutional Torts, and Takings*, 9 U Pa J Const L 797, 830 (2007) ("It is perhaps only a slight exaggeration to say that Levinson has revolutionized academic thinking about governmental damages liability").

224 Levinson, 67 U Chi L Rev at 361 (cited in note 26) ("[T]he accountability argument starts from the understanding that *elected* officials make decisions based solely on political costs and benefits.") (emphasis added). See also id at 363, 374, 377.

homogeneous incentives to maximize value, they force the principals of the firm to pursue that shared cost-minimizing, profit-maximizing goal.[225] By contrast, citizens as a group have no a priori preference for their representatives to pursue any particular goal, let alone a cost-reduction one.[226] As a result, the claim that elected officials will evaluate costs in the same way as a private firm was based on a flawed assumption—and that is on top of the fact that those officials are less faithful agents than are firm managers because the mechanisms of both selection and control are more attenuated in their electoral context.[227]

But it is not at all clear that this line of argument applies to bureaucrats with the same force with which it applies to elected officials. For one thing, bureaucrats in a particular agency share that agency's relatively more homogeneous goal and therefore aim to avoid costly expenditures that detract from that goal.[228] And while they may disagree about specific priorities or about the best ways to achieve them—just like in firms—the universe of interests is narrowed substantially. The list of possible maximands is therefore narrowed as well, which makes it at least marginally more possible for an agency head to identify and maximize some particular "value" in the same way that private firms do with profit. As a result, whereas Levinson was right that elected officials may not care about how money gets spent, the same cannot be said quite so easily with respect to bureaucratic actors.[229] Even if the analogy to firms is imperfect, then,

---

[225] Id at 354–55.

[226] Id at 355.

[227] Id at 355–56.

[228] See Michael D. Frakes and Melissa F. Wasserman, *Does Agency Funding Affect Decisionmaking?: An Empirical Assessment of the PTO's Granting Patterns*, 66 Vand L Rev 67, 83 (2013) (discussing the "ample evidence that many civil servants are mission minded").

[229] See Rosenthal, 9 U Pa J Const L at 864 (cited in note 223) (noting that the obligation for government to "budget for compensation" and attend to the opportunity costs associated with its payment restrains government action). See also John Rappaport, *How Private Insurers Regulate Public Police*, 130 Harv L Rev 1539, 1594–95 (2017) (noting, based on interviews with police officials, consultants, and insurers, that being made to pay for police (mis)conduct "impact[s] [some police agencies'] daily operations"); Joanna C. Schwartz, *How Governments Pay: Lawsuits, Budgets, and Police Reform*, 63 UCLA L Rev 1144, 1173, 1195 (2016) (observing that "[o]fficials want to maximize the amount of money they have available to achieve their agency's objectives" and finding that law enforcement agencies "do appear to be financially impacted" by having to pay for their misconduct); Kerr, 164 U Pa L Rev at 601 (cited in note 25) ("Police chiefs must staff cases, and they must distribute law enforcement resources within existing budgets. By influencing choices about where police resources will go, costs imposed on the government will influence how the police behave.") (citation

one need not be quite so fatalistic about the potential for an agency to be made to internalize costs at least to some degree.[230]

To be sure, Levinson does acknowledge that bureaucrats behave "quite differently" from "vote-maximizing legislators" but concludes that they do so in ways that are ultimately too indeterminate to predict.[231] Drawing on Professor William Niskanen's classic rational choice model, which assumes that the appropriator in charge of the agency's budget knows the agency's output but not its costs, Levinson explains how a bureaucrat's desire to maximize her agency's budget could result in the bureaucrat spending money either unwisely (so as to lead the appropriator to see low output and to raise the budget in response) or wisely (so as to avoid giving the appropriator the impression that the agency is a waste and should have its funding reduced).[232] It is certainly fair enough to note that predicting exactly what the bureaucrat will *do* in order to maximize value is not a simple task, even assuming that the value being maximized is merely budgetary and not mission-oriented. But to say as much is to concede that, unlike an elected official, a bureaucrat *is* trying to maximize a value, and minimize a cost, that is not only political.

Moreover, the structure contemplated by the DTA undoes one of Niskanen and Levinson's core assumptions: that the appropriator does not know the agency's cost schedule. Under the DTA, the investigating agency would have to pay for the data out of its budget and would be obligated to give Congress reports

---

omitted); Frakes and Wasserman, 66 Vand L Rev at 75 (cited in note 228) (modeling the "benevolent-but-resource-constrained bureaucrat").

230 Indeed, there is at least some empirical evidence to support the claim that the police do, in fact, take costs into account when deciding which investigations to pursue. See Minzner and Anderson, 9 Rev L & Econ at 189 (cited in note 208) (concluding, based on a study of federal criminal wiretaps, that "law enforcement [ ] considers the exogenous costs and benefits from each [wire]tap and chooses to pursue those taps that maximize the benefits it receives within its budget"). Department of Justice officials have even expressly identified costs as a central factor considered when determining whether to conduct a particular wiretap. See id at 174, citing *Wiretaps: A DEA Agent's Perspective: Interview with Special Agent Mark Styron*, in 45 USABulletin *29, 30 (Executive Office for United States Attorneys, Sept 1997), archived at http://perma.cc/3NJN-CCQF. For further evidence that law enforcement bureaucrats modify their behavior in light of cost considerations, see Itai Ater, Yehonatan Givati, and Oren Rigbi, *Organizational Structure, Police Activity and Crime*, 115 J Pub Econ 62, 66 (2014) (finding that police arrested more people once police stopped bearing the cost of housing arrestees).

