University of Miami International and Comparative Law Review

Volume 24
Issue 1 *Fall 2016*

Article 4

8-28-2017

Disposing With a (Not-So) Blunt Instrument, for Privacy's Sake

Victoria Ashley Paxton

Disposing with a (Not-so) Blunt Instrument, for Privacy's Sake

Virginia Ashley Paxton

I. INTRODUCTION

In a 2014 episode of *Morgan Spurlock: Inside Man*, Academy Award nominee Morgan Spurlock journeys through the shadowy world of data-brokering.[1] The object of Spurlock's quest is to learn who is keeping tabs on him, why they are keeping tabs on him, and, most importantly, what they know. Through his interview and experiments with private investigator Steve Rambam and an interview with Ladar Levison (the sole creator, owner, and operator of Lavabit, LLC[2]), Spurlock generates a foreboding portrait of

---

1. *Morgan Spurlock, Inside Man: Privacy* (CNN television broadcast May 4, 2014). About halfway through the episode, Spurlock observes, "This whole business operates in the shadows. No one will go on camera and put a face to this faceless industry. I just want answers." *Id.*

2. Edward Snowden had used Lavabit, an encrypted email service that aimed to protect its users from compelled production for government investigations. Kashmir Hill, *Lavabit's Ladar Levison: 'If You Knew What I Know About Email, You Might Not Use It'*, FORBES.COM (Aug. 9, 2013), http://www.forbes.com/sites/kashmirhill/2013/08/09/lavabits-ladar-levison-if-you-knew-what-i-know-about-email-you-might-not-use-it/. Levison, who had created the encrypted email service in 2004,

> was concerned that the FBI could send a company a national security letter . . . that would force [email service providers] to turn over information about a customer without going through a court first. "I wanted to put myself in the o of not having

the data brokering and marketing business. His portrait reveals how legal boundaries defining personal privacy in the commercial world have dissolved to mere illusion. Within the illusion, who the consumers are, what the commodity is, how the commodity is being packaged and sold, who is selling it—and why they are selling it—is so obscured by the ubiquitous presence of marketing chameleons that people have given up keeping up. The critical question emerging at the end of the episode concerns consumer knowledge and consent to electronic surveillance by data collection companies: "Do [consumers] have a choice?"[3]

> information to turn over," he said. "I didn't want to be put in the position of compromising people's privacy without due process." *Id.*

Levison was forced to shut the business down when the FBI came knocking on his door for information. *Id.*

[3]. *Spurlock, supra* note 1. *See, e.g.*, Kashmir Hill, *Lavabit's Ladar Levison: 'If You Knew What I Know About Email, You Might Not Use It'*, FORBES.COM (Aug. 9, 2013), http://www.forbes.com/sites/kashmirhill/2013/08/09/lavabits-ladar-levison-if-you-knew-what-i-know-about-email-you-might-not-use-it/. In her short biography, Senior Online Forbes editor and journalist, Kashmir Hill, declares, "I have no illusions about privacy." *Id.* Her affirmation, which echoes the perspective of most modern literate people, stands in noteworthy contrast to Levison's suggestion (at the end of his interview with Hill) that he does not presently use email because of the compromises it involves. *Id.*

A data brokerage company CEO answers, "Yes, of course" (because people can always "opt out," people can "opt out of everything"). While there's little doubt this option exists, the problem is that people rarely seek to opt out of something they don't know they're already in. Though consumers generally grasp they are consenting to another party's gathering some information about them during a given transaction, they cannot know the floodgate of information-sharing they enable each time they "check a box" to access a desired web page.[4]

In an August 2013 interview with law and technology journalist, Kashmir Hill, Spurlock's interviewee Ladar Levison pronounced, "I'm taking a break from email. . . . [and i]f you knew what I know . . . , you might not use it either."[5] Apple's chief executive, Tim Cooke, echoed Levison's outlook in a February 2015 interview where he stated that "consumers often don't fully understand what's going on. . . . One day they will, and will be very offended."[6] Spurlock's private investigator, Steve Ramdam, predicts a more dramatic public reaction to the depth of data gatherers'

---

4. *Spurlock, supra* note 1.

5. *Lavabit's Ladar Levison: 'If You Knew What I Know About Email, You Might Not Use It'*, FORBES.COM (Aug. 9, 2013), http://www.forbes.com/sites/kashmirhill/2013/08/09/lavabits-ladar-levison-if-you-knew-what-i-know-about-ed5trmail-you-might-not-use-it/.

6. Allister Heath, *Apple Boss: We Have a Human Right to Privacy*, THE TELEGRAPH (Feb. 27, 2015, 11:55 GMT), http://www.telegraph.co.uk/technology/apple/11441265/Terrorists-should-be-eliminated-says-Apples-Tim-Cook.html.

intrusions into consumers' private affairs. He suggests data brokerage companies resist sharing with consumers the information they collect because "first, they don't want to establish a precedent. If they give it to [one consumer] . . . three hundred million Americans would want it, and frankly there would be a revolution against these ad entities. If [consumers] knew, the information they had on [them], [*they*] *would go nuts*. There would be a second American Revolution."[7]

Information, defined as "knowledge communicated concerning some particular fact, subject or event" or "that of which one is apprised or told[, such as] intelligence [or] news,"[8] always constitutes some manufactured, projected reflection of reality. The modern world requires that people produce their personal information for identification purposes so they can participate in social, economic, and political activities. After producing information to create an identity, people use that identity to venture into the intangible cyber-world to live a large part of their lives. Personal information often, then, serves to represent and disseminate people's tangible reality to the world.

Today's data gatherers not only collect the "personally-identifiable information" people produce to create an acting persona on the internet, they also surveil and reproduce a reflection of every persona's experience *while the persona acts* on the internet. The aggregated, newly-

---

7. *Spurlock, supra* note 1 (emphasis added).

8. *See* OED ONLINE. Oxford University Press, September 2015. Web. 7 October 2015.

arranged data becomes a commodity, "capable of being reduced to money without changing in value, and completely interchangeable with every other commodity in terms of exchange value,"[9] for marketing companies. Because we live in a world where our "information" precedes us, this commodification process—which implicates the superficial signifiers comprising the identity (name, date of birth, and social security number) as well as the individual experiences that develop the identity—hinders our ability to make autonomous decisions regarding when, where, and how we engage with the world.

The economic incentive for gathering, arranging, and sharing practically free-for-all information about individuals' lives drives the futile public outcry for more privacy protection in the virtual domain.[10] "There are more than 1,000 data brokers in the United States, the largest of whom claim to have detailed data profiles of nearly every American consumer and household."[11] Personal information is rarely deemed the property of the individual subject,[12] but

---

9. Margaret Jane Radin, *Contested Commodities* 3 (1996).

10. Apple executive Tim Cook, for example, has declared that "privacy is a basic human right." Heath, *supra* note 6.

11. Sarah Ludington, *Reining in the Data Traders: A Tort for the Misuse of Personal Information*, 66 MD. L. REV. 140, 143 (2006).

12. *See In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1075 (N.D. Cal. 2012). "The weight of authority holds that a plaintiff's 'personal information' does not constitute property." *Id.* (citing *Thompson v. Home Depot, Inc.*, No. 07cv1058 IEG, 2007 WL 2746603, at *3 (S.D. Cal. Sept. 18, 2007); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 713–14 (N.D. Ca. May 12, 2011)).

it still has an exchange value and can be traded in the open market. The individual traveling along the virtual highway is ever-vulnerable to having his data "highjacked" and rarely travels without paying his dues to the faceless bandits who stalk him.

Cases of information hijacking have proliferated along the virtual highway over the last decade with inconsistent legal results.[13] The courts routinely analyze issues regarding personal-information "appropriation" by commercial entities—enabled mostly by internet surveillance—under the Title II of the Electronic Communications Privacy Act (also known as the Stored Communications Act (SCA)).[14] The laws reflect principles promoted by the Supreme Court at a critical mid-century pivot point in Fourth Amendment jurisprudence.[15] Inherent

---

13. *See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 988 F. Supp. 2d 434 (D. Del. 2013) ("Plaintiffs [did] not sufficiently allege[] that the ability to monetize their [PII] [was] diminished or lost by virtue of Google's previous collection of it"); *Del Vecchio v. Amazon.com, Inc.*, No. 11-366, 2012 WL 1997697, at *2 (W.D. Wash. June 1, 2012) (finding the plaintiffs' allegations of Amazon's "dissemination and use of personal information *belonging to [the plaintiffs]*, including sensitive information about their web browsing and shopping habits, purchases, and related transaction information, combined with their financial information such as credit and debit card information, and their mailing and billing addresses" sufficient for the plaintiffs to have standing (emphasis added)).

14. 18 U.S.C. § 2701 (2012). *See, e.g.*, *Google*, 988 F. Supp. 2d at 440; *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

15. These principles arise from shifting perspectives of what individuals can and should expect to remain private outside the context of property analysis. *See Katz v. United States*, 389 U.S. 347 (1967).

in these principles is the rule that once something is shared, the law no longer recognizes it as something the individual has a legitimate interest in keeping private.[16] If "legitimate" privacy expectations determine whether people have the right to control the dissemination of their personal information, the third-party doctrine will knock down appropriation actions just about every time they arise.[17] As Justice Marshall dissented in *Smith v Maryland*,[18] "Unless a person is prepared to forgo use of what for many has become a personal or professional necessity, he cannot help but accept the risk of surveillance."[19] Current privacy laws

---

16. *See, e.g.*, *Miller*, 425 U.S. at 443. "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed 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." *Id.*

17. *See e.g.*, *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 509 (S.D.N.Y. 2001) ("[P]laintiffs' argument is essentially that this Court should ignore § 2701(c)(2) because Congress failed to take adequate account of 'basic property and privacy notions.' However, it is not this Court's role to revisit Congress' legislative judgments").

18. 442 U.S. 750 (1976) (Marshall, J., dissenting) (critiquing the Court's holding that even if a person does entertain a subjective "expectation of privacy in the phone numbers he dial[s], . . . [such an] expectation [is] not legitimate." *Smith v. Maryland*, 442 U.S. 735, 745 (1976). Under the majority's reasoning, then, "[t]he installation and use of a pen register . . . was not a 'search,' and no warrant was required." *Id.* at 745–46).

19. *Smith*, 442 U.S. at 750 (Marshall, J., dissenting) (internal citations omitted). "It is idle to speak of 'assuming' risks in contexts where, as a practical matter, individuals have no realistic alternative." *Id.*

like the SCA give businesses no reason not to sell personal information about their customers to the highest bidder.

The third-party doctrine practically obliterates privacy interests in information that has been shared, at any time, with any one. Hence, Chief Justice Roberts recently remarked in a relatively lucid moment of insight, "[I]t would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment."[20] The Chief Justice never explained the reasoning behind his observation. His remark implies an at least dim awareness that the "blunt instrument" provides less protection for individuals against governmental intrusions than other sources the Court has consulted (like Webster's dictionary[21]) to define the boundaries of privacy protection against private entities.

Legal recourse premised on property rights for data brokerage companies' sale of personal information would curtail the incessant abuse of "lawful" surveillance by commercial entities.[22] This paper proposes, then, that data

---

These statements challenge the majority's reasoning that "individuals who convey information to third parties have 'assumed the risk' of disclosure to the government." *Id.* (internal citations omitted).

20. *Riley v. California* 134 S. Ct. 2473, 2497 (2014).

21. *See Reporter's Committee*, 489 U.S. at 763–64:

22. *See* Ludington, *supra* note 11. "[I]t is currently legal—in the sense that there is no penalty for data traders to sell personal information without the consent of the subject, to deny individuals information about the quantity or categories of lists that contain their

brokers' sale of consumer identities— without direct and explicit consent from the consumer at the point where any profit might be reaped—should qualify as an unauthorized interference with the consumers' identity. Whether the information signifies a valuable, or profit-bearing, enterprise to the individual subject matters less than the fact that almost every individual, by necessity, uses his identity in basic ways to support his livelihood; in some cases, a person's virtual persona functions to support his existence to a greater extent than his physical body does. When the profit incentive is removed from the system, businesses will focus their efforts elsewhere.

The paper examines the Stored Communications Act—as exemplary of statutory laws purporting to protect people's personal information—to reveal how modern legislation fails to protect personal information because it merely echoes Fourth Amendment notions of privacy (and property). Congress has mistakenly followed the Supreme Court's lead in ignoring the essential relationships among property, privacy, and autonomy. This argument unfolds by examining cases of information use by entities other than the subject. It compares constitutional and statutory law with common law theories of privacy and property, questioning why Congress would shape laws regulating commercial trade of personal information from an Orwellian notion of privacy rather than on models the Court has solidly legitimized in non-constitutional inquiries. Part II discusses

---

information, and to deny any requests to remove personal information from these lists." *Id.*

judicial constructions of privacy under constitutional law as well as analyses of common law, examining how the SCA inaptly integrates Fourth Amendment concepts to protect personal information. Part III examines judicial constructions of property, explaining that pecuniary damages requirements impede successful lawsuits brought on property bases.

II. PRIVACY

Nearly twenty years ago,[23] the Court denied a reporter's FOIA request for a rap sheet that was a public record; Justice Stevens observed that the aggregation of public records in such a fashion would negate the "practical obscurity" that otherwise protected those records. He noted, "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[24] The difference incorporates the immeasurable value—representing the work burden—of an organic approach to data compilation. Justice Stevens suggests the work burden imposed by an organic approach would suffice to mitigate exploitation of personal-data accessibility. Considered from a privacy-rights perspective, the opinion may "at first blush" appear arbitrary and

---

23. *Dept. of Justice v. Reporter's Committee for Freedom of the Press*, 489 U.S. 749 (1989).

24. *Id. at* 764.

"quaint,"[25] but "practical obscurity" also explains the economic incentive for technologically-enabled data trade. The workload required to produce an accurate representation of any individual by compiling his personal information is no longer impractical.

Just five years after *Department of Justice v. Reporter's Committee for Freedom of the Press*, Congress amended the SCA to become what it is today. It is upon modern judicial constructions of this statute that consumers watch their privacy dwindle at the hands of corporate commercial entities (most of whom they unwittingly "do business with"). In one landmark case, *In re DoubleClick Privacy*

---

[25]. *See* Hannah Bergman, *Out of Sight, Out of Bounds*, THE NEWS MEDIA & THE LAW 11 (Spring 2009) (quoting Utah's Judicial Council in 2004) (remarking,

> The most compelling argument against protecting aggregate compilations of otherwise public records is the obvious one: the individual records are public. This argument, while persuasive at first blush, ignores the very real benefits of 'practical obscurity' that exist when certain public information is available only in discrete, individual units, be they paper or electronic. Practical obscurity may well turn out to be nothing more than a quaint, Luddite notion, but, as things stand today, practical obscurity helps maintain a delicate balance between public access to court records and at least minimal personal privacy.).

Litigation, a data gathering service—undetected by internet users—"record[ed] [their] movements throughout . . . affiliated Web site[s] . . . [to] learn what information [they] sought and viewed."[26] When the plaintiffs sued under the SCA (and other like statutes), the New York district court declared, "[P]laintiffs' argument is essentially that this Court should ignore § 2701(ct)(2) because Congress failed to take adequate account of 'basic property and privacy notions.' However, it is not this Court's role to revisit Congress' legislative judgments."[27]

A. FOURTH AMENDMENT DERAIL: RIGHTS OF ACCESS

In *Hennessey v. Coastal Eagle Point Oil Company*[28] in 1992, New Jersey Supreme Court Justice Pollock noted Justice Black's dissenting opinion in *Griswold v. Connecticut*,[29]

---

26. 154 F. Supp. 2d 497, 504 (S.D.N.Y. 2001).

27. *See, e.g.*, *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 509 (S.D.N.Y. 2001).

28. 129 N.J. 81 (1992) (Pollock, J., concurring). The plaintiff in *Hennessey* was challenging his discharge from employment due to the results of a mandatory drug test. He argued that the drug test violated what he believed to be his constitutional right to privacy.

29. 381 U.S. 479, 510 n.1 (1965) (Black, J., dissenting). "Observing that 'the right of privacy . . . presses for recognition here,' today this Court, which I did not understand to have power to sit as a court of common law, now appears to be exalting a phrase which Warren and Brandeis used in discussing grounds for tort relief, to the level of a constitutional rule which prevents state legislatures from passing any law deemed by this Court to interfere with 'privacy.'" *Id.* Hence, Justice Pollock remarks in *Hennessey*, "Not finding any specific

remarking, "As with defamation law, the common-law right of privacy [was] first adopted, then absorbed by a parallel constitutional right. Courts have transformed the right, which was initially conceived as a means for courts to resolve differences between private parties, into a vehicle to protect individuals from state action."[30] Justice Pollock's observation underscores the ironic transposition of privacy law and its implications in the constitutional sphere. This transposition requires scrutiny here because legislatures and courts consistently regulate the information market by applying constitutional definitions of privacy.[31]

Until around mid-century, courts examining Fourth Amendment issues recognized privacy "rights" as naturally arising within property boundaries.[32] The two-pronged *Katz*

---

textual reference to support the right [to privacy] the United States Supreme Court, in the landmark case of *Griswold v. Connecticut*, placed it in 'a penumbra where privacy is protected from governmental intrusion.'" *Hennessey v. Coastal Eagle Point Oil Co.*, 129 N.J. 81, 110 (1992) (Pollock, J., concurring) (quoting *Griswold v. Connecticut*, 381 U.S. 479, 483 (1965)).