231 Levinson, 67 U Chi L Rev at 380 (cited in note 26).

232 Id at 381–82, citing William A. Niskanen Jr, *Bureaucracy and Representative Government* 24–30, 36–42 (Aldine 1971).

of what the agency spent on data takings, how many takings it made, and what law enforcement goals were advanced as a result. It hardly requires a great leap of faith to expect that a bureaucrat who consistently fails to make wise investments with her limited budget will either change tactics of her own accord or be prompted to change them by the appropriator. After all, it seems a perfectly fair assumption that Congress would prefer to see money spent on successes rather than on failures. Because Congress will possess the knowledge of how that money got spent, an agency with more failures than successes would naturally face budgetary repercussions. And a smart agency head would incorporate the *prospect* of having to divulge such information to Congress into her plans and be motivated to avoid those repercussions in the first place.[233]

To take a simple example from the law enforcement context—one that is a few steps outside the realm of the DTA but that will serve to illustrate the point—imagine that a police department that engaged in stop-and-frisk investigatory tactics had to pay the person stopped and then report to the local government how much money had been spent and whether the stops led to arrests.[234] We know that stop-and-frisk has a remarkably low success rate,[235] but a big part of why similar practices persist (where they have not been enjoined) is undoubtedly because the costs of the erroneous stops are borne only by the people who are stopped, and these people lack political power and/or are too diffuse to harness that power.[236] If

---

[233] See Michael C. Pollack, *Land Use Federalism's False Choice*, 68 Ala L Rev 707, 750 (2017) (arguing that such budgetary oversight can improve agency decision-making and make it more rational and less biased). See also William W. Buzbee, *Urban Sprawl, Federalism, and the Problem of Institutional Complexity*, 68 Fordham L Rev 57, 108 (1999).

[234] This hypothetical is a spin on Professor Baer's proposal for local police departments to pay a fee to a federal agency reflecting the harm of their search activity. See note 28.

[235] See, for example, *Floyd v City of New York*, 959 F Supp 2d 540, 573–75 (SDNY 2013) (discussing an expert report finding that just 12 percent of stops resulted in an arrest or summons, and 88 percent resulted in no further law enforcement action); Sharad Goel, Justin M. Rao, and Ravi Shroff, *Precinct or Prejudice? Understanding Racial Disparities in New York City's Stop-and-Frisk Policy*, 10 Annals Applied Statistics 365, 374–75 (2016); Friedman, *Unwarranted* at 141 (cited in note 11) ("[T]he NYPD has found weapons roughly 1.5 percent of the time, and guns in less than 0.1 percent of the stops. Barely ever.").

[236] See Kerr, 164 U Pa L Rev at 603 (cited in note 25) ("Those who typically bear the external costs of investigations—criminal suspects and those who live with or near them—tend to be relative outsiders to the political process. They are outnumbered considerably by those who see themselves as victims of crime.") (citation omitted); *Wiretaps* at *36 (cited in note 230); Friedman, *Unwarranted* at 61 (cited in note 11) ("[T]he people

police departments paid for every stop and then had to justify those unproductive expenses to their appropriators and political superiors, someone would surely start asking whether all the misses were worth the cost.[237] And those doing the asking might even start to come from more politically powerful groups.[238] The DTA would accomplish the same goal, replacing the status quo—which does not have this internalize-and-justify effect—with a regime that does.[239]

Second, even setting to one side these differences between elected officials and bureaucrats and taking Levinson's argument on its own terms, financial costs often *do* translate into the kinds of political costs Levinson said government is attuned to. When financial outlays are directed toward expenses that bring no social benefit—and that therefore cannot be exploited for political benefit—they are at best useless for politicians.[240] Even worse, in a world of finite resources, such useless expenses carry

affected by policing aren't usually as organized—or organized at all. It's no secret that the heaviest burden of aggressive policing falls disproportionately on the shoulders of minorities, on the less well-off.").

[237] See Minzner, 87 Tex L Rev at 940 (cited in note 24) (arguing that penalizing low search success rates—by, for example, discounting probable cause claims made by officers with low rates—would "force law enforcement to care a great deal about whether innocent people are searched and how to respond to those failures").

[238] See Baer, 58 Wm & Mary L Rev at 1150–51 (cited in note 24) (arguing that requiring police departments to pay an annual fee to a federal agency for their search activity would "perform[ ] a kind of risk-spreading function" that would "force[ ] citizens, who have heretofore not been subject to [policing activity], to at least recognize the police-related costs that a fraction of the city's residents experience on a daily basis"); Friedman, *Unwarranted* at 319 (cited in note 11) (arguing that, the more that policing affects everyone, the more reasons there are for more people to be "careful about the form it takes" and to "ask harder questions about the benefits and the costs"). See also Maureen E. Brady, *The Damagings Clauses*, 104 Va L Rev 341, 404–05 (2018) (arguing that compensation in the takings context works to discipline government officials by correcting for the relatively low political capital historically possessed by those most burdened by infrastructure projects).

[239] Of course, if agencies (including law enforcement agencies) are sensitive to costs under a warrant regime, see note 230, one might argue that the very cost-internalization theory that justifies the DTA demonstrates that it is unnecessary: the answer to the SCA's flaws is instead to replace it with a warrant regime. Recall, however, that the empirical claim that police are already sensitive to search costs arose in the context of uniquely expensive and labor-intensive searches. See note 208; Kerr, 164 U Pa L Rev at 612 (cited in note 25) (cautioning that it is "perhaps impossible to measure accurately" the extent to which the Fourth Amendment already causes police to internalize costs). These are not representative of all law enforcement investigatory activity. Moreover, as noted above, there are operational problems with an across-the-board warrant requirement that a regime like the DTA would avoid. See notes 107–08 and accompanying text.