30. 129 N.J. 81, 110 (1992) (Pollock, J., concurring) (referring to Griswold v. Connecticut, 381 U.S. 479, 510 n.1 (1965) (Black, J., dissenting)).

31. *See, e.g.*, The Stored Communications Act, 18 U.S.C. § 2701 (2012). *See also Google*, 988 F. Supp. 2d at 440; *DoubleClick*, 154 F. Supp. 2d 497.

32. *See* Sonia K. Katyal, *Privacy v. Piracy*, 7 YALE J. L. & TECH. 222, 233 (2004–05) (citing Jeremy Waldron, THE RIGHT TO PRIVATE PROPERTY 158 (1988)). "[J]ust as every person enjoys a property right in her person, she enjoys the right to exclude others from treading or trespassing on her privately owned property. By creating a boundary

v. United States test centered on "legitimate" privacy expectations, regardless of any corresponding property interests. *Katz* explored the constitutionality of law enforcement agents' use of an electronic listening device outside a telephone booth to obtain recordings of the calls. The Court dismissed the property analysis, which would have made the agents' actions constitutional, and instead generated an expectations-of-privacy test, which made the agents' actions unconstitutional. The resounding echo of *Katz* is that "the Fourth Amendment protects people, not places."[33] The *Katz* test, so embraced by the courts for almost half a century, was articulated in Justice Harlan's concurring:

> The inquiry . . . normally embraces two discrete questions. The first is whether the individual, by his conduct, has "exhibited an actual (subjective) expectation of privacy,"[34]—whether, in the words of the *Katz* majority, the individual has shown that 'he seeks to preserve [something] as private.'[35] The second question is whether the individual's subjective

---

between private and public ownership, the law permits an owner, by virtue of the right of exclusion, to confer a certain level of privacy on those objects." *Id.* at 235.

33. *Katz*, 389 U.S. at 351–53.

34. *Smith*, 442 U.S. at 740 (quoting *Katz*, 389 U.S. at 361).

35. *Id.* at 740 (quoting *Katz*, 389 U.S. at 351) (Harlan, J., concurring)).

> expectation of privacy is "one that society is prepared to recognize as 'reasonable,' " . . . whether, in the words of the *Katz* majority, the individual's expectation, viewed objectively, is "justifiable" under the circumstances.[36]

The test created an avenue for official application of the third-party doctrine about ten years later in *United States v. Miller*[37] and *Smith v Maryland*.[38]

Under the third-party doctrine, "[I]ndividuals who convey information to third parties have 'assumed the risk' of disclosure to the government."[39] The doctrine had been applied in various contexts long before *United States v. Miller*, but the *Miller* Court really sharpened its edges by imposing assumption of risk on individuals even when they disclose information they expect would be used only to

---

[36]. *Id.*

[37]. 425 U.S. 435 (1976).

[38]. 442 U.S. 735 (1976) (holding that even if a person does entertain a subjective "expectation of privacy in the phone numbers he dial[s], . . . [such an] expectation [is] not legitimate.") Under the majority's reasoning, "[t]he installation and use of a pen register . . . was not a 'search,' and no warrant was required." *Id.* at 745–46.

[39]. *Smith*, 442 U.S.at 749 (Marshall, J., dissenting). Justice Marshall laments the majority's holding as it turns a man's freedom to communicate and express himself to others against him, ultimately inhibiting free expression. *See id.*

conduct their personal business with the third party.[40] *Smith* outlined how the defendant's privacy expectation in telephone numbers he dialed was diminished since the information was, as a by-product of his using the telephone service, shared with the "third-party" telephone company. Though the Supreme Court initially invoked the third-party doctrine as a means to excuse certain governmental surveillance and collection of personal information from general Fourth Amendment requisites, the doctrine now curls its long tendrils into every aspect of commercial activity.[41]

---

[40]. *See Miller*, 425 U.S. at 443 (citing *United States v. White*, 401 U.S. 745, 752 (1971). *Cf. Reporter's Committee*, 489 U.S. at 767 (noting, "[O]ur cases have also recognized the privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public.").

[41]. *See, e.g.*, *Berger v. New York*, 388 U.S. 41, 113 (1967) (White, J., dissenting) (noting, "Unregulated use of electronic surveillance devices by law enforcement officials *and by private parties* poses a grave threat to the privacy and security of our citizens."). Earlier in his dissenting opinion, Justice White implies that he perceives conversations to constitute searchable, seizable private property: "Petitioner suggests that . . . the eavesdropper will overhear conversations which do not relate to criminal activity. But the same is true of almost *all searches of private property* which the Fourth Amendment permits." *Id.* at 108 (emphasis added). His observation is significant because it conveys the assumption—radical at the time—that oral words qualify as property. Elsewhere in his dissent, White remarks, "[I]ndividual searches of private property through surreptitious eavesdropping . . . must be carefully circumscribed to avoid excessive invasion of privacy and security." *Id.* This assumption directly contradicts Justice Black's position that, "by substituting the word 'privacy' for the language of the first clause of the [Fourth] Amendment,

The framework linking expectations of privacy with the third-party doctrine renders the Fourth Amendment obsolete in a world functioning mostly through intangible representations of reality. The fact that a digital representation of the subject, any subject, exists suggests that anything people do, anything they experience, anywhere they go, and anything they possess that has been digitally memorialized somewhere is—inherently—"shared." If everything that is our person is represented by the identity we project along the "virtual highway," then under the privacy rubric, the Fourth Amendment offers no protection from government surveillance in the information age.[42] The government can buy information from private eyes—or data brokers just trying to earn a buck—just as easily as marketing agents can.

---

the Court [has re-written and] expand[ed] the scope of the Amendment to include oral conversations." *Berger*, 388 U.S. at 86 (Black, J., dissenting). Fortunately, the Court integrated the content of intangible communications into Fourth Amendment domain. However, Justice Black's scrutiny of the Court's irreverent substitution of intact Fourth Amendment language with "privacy" highlights the unraveling of common law privacy.

42. *See e.g.*, *United States v. Dennis*, No. 3:13-cr-10-TCB, 2014 WL 1908734, at *10 (N.D. Ga. May 12, 2014). "An internet subscriber does not have a reasonable expectation of privacy in his IP address or the information he provides to his Internet Service Provider, such as Comcast, in order to legally establish an internet connection." *Id.* (quoting *United States v. Stanley*, Criminal No. 11-272, 2012 WL 5512987, at *12 (W.D.Pa. Nov. 14, 2012)) (internal quotation marks omitted).

1. CONSTITUTIONAL ECHOES

The *Katz* inquiry probably constitutes the underpinnings of nearly every judicial endorsement of privacy-related mischief that has passed through the courts since *Katz* was decided.[43] In determining Google's rights' to collect the plaintiffs' internet search history, Delaware District Court Judge Robinson cited a *Katz*-centric Fourth Amendment holding by a New York district court that declared "No expectation of privacy exists for . . . online transactional information, such as a user's Internet search history."[44]

When the Court considered business records in *Smith* and *Miller*, it neglected to predict whether, one day, such records would reflect people's whereabouts at any given moment in time. Today, in the course of conducting their business, cellular service companies keep records of the

---

[43]. Justice Blackmun explains in *Smith*, "In determining whether a particular form of government-initiated electronic surveillance is a 'search' within the meaning of the Fourth Amendment, our lodestar is *Katz v. United States*." 442 U.S. at 735. *See also United States v. Davis*, 785 F.3d 498, 507 (2015) (holding that, under the *Katz* test and its associated principles, the government's obtaining access to MetroPCS's records did not constitute a search within the meaning of the Fourth Amendment).