[240] See Baer, 58 Wm & Mary L Rev at 1163 (cited in note 24) (noting that a fee-for-search scheme would "highlight[ ] and render[ ] more salient a police department's inefficient search activity" and thus impose political costs).

large opportunity costs: every dollar spent on a program that is not beneficial or effective at advancing some political goal is a dollar not spent on a program that is beneficial or that could have advanced a political goal.[241]

Professor Lawrence Rosenthal persuasively made this same point with respect to government damages liability. If government were truly not attuned to costs, as in the most extreme version of Levinson's argument, then it would be largely indifferent to such liability.[242] One would therefore expect government to devote next to no resources toward minimizing such liability; if liability creates no cognizable costs, then government would have no reason to minimize those costs, let alone divert resources from other politically beneficial programs to do so. And yet, Rosenthal pointed out, governments go to great lengths to enact governmental tort immunity legislation despite the fact that there is no obvious lobby in favor of such legislation.[243] The conclusion must therefore be that immunity legislation itself confers political benefits, which means that liability "exacts a political price."[244]

The point is ultimately a fairly intuitive one. When a person is observed trying to avoid a particular outcome, one concludes that that person perceives the outcome to impose costs on herself. Whether those costs are financial, reputational, political, or otherwise—or whether one type of cost creates another type of cost—is largely beside the point.[245] And we perceive government trying to avoid incurring the very sorts of costs that Levinson said governments do not internalize. The

---

241 See id; Rappaport, 130 Harv L Rev at 1593–95 (cited in note 229) (describing ways in which financial incentives and costs can be translated into political ones); Rosenthal, 9 U Pa J Const L at 799 (cited in note 223) (noting the political price that is paid when funds are "divert[ed] . . . from what elected officials regard as their politically optimal use"); Christopher Serkin, *The Meaning of Value: Assessing Just Compensation for Regulatory Takings*, 99 Nw U L Rev 677, 728 (2005) ("[A]ny government that takes property will necessarily bear some political cost for having to outlay money, because that money must be raised either through increased taxes or cutting back on other services.").

242 Rosenthal, 9 U Pa J Const L at 841 (cited in note 223).

243 Id at 839.

244 Id. See also Myriam E. Gilles, *In Defense of Making Government Pay: The Deterrent Effect of Constitutional Tort Remedies*, 35 Ga L Rev 845, 859–61 (2001) (arguing that one salient way in which liability exacts a political price is in terms of adverse publicity, particularly on high-profile social issues).

245 See Gilles, 35 Ga L Rev at 861 (cited in note 244) (explaining that remedies, "although denominated in dollars, clearly translate into the political currency that moves political actors").

natural conclusion is that government *does* in fact internalize those costs even if it is not doing so in the financial way that firms do and, instead, is doing so only because those costs are transformed into political ones.

Accordingly, we can say that government will generally be deterred from taking a particular action when the political costs of that action outweigh the political benefits. The status quo imposes almost no political costs on agencies that use the legal tools at their disposal to access ISP-held data. For all the reasons discussed above, the result is likely to be overuse of those tools and, in turn, excessive intrusions on privacy. By contrast, legislation like the DTA would ramp up the costs associated with using those tools—whether one calls the costs financial or financial-cum-political—and thus bring their use closer to some level of social optimality.

Third, and closely related, widespread or fruitless data takings under the DTA are unlikely to go unnoticed by the general public. One critique of the story of political costs I discuss above—both those that arise as a result of bureaucrats who might care about how money gets spent and those that arise as a result of the appropriations and oversight relationship between agencies and Congress—is that the public will not care about the practice or the expense and that the resulting political pressure would therefore be low. But the attention associated with takings of ISP-held data would likely be particularly salient because that scheme would touch simultaneously on public sensitivities surrounding privacy—like those animated by the Apple-FBI dispute I discuss above[246]—*and* on public sensitivities surrounding eminent domain.

Indeed, at a minimum, if the potential for public outcry based on privacy sensitivities already limits the government's reach under the status quo, the DTA would do nothing to erode that limitation. But the DTA can go even further because, as the takings literature has long recognized, the public's reaction to eminent domain can be especially powerful as well. For example, Rosenthal has argued that the Takings Clause's "compensation requirement imposes political discipline well in excess of that usually operating in the political arena."[247] Professor Richard Epstein has likewise argued in the zoning context that regulation

---

[246] See notes 3–7 and accompanying text.

[247] Rosenthal, 9 U Pa J Const L at 867 (cited in note 223).

is "a lot easier to impose than outright takings" because, when regulating, "the government does not have to conduct a parcel-by-parcel condemnation paid for out of public revenues."[248] If you do not believe that the latter takings approach creates political opposition, Epstein says, "just think of the furious public response to *Kelo* [*v City of New London*[249]]," the 2005 case in which the Supreme Court held that private property could be condemned and transferred to another private party if the transfer is in furtherance of economic development.[250] Opposition to the very idea of such an exercise of eminent domain was so widespread that all but a handful of states amended their eminent domain laws to prohibit the kind of takings that *Kelo* held were constitutionally permissible.[251] Writing in the *New York Times*, Adam Liptak called the public reaction "a revolt" from "Democrats and Republicans, liberals and libertarians, and everyone betwixt and between."[252]

Of course, the taking at issue in *Kelo* became uniquely salient largely *after* the Court issued its decision. I do not mean to suggest that every individual taking spurs the same ferocity, though there remains some empirical and anecdotal evidence suggesting as much.[253] But all the same, there is reason to

---

[248] Richard A. Epstein, *The Unfinished Business of* Horne v. Department of Agriculture, 10 NYU J L & Liberty 734, 753 (2016).

[249] 545 US 469 (2005).

[250] Epstein, 10 NYU J L & Liberty at 753. See also *Kelo*, 545 US at 483–84.

[251] See Dana Berliner, *Looking Back Ten Years after* Kelo, 125 Yale L J F 82, 84–88 (2015) (cataloging the forty-four states that changed their laws after *Kelo* to tighten the definition of "public use" or "public purpose" and the additional three states' high courts that did the same); Ilya Somin, *The Political and Judicial Reaction to* Kelo (Wash Post, June 4, 2015), online at http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/06/04/the-political-and-judicial-reaction-to-kelo (visited Oct 22, 2018) (Perma archive unavailable) (noting that "[n]o other Supreme Court decision in all of American history has generated so much state legislation" and that "over 80% of the public disapproved of the ruling," but arguing that most of the flurry of new state legislation is ineffective).