[44]. *Google*, 988 F. Supp. 2d at 444 (citing *United States v. Polizzi*, 549 F. Supp. 2d 308, 393 (E.D.N.Y. 2008). *But see Riley*, 134 S. Ct. at 2490 (where Chief Justice Roberts acknowledged a contrary position in a 2014 opinion that was heavily steeped in *Katz*losophy: "An Internet search and browsing history . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

information consumers generate both intentionally and by default just by using cellular service. Cellular technology generates location information as a by-product of its operation.[45]

> [W]hen a cellular phone user makes a call, the user's cell phone sends a signal to a nearby cell tower, which is typically . . . the closer tower to the phone. . . . [A] cell tower would generally have a coverage radius of about one to one-and-a-half miles and . . . an individual cell phone user could "be anywhere" in the specified sector of a given cell tower's range.[46]

Consumers wanting to conduct their affairs and maintain their "persons, houses, papers, and effects" in time with current social, political, and economic forces have few, if any, "realistic alternative[s]"[47] to contracting with cellular service providers. Moreover, to keep pace with the rest of the world, people carry their cell phones with them everywhere they go.[48]

---

45. *See Davis*, 785 F.3d at 503.

46. *Id.* (referring to witness testimony by a custodian of records from MetroPCS).

47. *Smith*, 442 U.S. at 750 (Marshall, J., dissenting) (internal citations omitted).

48. As one journalist recently observed,
> [T]he vast majority of us move around each day with a live transmitter in our pocket that constantly pings cell towers without our knowledge. In my

Last year, the Eleventh Circuit examined whether "the Fourth Amendment precludes the government from obtaining a third-party company's business records showing historical cell tower location information . . . without a search warrant issued to that third party."[49] The panel opinion, deviating from decisions in the Third and Fifth

---

> commute to my office each day, an approximately 20 mile journey, I likely transverse multiple cell tower coverage areas. I certainly do no [sic] know where they start and stop, nor do I always use my mobile phone during that commute. . . . Without my knowing it, my device is communicating with cell towers in order to receive those notifications. I am hardly disclosing my personal whereabouts voluntarily to my service provider in order to make that happen. Simply put, we do not knowingly turn over data to mobile telephone companies in the same way as was contemplated in *Smith*, where the defendant made the conscious decision to dial a phone number and a primitive investigative tool captured that volitional conduct.

Matthew S. Adams, *The Great Cell Phone Tower Data Debate Bound to Hit SCOTUS' Docket Soon – Are We Living in George Orwell's 1984?*, THE E-DISCOVERY STAGE (Jan. 2, 2015), http://ediscoverystage.foxrothschild.com/2015/01/articles/metadata/the-great-cell-phone-location-data-debate/.

[49]. *Davis*, 785 F.3d at 505.

Circuits, resounded in the affirmative.[50] Upon rehearing, however, the en banc court—in a split decision in which three judges concurred and two dissented—took the safe route, clinging tightly to *Katz* and its progeny. Judge Hull, writing for the majority, held that court orders "compelling the production of a third-party telephone company's business records containing historical cell tower information" do not violate an individual's Fourth Amendment rights.[51] Since the records were created by a third party; Davis neither owned nor possessed them; and they "d[id] not contain private communications of the subscriber,"[52] he had no subjective or objective reasonable expectation of privacy in them (and thus no legally-cognizable interest in their protection).[53]

2. CONSTITUTIONAL MIRRORS: THE STATUTES

Beginning in 1986, as the intangible realm started coming into focus, Congress passed the Stored Communications Act and the Communications Assistance for Law Enforcement Act—its name says it all—of 1994, to "fill constitutional gap[s] by protecting against unauthorized access to electronic communications in third-party hands,

---

50. *United States v. Davis*, 754 F.3d 1205 (11th Cir. 2014), *reh'g en banc granted, opinion vacated*.

51. *Davis*, 785 F.3d at 500.

52. *Id.* at 512.

53. *Id.*

e.g., internet service providers."[54] Accordingly, the Ninth Circuit asserted, "The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address."[55] Like prevailing Fourth Amendment models, the laws focus more on individual privacy than on property.[56] These statutes generally withdraw protection if one of the parties having

---

[54]. *Google*, 988 F. Supp. 2d at 445. *See also Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900 (9th Cir. 2008) (declaring, "The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.").

[55]. *Quon*, 529 F.3at 900 (emphasis added) (citing 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, 1209–13 (2004)). "The SCA prevents 'providers' of communication services from divulging private communications to certain entities and individuals." Kerr, *supra*, at 1213.

[56]. *See e.g.*, *Crispin v. Christian Aldigier, Inc.*, 717 F. Supp. 2d 965, 971 (C.D. Cal. 2010). The SCA "creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users' private information." *Id.* at 972 (quoting Orin S. Kerr, *supra* note 55, at 1212 (internal quotation marks omitted)). "First, the statute limits the government's right to compel providers to disclose information in their possession about their customers and subscribers." *Id.* (citing 18 U.S.C. § 2703 (2012)). "Although the Fourth Amendment may require no more than a subpoena to obtain e-mails, the statute confers greater privacy protection." *Id.* (quoting *Kerr, supra,* note 55, at 1212–13) (internal quotation marks omitted). "Second, the statute limits the right of an Internet Service Provider ("ISP") to disclose information about customers and subscribers to the government voluntarily." *Id.* (citing 18 U.S.C. § 2702 (2012)).

the information (most frequently, some "third party" internet service provider) has promoted, consented to, acquiesced in, or even itself engaged in, the "hijacking." A Washington district court recently reiterated that

> "the sort of trespasses to which the Stored Communications Act applies are those in which the trespasser gains access to information to which he is not entitled to see, not those in which the trespasser uses the information in an unauthorized way."
>
> . . .
>
> [T]hough Plaintiff frequently invokes the specter of Microsoft tracking users and crowd-sourcing location data, the subsequent uses (or misuses) of any data are not relevant considerations under this provision, which is concerned solely with unauthorized access.[57]

The "highjacking" this paper refers to, then, actually alludes to the trespass (usually lawful, under the SCA) that enables the under-regulated appropriation and conversion of information by the party obtaining the information.

---

[57]. *Cousineau v. Microsoft Corp.*, 6 F. Supp 3d 1167, 1171–72 (W.D. Wash. 2014) (quoting *Educational Testing Serv. v. Stanley H. Kaplan Educ. Ctr.*, 965 F. Supp. 731, 740 (D. Md. 1997)).

3. MISAPPLYING FOURTH AMENDMENT (MIS)JURISPRUDENCE

DoubleClick illustrates how the contours of the third-party doctrine as applied in *Miller* emerge in modern statutory commercial law.[58] Because DoubleClick only collected "information concerning users' activities on *DoubleClick-affiliated Web sites*,"[59] the company's surveillance of the individual users' activities was lawful. One of the "parties," the website, had consented to the surveillance. The court analyzed the case under the SCA.[60] The statute "imposes liability on a person who 'intentionally intercepts' and discloses the 'contents' of an 'electronic communication' . . . *unless* 'such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception.'"[61] Furthermore, it contains an exception to the act's general prohibition: "Subsection (a) of this section does not apply with respect to conduct authorized... (2) by a user of that [wire or electronic

---

58. *See* 154 F. Supp. 2d 497 (S.D.N.Y. 2001).

59. *DoubleClick*, 154 F. Supp. 2d at 504.

60. *Id.* at 507.

61. *Google*, 988 F. Supp. 2d at 445 (quoting 18 U.S.C. § 2511 (2012)). "Since the Wiretap Act concerns the unauthorized interception of electronic communication, the consent of one party is a complete defense to a Wiretap Act claim." *In re Yahoo Mail Litig*., 7 F. Supp. 3d 1016, 1026 (2014) (citing *Murray v. Fin. Visions, Inc*., CV–07–2578–PHX–JM, 2008 WL 4850328, at *4 (D.Ariz. Nov. 7, 2008)).

communications] service with respect to a communication of or intended for that user."[62]

Defining both human individuals as well as websites as users under the Act,[63] District Court Judge Buchwald wrote, "Examining DoubleClick's technological and commercial relationships with its affiliated Web sites, we find it implausible to infer that the Web sites have not authorized DoubleClick's access. . . . [T]he very reason client [websites] hire DoubleClick is to target advertisements based on users' demographic profiles."[64] Thus, the *DoubleClick* plaintiffs came up empty-handed when they sued under the SCA, common law invasion of property, and common law trespass to property. Neither could the plaintiffs find retribution in the Computer Fraud and Abuse Act ("CFAA"),[65] which punishes "(a)-whoever. . . (2)(c) intentionally accesses a computer without authorization, or exceeds authorized access, and thereby obtains . . .

---

62. *DoubleClick*, 154 F. Supp. 2d at 507.

63. *Id.* at 509. *But see iPhone*, 844 F. Supp. 2d at 1058 (citing *Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001) (rejecting plaintiffs' argument that under the SCA, personal computers are "facilities through which an electronic communication service is provided" for the very reason that such an assumption would mean that web sites are users of the communication service, and "any communication between the individual computer and the web site is a communication 'of or intended for' that web site, triggering the § 2701(c)(2) exception for authorized access"). *Id.*

64. *DoubleClick*, 154 F. Supp. 2d at 510.

65. 18 U.S.C. § 1030.

information from any protected computer if the conduct involved an interstate or foreign communication."[66] The latter statute requires a $5000 damages threshold, which the plaintiffs did not plead.

Considering that the SCA reflects Fourth Amendment definitions of privacy, plaintiffs complaining of commercial entities' improper interference with their personal information will find themselves circling endlessly through an unsatisfying maze of third-party doctrine. While people might intuit that a violation of their "selves" has occurred, the law perceives no right of privacy in the personal information gathered, engineered, and reproduced by other entities to create their commodified "selves." If the SCA was, indeed, "enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address,"[67] then Congress missed the mark. The statute inappropriately dresses *Katz*-centric concepts in new clothes, emphasizing non-pertinent issues (like "the computer" representing some phenomenal new medium that requires its own fitting of third-party doctrine) at the expense of critical considerations that actually entail a theoretical overhaul in the law. Congress's modern solution starkly ignores how the commodification of information creates new property interests; it fails—miserably—to consider how the permeability of information

---

66. *Id.*

67. *Quon*, 529 F.3d at 900 (emphasis added) (citing Kerr, *supra* note 55, at 1209–13. "The SCA prevents 'providers' of communication services from divulging private communications to certain entities and individuals." Kerr, *supra* note 55, at 1213.

necessitates evolution in the principles defining privacy interests. Privacy interests in personal information are, as privacy interests have always been, nearly inextricable from their identification with the property interests that used to protect them.

Under Congress's regime, individuals' privacy interests lie defenseless under the tired—and confused—old third-party doctrine. *DoubleClick* demonstrates how Congress perpetuates the cycle of non-protection by premising its legislation on idiosyncratic designs aimed to protect against state action (not that they do) and ignoring the manipulation such legislation promotes among private entities. Moreover, the SCA actually uses the Court's theories regarding privacy to promote state action by enabling a free-for-all whenever the two-faced "user" doing business with the unwitting consumer "consents" to state access.[68]

---

[68]. *See United States v. Ackerman*, 2014 U.S. Dist. LEXIS 89243, *10, *12 (D. Kan. 2014) (quoting *United States v. Benoit*, 713 F.3d 1, 9 (10th Cir. 2013) (stating, "The Fourth Amendment is 'wholly inapplicable to a search or seizure, even an unreasonable one, effected by a private individual not acting as an agent of the Government or with the participation or knowledge of any governmental official.'"). Fourth Amendment privacy constructions and the SCA neatly withdraw protection of personal information once a person has granted initial access to the information to another entity. From a property perspective, the information is now the property of the party who accessed it for its own use (with the subject's consent), and he can do whatever he wants with it. As *Miller* and *Smith* demonstrate, this careful renunciation of protection by the courts dissolves privacy interests by enabling a property right in the collected information.

B. COMMON LAW PRIVACY AND TORT LAW: THE RIGHT TO DISSEMINATE

On *Inside Man*, Spurlock explains that companies' right to share our information and internet activity is embedded in the service agreements we agree to "every time [we] buy or sign up for something," and each time we check the box indicating our agreement to the site's terms—usually the only way to move to the next page on a website site—we opt in.[69] "Every time [we] visit a website, put an item in [our] shopping cart, or like a friend's status, data aggregators are collecting that information. They send it out to marketing companies who bid against each other to show [us] a targeted ad."[70] Ramdam tells Spurlock that data brokerage companies, called "lifestyle companies," start gathering information on us when "[our] mother[s] are pregnant with [us]. They buy every single motor vehicle registration . . . every voter registration . . . property record."[71] They even collect the names of "every book [we] buy [and] every movie [we] watch."[72]

No doubt, prudent consumers weigh their interests (like time and privacy) each time they face a service agreement. After weighing their interests, they decide that whatever piece of information they are giving up in that

---

69. *Spurlock, supra* note 1.

70. *Id.*

71. *Id.*

72. *Id.*

transaction, whether a book title, search query, or cosmetic purchase, won't be missed. What any person can guess about another's identity based on a single purchase amounts to nothing more than a guess. However, that piece of information represents one dot in a "gigantic trove of data,"[73] holding—for each piece of information we knowingly, willingly give up—"five other things that [we] didn't know . . . [we] gave up."[74] Data collectors compile our clicks, our purchases, our likes, and our registrations; they synthesize and interpret them. Their work product then becomes a valuable commodity they own and lawfully possess the right to trade.

1. DEFINITIONS OF PRIVACY

In *Reporter's Committee*, Justice Stevens meanders from Fourth Amendment bases of privacy in a deliberate and focused discussion of common law privacy. His clear delineation of common law standards implies two important points. First, theoretically, the common law recognizes and protects a broader range of personal information than the Fourth Amendment protects.

> To begin with, both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person. In an organized society, there are few facts that are not at one

---

[73]. Heath, *supra* note 6.

[74]. *Id.*

> time or another divulged to another. Thus the extent of the protection accorded a privacy right at common law rested in part on the degree of dissemination of the allegedly private fact and the extent to which the passage of time rendered it private. According to Webster's initial definition, information may be classified as "private" if it is "intended for or restricted to the use of a particular person or group or class of persons: not freely available to the public."[75]

Second, while the Fourth Amendment might allow government access to certain kinds of information, common law rules of privacy steer the government's disclosure of whatever information it gathers. Justice Stevens carefully adds in a footnote, however, that "[t]he question of the statutory meaning of privacy under the FOIA is, of course, not the same as the question whether a tort action might lie for invasion of privacy."[76] Therefore, though the Court refuses to compel the FBI to share its compilation of criminal histories under the Freedom of Information Act (because to do so would invade citizens' privacy), the Court declines to pronounce whether a tort would lie over such sharing. However, the fact that the Court makes its findings based on common law tort theory indicates that plaintiffs suing under the same theory have strong support for their position that

---

75. *Id.*

76. *Id.* at 762n.2.

commercial distribution of their personal information constitutes an invasion of their privacy.

The stark absence of third-party doctrine in Justice Steven's discussion of privacy definitions in *Reporter's Committee* [77] implies the Court's deliberate attempt to maintain a distinction between common law privacy and whatever type of privacy the Court perceives is inherently protected by the Fourth Amendment. The Court's compulsory use of the chameleonic balancing test reinforces the notion that privacy is an abstraction, incapable of precise definition or boundaries and measurable only in relative increments.[78] The substantive content at issue in the case—compiled records of "sensitive" information about private citizens—the sensitivity of which Justice Stevens emphasizes throughout the opinion, should not distract from the fact that the Court enforces protection of these records from public access in the name of "personal privacy" as the common law defines it.

2. COMPILATIONS LEAD TO GREATER INVASION

On *Inside Man*, Morgan Spurlock warns, "Your data starts out as just a bunch of ones and zeroes, and shouldn't . . . be traced back to you, but the more it's collected and

---

77. *See Reporter's Committee*, 489 U.S. at 763–64.

78. *See id.* at 762. "Exemption 7(C) requires us to balance the privacy interest in maintaining, as the Government puts it, the "practical obscurity" of the rap sheets against the public interest in their release." (citing 5 U.S.C.S. § 552(b)(7)(C)).

collated, the easier it is for someone with the right tools to put it all back together."[79] Similarly, Justice Stevens characterizes the information at issue in *Reporter's Committee* as sensitive *because it has been aggregated*. Justice Stevens moreover references the Court's thinking in *Whalen v. Roe*[80] that "the State of New York may record, in a centralized computer file, the names and addresses of all persons who have obtained, pursuant to a doctor's prescription, certain drugs for which there is both a lawful and an unlawful market" because "the Federal Constitution does not prohibit such a compilation."[81] However, Justice Stevens remarks, "we recognize[] that such a centralized computer file pose[s] a "threat to privacy."[82]

This remark is notable because *Reporter's Committee* implicated the Freedom of Information Act; it had nothing to do with the Fourth Amendment. Justice Stevens's focus on traditional privacy definitions highlights the philosophical irony arising in cases that do implicate issues of government trespass and taking. In Fourth Amendment cases, the Court conjures definitions of privacy that are diametrically opposite to traditional common law (and Webster's)[83]; the

---

79. *Spurlock, supra* note 1. *See also* Heath, *supra* note 6 (noting that "[r]elatively minor pieces of information, added together, become greater than the sums of their parts").