[252] Adam Liptak, *Case Won on Appeal (to Public)* (NY Times, July 30, 2006), online at http://www.nytimes.com/2006/07/30/weekinreview/30liptak.html (visited Oct 22, 2018) (Perma archive unavailable).

[253] See, for example, Logan Strother, *Beyond* Kelo*: An Experimental Study of Public Opposition to Eminent Domain*, 4 J L & Courts 339, 359 (2016) (reporting survey and experimental data showing that Americans generally oppose eminent domain); Logan Strother, *Trump's Border Wall Would Become a Lot More Unpopular If He Tried to Build It* (Wash Post, Oct 12, 2016), http://www.washingtonpost.com/news/monkey-cage/wp/2016/10/12/trumps-border-wall-would-become-a-lot-more-unpopular-if-he-tried-to-build-it/ (visited Oct 22, 2018) (Perma archive unavailable); Annmarie Timmins, *Poll: Most Granite Staters Oppose Eminent Domain for Northern Pass* (Concord Monitor, Jan 17,

believe that coupling invasions of privacy with invasions of property would meaningfully amplify the political costs associated with investigations of ISP-held data. After all, the required compensation for the taking is owed immediately and predictably, which means that "the political impact of compensation is unusually direct, immediate, and predictable."[254] Because it is difficult for government to evade or to mask the financial outflow associated with takings, both the expense *and* the public accounting of opportunity costs—the prospect of what else that money could have been spent on—can quickly become political facts that get weaponized by opposition or other interest groups.[255]

Fourth and finally, the political toxicity of takings makes at least some scholars concerned that the government's obligation to pay compensation *overdeters* action.[256] Professor Bethany Berger, for example, has examined the effect of state statutes requiring compensation for losses caused by land use regulation and concluded that the result of them all was to "simply shut regulation down."[257] For example, Oregon's Measure 37, a ballot initiative that required local governments to compensate property owners for losses in value caused by land use restrictions enacted subsequent to acquisition, led most local governments to simply waive the relevant restrictions with respect to the affected parcels.[258] Paying compensation, the localities explained, was simply a bad use of limited funds.[259] The same pattern emerged under similar regimes in Florida and Arizona.[260]

---

2012), http://www.concordmonitor.com/Archive/2012/01/999694482-999694483-1201-CM (visited Oct 22, 2018) (Perma archive unavailable).

254 Rosenthal, 9 U Pa J Const L at 864 (cited in note 223).

255 See Baer, 58 Wm & Mary L Rev at 1162–63 (cited in note 24) (noting that a transparent and immediate payment scheme makes political costs more likely to be perceived by officials and, therefore, to be effective deterrents); Rappaport, 130 Harv L Rev at 1593 (cited in note 229) (observing that "many police agencies," for example, "care about professionalism—about *being seen as* doing things 'the right way'") (emphasis added); Serkin, 99 Nw U L Rev at 728 (cited in note 241) (following the "decades of scholarship" that accepts that "increased compensation will decrease the government's appetite" for interferences with private property).

256 See, for example, Harcourt and Meares, 78 U Chi L Rev at 869 (cited in note 28) (discussing the concern that a compensation requirement will be internalized by police too much and to the detriment of effective policing).

257 Bethany R. Berger, *The Illusion of Fiscal Illusion in Regulatory Takings*, 66 Am U L Rev 1, 34 (2016).

258 Id.

259 Id. See also Bethany R. Berger, *What Owners Want and Governments Do: Evidence from the Oregon Experiment*, 78 Fordham L Rev 1281, 1303, 1307 (2009).

260 Berger, 66 Am U L Rev at 35–36 (cited in note 257).

Of course, the subject of this Article is not regulatory takings, but the lesson applies all the same: governments and agencies with limited resources acting in an area of high political salience can be expected to react to a compensation requirement with at least some degree of hesitation—to perceive some degree of deterrence—over and above that which would have existed in the absence of a compensation requirement.[261] Insofar as the experiences in Oregon, Florida, and Arizona suggest that the degree of deterrence may even be excessive, that is simply further evidence that a flat-out rejection of the idea that government internalizes costs in this context is mistaken.

But as for the countervailing concern that a regime like the DTA could similarly overdeter, it seems unlikely that the government would drop serious, major investigations. Instead, the government's desire not to miss out on catching a potential terrorist or major criminal figure or fraudster (and incurring the attendant political costs) could be expected to meet the government's desire not to misallocate resources toward fruitless data takings and privacy intrusions (and to avoid the attendant political costs) and produce a relatively balanced posture toward investigative takings.[262]

### B. Measuring Compensation

With all of this in mind, the next obstacle to overcome with respect to identifying the upside of a regime like the DTA has to do with the level of compensation—how much the government would have to pay for a particular slice of ISP-held data—and its deterrent or efficiency-promoting effect. Generally speaking, just compensation is the fair market value of the property taken, assessed at the time of the taking.[263] One might therefore make two

---

[261] See Hanoch Dagan, *Just Compensation, Incentives, and Social Meanings*, 99 Mich L Rev 134, 138 (2000) ("Assuming that democratic mechanisms make public officials accountable for budget management, compensation is important to create a budgetary effect that forces governments to internalize the costs that their decisions impose on private resource holders.").

[262] See Gilles, 35 Ga L Rev at 875 (cited in note 244) (arguing that "decreased law enforcement output" is a "singularly unlikely result" of subjecting municipalities to punitive damages for constitutional violations because "the penalty for inaction," that is, reduced policing, "would seem to be at least as high" as the financial penalty associated with "incurring liabilities"); Rosenthal, 9 U Pa J Const L at 843 (cited in note 223) (arguing that "there is little reason to believe that the government will overinvest in loss prevention, or underinvest in eminent domain").

[263] See note 119 and accompanying text. Of course, many have noted that compensation based on fair market value will often be inadequate. See, for example, Lee Anne

objections: first, that measuring the value of this kind of data will not be easy to do, and second, that even if doing so were feasible, the value would be so low that the compensation owed by the government would be too little to have a meaningful privacy-promoting effect. This final Section tackles both objections.

As for the first objection, there are a number of ways one might measure the value of the privacy stored in ISP-held data. There are already fairly widespread markets in some personal data like consumer information—including browsing histories.[264] The prices generated in those markets could provide a useful starting point. Valuation methods under the DTA could then be further refined to reflect the DTA's operating context. To start, imagine that a particular piece of data is a potentially inculpatory piece of evidence in the investigation of a significant crime, terrorist enterprise, or civil fraud. There are, of course, any number of people who would want that sort of information not to be private—who, in other words, would pay to purchase and lift from the data its private quality: the investigating governmental entities, to be sure, but also the press, amateur sleuths, victims' families, academic researchers, or even museums and libraries interested in archiving a potential piece of history. There is also, of course, the set of people who would like to keep their own information private.[265] All of those people are potential buyers in a hypothetical market for the information. A sense of the data's value can therefore be developed in the same way that value is measured for property in the ordinary takings context: by comparing what those other market participants have paid in the past to uncover similar private information.[266] For example,

---

Fennell, *Taking Eminent Domain Apart*, 2004 Mich St L Rev 957, 962–67 (calling it a "truism" that fair market value does not offer complete compensation because it does not account for subjective value, the owner's opportunity to realize some surplus from a voluntary transfer of the property, or the loss of autonomy). I do not mean to suggest that that problem will be overcome in this context, but some of the valuation techniques discussed below—particularly those tied to the user's willingness to pay to keep her data private—would go some way toward ameliorating it here. See notes 277–84 and accompanying text.

[264] See *Data Brokers: A Call for Transparency and Accountability* *13–14 (Federal Trade Commission, May 2014), archived at http://perma.cc/CZH7-9T3R.

[265] See notes 151–54 and accompanying text (discussing the value of the right to exclude); Stern, *Intellectual Property* at *61–62 (cited in note 154) (emphasizing that the private nature of a private communication represents much of that communication's value).

[266] See *United States v 564.54 Acres of Land, More or Less, Situated in Monroe and Pike Counties*, 441 US 506, 513 (1979) (examining "recent sales of comparable facilities in the vicinity"); *United States v Toronto, Hamilton & Buffalo Navigation Co*, 338 US

while governmental entities have not previously been made to pay in this context, other entities like museums or collectors often do pay to acquire historically significant items that might be reasonably analogous.[267] And once the DTA's regime picked up speed and experience, courts and investigating entities would have little trouble arriving at valuations based on similar past DTA-based acquisitions.

Granted, this might be easier said than done. But the DTA would hardly be the first context in which agencies and courts have encountered difficult-to-quantify values, so more than a few solutions have been developed. For example, executive branch agencies are all required by executive order to undertake cost-benefit analyses for new regulatory actions.[268] Given the fact that certain benefits resist ready quantification—for example, the aesthetic value of clear air—regulators have turned to other "appropriate proxies that simulate market exchange."[269] One proxy "widely considered the best" uses revealed preference methods.[270] Revealed preference methods estimate the value of something by observing people's "actual behavior in market or market-like settings" that are roughly analogous.[271] So in the context of the DTA, even if we cannot measure the value of the private quality of a particular piece of data, we might be able to observe the lengths to which similarly situated people go in order to keep private similar information and measure the costs of that activity.[272] For example, we could draw

396, 404 (1949) (explaining that "price at the market nearest the taking is, at least in the usual case, a practical rule of thumb"); Serkin, 99 Nw U L Rev at 683 (cited in note 241).

[267] See, for example, Daniel Grant, *With the Economy Improving, Museums Go on a Buying Spree* (Observer, Jan 28, 2015), archived at http://perma.cc/WZX6-AH9G (describing multimillion-dollar museum acquisitions).

[268] See Executive Order 13563, 3 CFR 215, 215 (2011); Executive Order 12866, 3 CFR 638, 638 (1993); *Circular A-4: Regulatory Analysis* *1 (Office of Management and Budget, Sept 17, 2003), archived at http://perma.cc/VFU5-629N ("Circular A-4") ("This Circular is designed to assist analysts in the regulatory agencies by defining good regulatory analysis . . . and standardizing the way benefits and costs of Federal regulatory actions are measured and reported.").

[269] *Circular A-4* at *19 (cited in note 268).

[270] John Bronsteen, Christopher Buccafusco, and Jonathan S. Masur, *Well-Being Analysis vs. Cost-Benefit Analysis*, 62 Duke L J 1603, 1658 (2013).

[271] Richard H. Pildes and Cass R. Sunstein, *Reinventing the Regulatory State*, 62 U Chi L Rev 1, 76 (1995). See also, for example, Bronsteen, Buccafusco, and Masur, 62 Duke L J at 1613, 1647 (cited in note 270) (discussing revealed preference methods); *Circular A-4* at *20–21 (cited in note 268).