80. 429 U.S. 589 (1977).

81. *Whalen v. Roe*, 429 U.S. 589, 591 (1977).

82. *Id.*

83. The contrast in the Court's allowances of privacy different contexts can be illustrated by comparing *Miller*, 425 U.S. at 443,

Court's choices in this regard promote, rather than challenge, law enforcement agencies' access to personal information about private citizens. This relationship indicates the delusion—apparently held by both Congress and the Supreme Court of the United States, that Americans can rest secure: the government can access (and keeps careful records of) our secrets, but it will keep those secrets safe so we can maintain our reputations within our communities.

Under the balancing test promulgated in *Reporter's Committee*, some situations might prompt courts to enforce disclosure of governmental records where "the public interest" in such disclosure outweighs "personal privacy." *Reporter's Committee* might be "quaint" because Americans today have few expectations of privacy in compiled rap sheets; its foreboding arises from the practically limitless range of "personal information" precariously "kept" by

---

in which the Court states "This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed 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," with *Reporter's Committee*, 489 U.S. at 767, where Justice Stevens notes, "[O]ur cases have also recognized the privacy interest inherent in the nondisclosure of certain information even where the information may have been at one time public." While public information is not exactly analogous to information "revealed on the assumption that it will be used only for a limited purpose," the deviation only further underscores the radical difference in what the Court deems to be a legitimate expectation of privacy.

government officials, who might be compelled to disclose that information in the public interest.

If not for *Katz*, the "lodestar,"[84] the government would have little access (without due process) to people's personal information. If not for the shapeshifting conception of privacy espoused in *Katz*, *Miller*, and *Smith*, the SCA might afford consumers some property rights against intangible trespass. Now they stand defenseless against their merchants, who clear paths into consumers' lives with boilerplate consent agreements and cookies and then sell their findings to information brokers. However, a closer inspection suggests that *Reporter's Committee*—unlike numerous district court holdings discussed in this paper—justifies an appropriation action for the unauthorized sale of commodified personal data *because* the data is bound for compilation and systematization. If the sale of the "ones and zeros" alone cannot give rise to such an action, then the sale of the compilation itself should give rise to the action.

---

[84]. Justice Blackmun explains in *Smith*, "In determining whether a particular form of government-initiated electronic surveillance is a 'search' within the meaning of the Fourth Amendment, our lodestar is *Katz v. United States*." 442 U.S. at 735. *See also Davis*, 785 F.3d at 507 (holding that the government's obtaining access to MetroPCS's records did not constitute a search within the meaning of the Fourth Amendment).

C. PRIVACY, IDENTITY, AND AUTONOMY

The distinction between identity as a product of creation—built through the gathering and aggregation of various pieces of information about an individual—and identity as an ever-in-flux, incidentally-manifested by-product of living, is as subtle and difficult to pin down as the distinction between energy and subatomic matter (where bits of matter are so tiny and moving so fast, they are virtually indistinguishable from the energy that creates them). Information belongs to no one until someone decides to detach from the experience that creates it and begin collecting, arranging, and bottling and labeling it for trade. The law enables a property right to information *in the entity that converts the information*, though it backs into the enabling by denying that an expectation of privacy can exist shared information. Since personal information is not protected by privacy law, it should qualify as converted the moment it is generated and used (by some entity other than the subject whom it concerns) for any purpose other than identification.

The property-privacy conundrum manifests in the gray area where experience becomes recorded and begs the question: to whom does the experience then belong? Surely, the law must recognize that once a person becomes bound by his every movement, action, and thought, his liberty of person is at stake. Legal scholar and professor Paul Schwartz appropriately tethers the myriad platitudes referencing Orwell's *1984* to this discrete concept, quoting from the novel, "There was of course no way of knowing whether you were being watched at any given moment. . . . You had

to live—and did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every moment scrutinized."[85]

The position advanced in this paper relies on two assumptions, the most critical being that individual autonomy is the basic unifying policy of our nation. This policy manifests in the organizational structure of our social, political, and economic systems and functionally informs our legal tradition.[86] The second assumption is that honoring individual autonomy is a central goal of our legal system.[87]

---

[85]. *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2073 (2004) (quoting George Orwell, *1984* 6–7 (1949)).

[86]. *See, e.g., Obergefell v. Hodges*, 135 S. Ct. 2584, 2635 (2015) (Thomas, J., dissenting). Justice Thomas quotes from a 1756 editorial in the *Boston Gazette* to show how John Locke's philosophies on civil liberty "permeated the 18th-century political scene in America: "'Liberty in the State of Nature' was the 'inherent natural Right' 'of each Man' ' to make a free Use of his Reason and Understanding, and to chuse that Action which he thinks he can give the best Account of,' but that, 'in Society, every Man parts with a Small Share of his natural Liberty, . . . that he may possess the Remainder without Controul.'" (quoting *Boston Gazette and Country Journal*, No. 58, May 10, 1756, p. 1). Justice Thomas further discusses the likely meaning of "civil liberty" from the founding fathers' perspective. "When the colonists described laws that would infringe their liberties, they discussed laws that would prohibit individuals 'from walking in the streets and highways on certain saints days, or from being abroad after a certain time in the evening, or restrain [them] from working up and manufacturing materials of [their] own growth.'" *Id.* (quoting Downer, *A Discourse at the Dedication of the Tree of Liberty*, in 1 C. Hyneman & D. Lutz, *American Political Writing During the Founding Era 1760-1805* 101 (1983). In this case, Justice Thomas, joined by Justice Scalia, emphasizes throughout his lament that, as used in the Due Process clauses, "liberty most likely refers to the power of locomotion, of

1. THE RIGHT TO BE LET ALONE

The threat of personal injury imposed by the information market extends beyond the superficial, defamation-based interferences discussed in Warren and Brandeis's *Right to Privacy* because the modern virtual persona constitutes a utilitarian duplicate of the physical person. In *Stanley v. Georgia*, the Court observed,

---

changing situation, or removing one's person to whatsoever place one's own inclination may direct, without imprisonment or restraint." *Id.* at 2632 (quoting 1 W. Blackstone, COMMENTARIES ON THE LAWS OF ENGLAND 130 (1769). Justices Thomas and Scalia urge that such freedom pertains to the physical person.

[87]. *See Obergefell*, 135 S. Ct. at 2593. (opening with, "The Constitution promises liberty to all within its reach, a liberty that includes certain specific rights that allow persons, within a lawful realm, to define and express their identity." *But see id.* at 2615–16 (Roberts, C.J., dissenting): "[T]he majority's approach has no basis in principle or tradition, except for the unprincipled tradition of judicial policymaking that characterized discredited decisions such as *Lochner v. New York*, 198 U.S. 45." This paper interprets the referenced debate in *Obergefell* to focus *not* on the ideological tradition of autonomy in America, but on whether the Court has the constitutional authority to define and enforce it through the Due Process Clause of the Fourteenth Amendment. This paper relies not on the majority's approach nor reasoning to support the majority's position that the Court is authorized to decide such issues; rather, this paper references the case to illustrate how *one branch of our legal system* incorporates personal autonomy considerations, even from a policy standpoint, to make decisions regarding constitutional law.

> [The defendant] is asserting the right to read or observe what he pleases-the right to satisfy his intellectual and emotional needs in the privacy of his own home.... If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.[88]

Unbridled surveillance by private entities records every movement the virtual persona makes. The fact that the private actor conducting the surveillance has the power to distribute the fruits of his labors however he pleases (including to government officials) does give the government the ability to "control men's minds" because "[t]he use, transfer, or processing of personal data by public and private sector organizations will affect the choices that we make."[89] Without property lines in the virtual world, the fact that a man is sitting alone in his own house affords him little protection from surveillance, investigation, or public scrutiny.

---

88. *Stanley v. Georgia*, 394 U.S. 557, 564–66 (1969).

89. Paul Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2058 (2004).

> [P]roperty and privacy are each grounded in territorial metaphors which construct boundaries that define realms of physical or social immunity from state interference. Property rights confer a certain amount of spatial sovereignty in the property owned,[90] a factor which directly complements the right to be left alone. This is why the Supreme Court, at various points, has emphasized that 'one who owns or lawfully possesses or controls property will in all likelihood have a legitimate expectation of privacy by virtue of this right to exclude.'[91]

Further, our choices create our experience. Just knowing that our movements are tracked restricts our liberty to develop and express our own selves.