[272] See Serkin, 99 Nw U L Rev at 688 (cited in note 241) (noting that "it is common to value takings by the property owner's harm" when the gain to the buyer is "not immediately quantifiable").

inferences from the consumer market for privacy technologies like two-factor authentication, thumbprint or facial scanners, and the like. Or we might observe how much various actors generally pay to make public documents and information with similar potential and draw inferences from that behavior. Agencies and experts would be able to further refine these practices as they gained experience with the statute's scheme.[273]

Another common method is just to ask people how much they would be willing to pay for a particular outcome or benefit or to avoid a particular harm.[274] To continue with the clear air example noted above, when the EPA considered a proposal to regulate emissions from a power plant near the Grand Canyon, one of the inputs for its cost-benefit analysis was naturally the aesthetic benefit of clear air over the Grand Canyon.[275] There is no market in clear air, so the EPA estimated the value of clear air by showing people photos of the Grand Canyon in different conditions and asking them how much they would pay to enjoy a particular level of visibility on their visits.[276] It would not be hard to adapt that kind of study to the context of the DTA. The same kind of hypothetical market participants listed above could be surveyed and asked how much they would pay to either acquire or keep private information similar to the subject of a particular DTA taking.[277]

---

[273] To be sure, revealed preference methods are far from perfect. Consumers' imperfect information, cognitive biases, and difficulty predicting how particular events or conditions will make them feel all can undermine the conclusions one might draw from their behavior. See Bronsteen, Buccafusco, and Masur, 62 Duke L J at 1648–56 (cited in note 270). All I mean to suggest, then, is that they can serve as a proxy—just as they do in a host of other regulatory arenas—until the courts and investigatory agencies, through experience, refine their assessments of value.

[274] See Pildes and Sunstein, 62 U Chi L Rev at 80 (cited in note 271). This is called a "contingent valuation" or "stated preference[ ]" study rather than a "revealed preference[ ]" study. Bronsteen, Buccafusco, and Masur, 62 Duke L J at 1613 (cited in note 270); *Circular A-4* at *22 (cited in note 268).

[275] Alexander Kazam, *From Independence Hall to the Strip Mall: Applying Cost-Benefit Analysis to Historic Preservation*, 47 Envir L 429, 450 (2017).

[276] See id at 450–51.

[277] There are, of course, drawbacks to willingness-to-pay surveys, and a significant one in this context is the danger of wealth bias: "[A] wealthy person might think nothing of paying $10,000 for cleaner skies, whereas a poorer individual would be highly unlikely to suggest such a price." Bronsteen, Buccafusco, and Masur, 62 Duke L J at 1662 (cited in note 270). But this is not because the two individuals actually assign different values to the benefit; rather, it is because "the *money* is worth less to the wealthy person." Id at 1652. Unless it is accounted for, the declining marginal value of money can thus distort the conclusions one would draw from a willingness-to-pay survey. To prevent DTA compensation from replicating this effect (and, for example, assigning higher prices to a

In fact, scholars have already begun to conduct precisely these kinds of surveys, and while they are focused largely on the willingness-to-pay-for-privacy side rather than on the willingness-to-pay-for-acquisition side, it would not be hard to ask those questions too.[278] Many of these surveys have found, however, that, "when asked to pay" for privacy, people are "strikingly stingy."[279] Studies have found, for example, that people are willing to pay no more than $15 per year to avoid automated content analysis of email messages.[280]

Findings like these give rise to the second objection: even if it were easy to arrive at a measurement of the value of the relevant data's private nature, the price will be too low to effectively deter the government. There are a few key points to remember here, however. First, the question under a takings regime is not asked generally ("How much would you pay to keep/how much would you accept to sell your property?") but specifically ("How much would you pay to keep/how much would you accept to sell *this* property?").[281] When the subject is tangible property, the specific question ought to yield a lower price than the general one because people will rationally aggregate their property values when answering the general question. But the opposite effect is at least possible when the subject is personal data. After all, people may not remember each and every embarrassing website they have visited and so may offer a low price when answering the general question, but once confronted with even a single embarrassing piece of data, they may put a higher price on that information.[282] Further, even if people are relatively

---

wealthier person's data), it would be necessary to control for it in some fashion. Solutions range from relatively minor adjustments—such as introducing a "percentage of wealth" factor, see Gregory Scott Crespi, *Correcting for the Wealth Bias of Cost-Benefit Analysis through Use of "Percentage of Wealth"–Based Valuations*, 46 Creighton L Rev 149, 155 (2013)—to more dramatic ones—such as using a social "well-being" analysis rather than a traditional willingness-to-pay model, see Bronsteen, Buccafusco, and Masur, 62 Duke L J at 1607 (cited in note 270).

[278] See Omri Ben-Shahar and Lior Jacob Strahilevitz, *Contracting over Privacy: Introduction*, 45 J Legal Stud S1, S5 (2016) (collecting sources).

[279] Id.

[280] See id.

[281] See notes 119 and 145 and accompanying text (discussing the fair-market-value standard for takings).

[282] Of course, people are generally bad at predicting "how much pleasure or displeasure future events will bring." Timothy D. Wilson and Daniel T. Gilbert, *Affective Forecasting: Knowing What to Want*, 14 Current Directions Psychological Sci 131, 131 (2005). See also Bronsteen, Buccafusco, and Masur, 62 Duke L J at 1656, 1659 (cited in note 270) (noting that people are "notoriously bad" at speculating about how certain

comfortable with exposure of their personal data to automated systems, they may feel considerably different about exposure of that same data to actual human beings.[283] So while it may well be that some would feel just as cavalier either way, there is at least some reason to believe that, when primed to focus on a specific salient piece of information that would be exposed to an actual person, many would offer higher estimates of their willingness to pay.[284] Add in the fact that the information would be exposed in a personally identifiable fashion to the government, and people might really begin to feel differently.[285]

---

events would make them feel or about how much they would be willing to pay to achieve or avoid that event). This is a problem that inheres in any sort of stated preferences evaluation, but it is especially pernicious when the event in question is vague, remote, or foreign to people's regular lives. See id at 1655–56, 1659–60 (cited in note 270). One virtue of a takings-inspired regime like the one this Article discusses is that the valuation question operates in a relatively more salient and tangible context. See also id at 1615 (cited in note 270) (arguing that the more the question being asked is rooted in immediate and in-the-moment self-assessments, the more trustworthy the answers will be).

[283] Professor Matthew Tokson has argued that, while "the available evidence indicates that Internet users do not consider disclosure of their online information to automated equipment to be a privacy harm in and of itself," they nonetheless "consider disclosure of their information to other human beings to be a substantial harm" and have in fact been "actively hostile to the latter." Matthew Tokson, *Automation and the Fourth Amendment*, 96 Iowa L Rev 581, 628 (2011). Tokson has also presented survey results suggesting that people "distinguish between exposure to human beings and exposure to automated systems" when evaluating privacy invasions, rating as exceptionally intrusive scenarios in which individuals "read user e-mails" or "view[ ] their e-mail to/from addresses" while assigning dramatically lower ratings to scenarios in which e-mail content was read by "automated spam detection software." Id at 624–25.

[284] In a recent revealed preference study of "right to roam" legislation in the United Kingdom, Professors Jonathan Klick and Gideon Parchomovsky found that even laws that require "minimally invasive" public access to private property and that therefore "may seem to have only a trifling effect on the right to exclude" nonetheless lead to "a statistically significant and substantively important drop in property values." Klick and Parchomovsky, 165 U Pa L Rev at 963, 966 (cited in note 151). In other words, intrusions upon the right to exclude that may seem minor in the abstract can translate into demands from property owners for more significant compensation once those intrusions are made concrete.

[285] See Matthew B. Kugler and Lior Jacob Strahilevitz, *Actual Expectations of Privacy, Fourth Amendment Doctrine, and the Mosaic Theory*, 2015 S Ct Rev 205, 259–60 (finding that survey respondents believed that it would be a greater intrusion on privacy for the police to obtain emails from an ISP than it would be for police to track cell phones; acquire cell site location data from a cell service provider; inspect a hotel registry to discover names, addresses, and room numbers of the guests who stayed at the hotel on a particular night; use facial recognition software to check whether fans at the Super Bowl matched a Department of Homeland Security database; or install a video camera to watch a public park where criminal activity had recently occurred). See also Joseph Turow, Michael Hennessy, and Nora Draper, *The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them up to Exploitation* *3 (Annenberg School for Communication, June 2015), archived at http://perma.cc/S2Z5-42XT (finding that people

This valuation reasoning applies all the same even if the data taken is merely a duplication and not the original.[286] One might argue that no compensation would be owed under those circumstances, but that claim overlooks the fact that, ultimately, the value being taken is the private quality of the data. In other words, when the government copies personal data for its own use, it interferes with the owner's rights to exclude others from that data and to control the use of that data just as if it took the original.[287] So even though the government does not eliminate the owner's right to possess the data when it does not take the original, it still invades some of the owner's core property rights. And when the data in question is valuable to its owner or creator precisely because it is private, the loss of privacy that comes from the loss of the right to exclude is especially important.[288] In fact, recognizing as much is another advantage of a takings-inspired approach like the DTA. In the Fourth Amendment context, a seizure occurs only when the government has made "[a] meaningful interference with an individual's possessory interest" in the property in question.[289] On that theory, the government's copying of computer data might not implicate the protections of the Fourth Amendment at all.[290] An approach like the DTA, by contrast, would recognize that the data's value is primarily its private nature and would therefore put a price—and thus a limitation—on the government's ability to copy it.

The foregoing has focused on the market price from the perspective of a creator of data, but there is also reason to believe that the opposite perspective—that of potential buyers—would likewise generate significant prices. For example, given the lengths to which people and the press have gone to find and publicize them, and the urgency with which they have been

---

who provide personal information to marketing companies in private commerce do so not because they do not value their privacy, but because they are "resigned to giving up their data" and "believe it is futile to manage what companies can learn about them").

286 Of course, it is also not hard to imagine reasons why the government might wish to control further dissemination of the subject data and would therefore find it necessary to acquire the original.

287 See notes 151–54 and accompanying text.

288 See id; Stern, *Intellectual Property* at *61–62 (cited in note 154). See also *Monsanto*, 467 US at 1013 (holding that government effects a taking when it discloses a company's confidential information).

289 *United States v Jacobsen*, 466 US 109, 113 (1984).

290 See Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv L Rev 531, 560 (2005) (outlining such a result and calling it "troublesome").

reported, the imputed market value of President Donald Trump's tax returns or of evidence of any communications between him or his staff and Russian operatives or businessmen is likely quite high indeed.[291] And that is even without any other evidence that such documents would ultimately reveal any crime to have been committed.

Finally, even if the magnitude of the compensation owed to an individual were low, that would not mean that the government would avoid facing a meaningful constraint on its behavior. In many circumstances—indeed, perhaps the most vexing for privacy advocates—the government may not know precisely who its target is and so will instead set out to obtain hundreds, thousands, or even more pieces of data before filtering them to find what it needs.[292] Each individual person whose information was collected in this sort of "big data" sweep might not receive very much compensation if the fair market value of her data turned out to be low, but the aggregation of all of that compensation would translate to a much heftier bill for the investigating entity. And it is from that perspective that the constraint would emerge—much as it does in the context of, for example, class actions involving a large number of small claims.[293]

For all of these reasons, there is at least some reason to believe that the costs to government that would attend the acquisition of this kind of data in a takings-based regime would create a meaningful deterrent effect for law enforcement and result in some degree of privacy promotion. There is also, however, another concern from the opposite direction. One might say that

---

[291] See, for example, David Barstow, et al, *Donald Trump Tax Records Show He Could Have Avoided Taxes for Nearly Two Decades, the Times Found* (NY Times, Oct 1, 2016), online at http://www.nytimes.com/2016/10/02/us/politics/donald-trump-taxes.html (visited Oct 24, 2018) (Perma archive unavailable). See also note 24 (collecting sources noting substantial prices paid for potentially incriminating recordings from associates of Charles Manson and President Nixon).