Constitutional and common law analyses perpetually approach identity "interference" through the lens of privacy interests under the decisional autonomy prong of the privacy rubric in constitutional law[92] and under tort actions

---

90. Katyal, *supra* note 32, at 235 (citing Sadhika Rao, *Property, Privacy, and the Human Body*, 80 B.U. L. REV. 359, 425 (2000)).

91. *Id.* (quoting *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978)).

92. In 1977, the Court delineated another class of privacy interests, "based upon a substantive concept of personal liberty . . . found in the Fourteenth Amendment," *Shields v. Burger*, 874 F.2d 1201, 1210 (7th Cir. 1989) (citing *Paul v. Davis*, 424 U.S. 693, 713 (1976)), which differs connotatively from the confidentiality interests that have been practically

like appropriation, intrusion on privacy, rights of publicity, and defamation in common law. Despite the substantive distinctions courts make regarding decisional autonomy,[93] the existence of an underlying policy that recognizes a fundamental right to such autonomy denotes the recognition that a person's ability to navigate his own ship, at least with regard to certain decisions,[94] is implicit in the concept of ordered liberty.[95]

---

obliterated by the third-party doctrine. This class represents "the interest in independence in making certain kinds of important decisions."[92]

[93]. *See Shields v. Burger*, 874 F.2d 1201, 1209–10 (7th Cir. 1989) (citing *Paul*, 424 U.S. at 713. Generally, the kinds of "important decisions" that qualify for protected autonomy regard "family-related matters, including marriage, procreation, abortion, contraception, family relationships, and child rearing and education."

[94]. "The focus of decisional privacy is on freedom from interference when one makes certain fundamental decisions . . . [I]nformation privacy is concerned with the use, transfer, and processing of the personal data generated in daily life." *See* Schwartz, *supra* note 88, at 2058.

[95]. *See id.* at 2087. Here, Schwartz notes,

> [P]rivacy is necessary for both "individual self-determination" and "democratic deliberation." Based in part on civic republicanism, this conception views democracy as dependent on common participatory activities, reciprocal respect, and the need for consensus about political issues. To borrow a phrase from Robert Post, the process at stake is the "creation of the

2. MOVEMENT AND AUTONOMY

Granted, whether intangible forces can inhibit liberty of movement is debatable. As Justice Thomas, joined by Justice Scalia, recently lamented in *Obergefell v. Hodges*,[96] the "Court appears to lost its way" in construing the Framers' formulation of the Due Process Clause of the Fourteenth Amendment:

> When read in light of the history of [the] formulation, it is hard to see how the "liberty" protected by the Clause could be interpreted to include anything broader than freedom from physical restraint. That was the consistent usage of the time when "liberty" was paired with "life" and "property." And that usage avoids rendering superfluous those protections for "life" and "property." . . . That the Court appears to have lost its way in . . . recent years does not justify deviating from the original meaning of the Clause[].[97]

> autonomous self required by democratic citizenship." In this conception, deliberative democracy requires limits on access to personal information because Americans will hesitate to engage in democratic self-rule should widespread and secret surveillance become the norm.

96. 135 S. Ct. 2584, 2633 (2015) (Thomas, J., dissenting).

97. *Id.*

Significantly, Justice Thomas stresses that "liberty most likely refers to the power of locomotion, of changing situation, or removing one's person to whatsoever place one's own inclination may direct, without imprisonment or restraint."[98]

The law must regard the identity a person uses online as his "person," deserving the same privileges, protections, and entitlements his physical person deserves. In *Hiibel v. Sixth Judicial Dist. Ct. of Nevada, Humboldt County, et al*,[99] three justices revived the Court's acknowledgement in *Terry v. Ohio*[100] that "the Fourth Amendment protects the 'right of every individual to the possession and control of his own person.'"[101] As one writer observes, "Lockean notions of property in one's person are inextricably linked to the protection of privacy. Because they presuppose the ability to exclude others from bodily invasion, they suggest that protection of bodily privacy also involves a metaphor of ownership."[102] Modern, legal conceptions of identity must regard it as a product, an autonomous "agent," really, of the

---

98. *Id.* at 2632 (quoting 1 W. BLACKSTONE, COMMENTARIES ON THE LAWS OF ENGLAND 130 (1769)).

99. 542 U.S. 177 (2004).

100. 392 U.S. 1 (1968).

101. *Hiibel*, 542 U.S. at 197 (Breyer, Souter, and Ginsberg, JJs., dissenting) (quoting *Terry v. Ohio*, 392 U.S. 1, 9 (1968)).

102. Katyal, *supra* note 32, at 233 (citing Radhika Rao, *Property, Policy, and the Human Body*, 80 B.U. L. REV. 359, 422 (2000)).

physical body, which people build, assimilate, and use very practically to conduct their business.

III. A ROOM OF ONE'S OWN

Before *Katz*, the zone of privacy—within which, pursuant to the Fourth Amendment, an individual is said to be protected from governmental investigative activities[103]—used to have clear and objectively-discernible boundaries represented by the structures of private property. For example, dwellings create privacy by literally shielding individuals from the world.[104] People used to enjoy privacy

---

[103]. *See id.* at 440. "'No interest legitimately protected by the Fourth Amendment' is implicated by governmental investigative activities unless there is an intrusion into a zone of privacy, into 'the security a man relies upon when he places himself or his property within a constitutionally protected area.'" *Id.* (quoting *Hoffa v. United States*, 385 U.S. 293, 301–02 (1966)).

[104]. *See* Katyal, *supra* note 32, at 235 (quoting HANNA ARENDT, THE HUMAN CONDITION (1958)) (observing that

> the four walls of one's private property offer the only reliable hiding place from the common public world, not only from everything that goes on in it but also from its very publicity, from being seen and being heard. A life spent entirely in public, in the presence of others, becomes, as we would say, shallow. While it retains visibility, it loses the quality of rising into sight from some darker ground which must remain

within such zones because there was no "eye in the sky" that literally created records reflecting every movement they made.

Under *Katz*, people today have to ditch a whole lot of property, including their credit and debit cards, their phones, their computers, and even their cars, before they can rest safely within some conceptual realm resembling a zone of privacy, even when that "zone" is their dwelling.

A. INTANGIBLE PROPERTY

The labor theory of value, as posited by Adam Smith, defines "[t]he real price of every thing . . . [as] the toil and trouble of acquiring it. What everything is really worth to the man who has acquired it."[105] Hence, the Court in *Reporter's Committee* could, perhaps, in 1989, conceive of the government's framing a limitation like "practical obscurity" to the exploitation of personal information. Though Justice Stevens framed the issue through the language of privacy, the compilation of information the reporter sought in the case did represent property, property of the FBI.

---

hidden if it is not to lose its depth in a very real, non-subjective sense.).

[105]. ADAM SMITH, WEALTH OF NATIONS Book 1, chapter V (1776).

1. INTERNATIONAL NEWS SERVICE V. ASSOCIATED PRESS

Since at least as early as 1918, the Court has recognized an intangible property right in business enterprises related to the collection, organization, and dissemination of information. For purposes of this argument, property is defined by its capacity for "exclusion by law from interference."[106] The tension between Justice Pitney's 1918 majority opinion and Justice Holmes's dissenting opinion in *International News Service v. Associated Press*[107] forecasts the difficulties bound to arise when present-day courts try to apply industrial-age rationale to problems emerging in an era where personal information is the hottest commodity on the market. Justice Pitney wrote, "[N]ews matter, *however little susceptible of ownership or dominion in the absolute sense*, is stock in trade, to be gathered at the cost of enterprise, organization, skill, labor, and money, and to be distributed and sold to those who will pay money for it."[108]

Justice Holmes—observing that shared information is always susceptible to interference—countered that "[p]roperty, a creation of law, *does not arise from value*, although exchangeable. . . . Property depends upon exclusion by law from interference."[109] The majority's

---

106. *International News Service v. Associated Press*, 248 U.S. 215, 246 (1918) Holmes, J., dissenting).

107. 248 U.S. 215, 236 (1918).

108. *International News*, 248 U.S. at 236.