[292] See Friedman, *Unwarranted* at 259, 263–71 (cited in note 11) (discussing government database-formation and associated large scale data-collection). See also *Carpenter*, 138 S Ct at 2225 (Kennedy dissenting) (observing that the "market for cell phone data," for example, "is now estimated to be in the billions of dollars").

[293] See Alexandra D. Lahav, *The Political Justification for Group Litigation*, 81 Fordham L Rev 3193, 3200 (2013) (explaining that class actions "make it possible to hold institutions and individuals accountable for their actions" even when those actions generate claims that are of low value to individuals because they allow those claims to be aggregated); Jonathan R. Macey and Geoffrey P. Miller, *The Plaintiffs' Attorney's Role in Class Action and Derivative Litigation: Economic Analysis and Recommendations for Reform*, 58 U Chi L Rev 1, 8–9 (1991) (discussing the economic rationale for class action litigation).

this kind of data may well be valuable—too valuable, in fact. In other words, the market might price information that relates to a particularly major investigation higher than it does more quotidian information. From one perspective, one would desire the opposite effect: make it cheaper for government to access information closely and obviously related to major investigations while making it more expensive for government to access information that is much farther afield. One might worry that government would shift toward the low-hanging fruit and be more apt to acquire such run-of-the-mill information (or, more precisely, less likely to be deterred from acquiring it). But, for all the reasons I discuss above, it is unlikely that government would forgo the expensive yet fruitful investigation and instead engage in many cheap yet fruitless investigations.[294] Instead, the more likely effect is that agencies would marshal their limited resources and save their money for the expensive yet fruitful investigations by *not* wasting it on cheap yet fruitless ones. In other words, increasing the cost of the investigations that are most central to the government's mission and that are most politically salient could be expected to decrease the extent to which government engages in unrelated investigations that are unlikely to produce actionable information.[295]

Finally, if these arguments about the government facing a meaningful level of compensation are unsatisfying, one solution would be to embed into the DTA the equivalent of a liquidated damages clause: a statutorily set minimum amount the government must pay as compensation. Congress has done exactly this in other privacy statutes. For example, the Video Privacy Protection Act and the Driver's Privacy Protection Act, both discussed above, provide that the court may award "actual damages but not less than liquidated damages in an amount of $2,500."[296] Similarly, the Cable Communications Policy Act,[297] a statute that protects cable subscriber information, provides that a court can award "liquidated damages computed at the rate of $100 a day for each day of violation or $1,000, whichever is

---

294 See notes 235–62 and accompanying text.

295 Another solution to this concern would be to embed in the statute clearly delineated circumstances or triggers under which the data-taking power could be exercised. See note 141 (addressing this possibility). Rigorous legislative oversight and public reporting would likely go a long way toward ameliorating this concern as well.

296 18 USC §§ 2710(c)(2), 2724(b)(1).

297 Pub L No 98-549, 98 Stat 2794 (1984), codified at 47 USC § 521 et seq.

higher."[298] For the purposes of the DTA, Congress—informed by experts—could make its best judgment about what minimum amount would lead investigating agencies to adequately internalize the costs of their privacy intrusions. To be clear, relative to market pricing, this would generally be a second-best solution in terms of optimizing the government's investigatory activity. But it could at least be a starting point for further tinkering. And if set even close to correctly, it would represent an improvement upon the status quo.

After all, keep in mind that the status quo imposes on government nearly no costs at all with respect to investigating ISP-held data. Recall that the SCA empowers government to access this sort of data without a warrant in many cases.[299] And the administrative costs associated with securing subpoenas or court orders—even more so than those associated with warrants—are low.[300] But even if those administrative costs were meaningful, a data taking would be accompanied by administrative costs of its own too. The important difference is that the DTA would *add* the costs of compensation. And even if the compensation associated with data acquisition were small or imperfectly set, it would still be greater than zero. Requiring the payment of such compensation should, therefore, be expected to throw *some* sand into the gears and, at least relative to the baseline, introduce *some* deterrent effect.[301]

## CONCLUSION

The government's power to intrude upon citizens' privacy in the course of investigating potentially unlawful and dangerous conduct is an awesome one. How it ought to be exercised and channeled in the digital age is a question of central importance that is actively debated by policymakers, lawyers, judges, scholars, and citizens alike. Lost among all the various proposals in that debate, however, is the fact that this elusive balance between private burdens and public benefits has already been struck to at least some degree of satisfaction in an

---

298 47 USC § 551(f)(2)(A).

299 See note 86 and accompanying text.

300 See notes 50–55 and accompanying text.

301 Of course, if it turns out that requiring compensation throws little to no sand in the gears, that may be a sign that privacy is not as highly valued as we think, which would itself represent something of a solution to the struggle between privacy and law enforcement.

analogous context: the government's power under the Takings Clause. There, too, the government has the ability to interfere with citizens' privacy—including the enjoyment and possession of their private property—for the public good. But the fact that the government must compensate people for the property it takes—and the fact that that compensation turns on the value of the specific property being taken—disciplines the exercise of this otherwise wide-ranging ability to intrude at the government's own pleasure.

This Article has, therefore, explored how this area of property law might inspire a different kind of statutory framework for the investigation of ISP-held data. Specifically, drawing on the processes under which the government uses its takings power, Congress could enact a statute that creates a form of property ownership in the author of certain ISP-held data, requires the government to "take" the private data it wants, and forces the government to pay the owner just compensation for that data. By enabling the government to access information that may be important for the protection of public safety and welfare while at the same time requiring the government to internalize the privacy costs of its investigatory activity, and by allowing market prices rather than one-size-fits-all legislation to determine those costs, taking data has the potential to coherently and efficiently protect privacy and the public all at once.