109. *Id*. at 246 (Holmes, J., dissenting).

reasoning specifically implied, however, that the property interest at issue in *International News* encompassed more than information; the business enterprise itself constituted the property with which the defendant had no right to interfere.[110] "The process [by which the defendant profited from the plaintiff's work] amounts to an unauthorized interference with the normal operation of complainant's legitimate business precisely at the point where the profit is to be reaped."[111] Justice Pitney's statements do not contradict Justice Holmes's perspective that exclusion from interference—rather than value—defines property interests, but his emphasis on the profit-bearing enterprise suggests that some economic value is necessarily implicated in the intangible-property rights analysis.

2. APPLYING THE BUSINESS ENTERPRISE MODEL

Nearly seventy years after *International News*, Justice White, writing for an unanimous Court in *Carpenter v. United States*,[112] added to *International News's* business enterprise model by holding that "[a newspaper's] interest in the *confidentiality* of the contents and *timing* of [its] . . . column [was] a property right."[113] Here, the Court examined

---

110. *See International News*, 248 U.S. at 240 (1918).

111. *Id.*

112. 484 U.S. 19 (1987).

113 *Carpenter v. United States*, 484 U.S. 19, 26 (1987) (internal citations and quotations omitted) (italics added for emphasis).

whether the writer of an influential stocks and bonds column, who conspiratorially leaked the contents of next day's column to turn a quick profit, committed statutory fraud against the paper. Carpenter contended his activities landed outside the statutory restrictions because "the newspaper [was] the only alleged victim of fraud and ha[d] no interest in the securities traded."[114] Echoing Pitney's and Holmes's discourse in *International News*, Justice White explained that property deprivation doesn't necessarily equate to monetary loss; the property interest Carpenter wiled the newspaper out of was exclusivity.[115]

Justice Pitney distinguished in *International News* between authorized and unauthorized use of information; the defendant's use of the information *for profit* constituted the unauthorized interference with the complainant's business enterprise. The business enterprise model serves few people demanding legal rights to their personal information today; unless someone is a celebrity or person of public interest, his personal information lacks economic value in his own "hands," and it thus has little legal

---

114. *Id.* at 25.

115. *See id.* at 26–27. *Cf. United States v. Sadler*, 750 F.3d 585, 591 (2014) (noting that *Carpenter* "stopped [the] expanding universe of intangible-right protections, limiting the fraud statutes' scope to rights that sounded in property"). This opinion implies that property must have some sort of pecuniary value to be protected by the fraud statute. Juxtaposed with *Sadler*, *Carpenter* could be read to suggest that the *confidentiality* and *timing* of the column, as well as "confidential business information," *see Carpenter*, 484 U.S. at 26, due to its relationship to the business enterprise, actually does have monetary value (as it represents an income-generating asset).

protection as a form of property.[116] The Second Circuit has acknowledged that under New York law, "an action for conversion will not normally lie over intangible property."[117] Under the exception to this rule, "documents that embody an intangible right, like stock certificates . . . may be the subject of conversion."[118] Case law involving the right of publicity,[119] appropriation,[120] and fraud[121] also reveals this premise.

---

[116]. *See McNally v. United States*, 483 U.S. 350 (1987). Here, the Court emphasizes the protection of property rights over other intangible rights and, according to Justice Ginsburg, lays to rest prosecutions against defrauders who "deprived victims of 'intangible rights' unrelated to money or property." The Court moreover emphasizes a distinction between intangible "interests" that may have been protected by the mail fraud statute before *McNally* and those that Congress aimed to protect when *McNally* had appeared to preclude protection of intangible, non-economic interests.

[117]. *Thyroff v. Nationwide Mutual Insurance Co.*, 460 F.3d 400, 405 (2d Cir. 2006).

[118]. *Id.*

[119]. *See, e.g.*, *Haelan Labs. v. Topps Chewing Gum, Inc.*, 202 F.2d 866 (2d Cir. 1953). The *Haelen* court observed, "[I]t is common knowledge that many prominent persons . . . , far from having their feelings bruised through public exposure of their likenesses, would feel sorely deprived if they no longer received money for authorizing [the use of their personae in advertising]." *Id.* at 868. "The right of publicity is limited to situations involving the taking of the 'commercial value' of a person's identity. . . . It is wielded almost exclusively by celebrities as a way to control their right to profit from their fame." Andrew J. McClurg, *A Thousand Words are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 107 (2003). McClurg emphasizes throughout his article that appropriation is a privacy tort and should be analyzed distinctly from the right of publicity. *See id.*

[120]. In *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995), the court "dismissed an appropriation claim, 'finding that the plaintiffs had failed to show an appropriation because a single, random cardholder's name has little or no intrinsic value.' Rather, the value attached to the name derived from the aggregation and analysis of the data conducted by American Express." Ludington, *supra* note 11. *See also* McClurg, *supra* note 118.

> Unfortunately, too many courts . . . have lost sight of the distinction between [appropriation and the right of publicity]. Courts] stew them together in radically under-analyzed opinions that, . . . because almost all the relevant cases are brought by celebrities, exalt the property-based right of publicity interest over the personal privacy interest the appropriation tort was created to protect. The result is that appropriation is being obscured to the point of possible extinction.

Id.

[121]. *See Carpenter*, 484 U.S. 19 (holding that "it is sufficient that the [Wall Street] Journal has been deprived of its right to exclusive use of the [stock trade] information, for exclusivity is an important aspect of confidential business information and most private property"). In reaching its holding, the *Carpenter* Court references *Ruckelshaus v. Monsanto Co.*, 467 U.S. 986, 1001–04, where the Court had observed, "Confidential business information has long been recognized as property." *Id. See also Cleveland v. United States*, 531 U.S. 12, 22 (2000) (holding that the defendant did not violate the federal wire fraud statute when lying on his poker game license application because, even assuming poker game licenses *were* characterized as property in the hands of the state (a position the Court did not support), "the nature of that property [could not] be economic"). Justice Ginsburg writes, "State municipal licenses in general, and Louisiana's video poker licenses in

Virtual "persons . . . papers and effects" cannot be trespassed[122] and stolen in such a way as to deprive a person of his property rights.[123] Hence, courts rarely find the

---

particular, we hold, do not rank as 'property' for purposes of § 1341, in the hands of the official licensor." *Id.* That an object has the capacity to "rank" implies its capacity to represent value. This paper argues that, in the Court's perspective, the value represented by the object's "rank" is its economic value. Once an object has the capacity for economic value, it "ranks" as property.

[122]. *See Dennis*, No. 3:13-cr-10-TCB, 2014 WL 1908734, at *9. ("Because '[t]his investigation involve[d] the transmission of electronic signals without trespass,' it did not 'implicate [the defendant's] Fourth Amendment rights under *Jones*.'") (quoting *United States v. Bashear*, Criminal No. 4:11-CR-0062, 2013 WL 6065326, at *3 (M.D.Pa. Nov. 18, 2013)). *See also* Katyal, *supra* note 32, at 233. "[I]n real space, property rights coupled with architecture serve as a defensive shield to protect privacy. In contrast, . . . the nature of cyberspace couples the relationship between property and privacy, creating a host of challenges for the protection of privacy. Unlike real space, which is reified boundaries between private and public space, boundaries in digital space are largely permeable and transparent, engendering a nearly limitless potential for consumer surveillance." *Id.*

[123]. *See, e.g., United States v. Williams*, 592 F.3d 511, 517– 18 (2010) (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L.REV. 531, 584–85 (2005)):

> For most of its first two centuries, the Fourth Amendment was used almost exclusively to regulate government searches of homes and containers. The mechanisms of home and container searches directed Fourth Amendment doctrine to focus primarily on the entrance to the home or container. In a

damages required for a plaintiff to have standing[124] and bring action against the alleged thief. However, if the theft of such virtual "persons . . . papers and effects" leads to a loss of property rights in something like money (as when a credit card might be stolen), such damages could be relied on to bring a cause of action for trespass.[125]

> world of physical barriers, actions that broke down those physical barriers became the focus of judicial attention. The world of digital search and seizure shows that this focus is contingent on the architecture of physical searches. As computer searches and seizures become more common in the future, we will begin to see twentieth-century Fourth Amendment doctrine as a contingent set of rules that achieves the foundational goals of the Fourth Amendment law given the dynamics of searching physical property. Those physical rules will be matched by a set of rules for digital searches and seizures that attempts to achieve the same purpose in a very different factual context.

[124]. *See, e.g.*, *DoubleClick*, 154 F. Supp. 2d at 523 (remarking, "The facts . . . illustrate[] the difference between 'loss' and 'damage'—there was no 'damage' to the function of [the computer] system or the data within it, only plaintiff's 'loss' from defendant's trespass."). "Nonetheless, the court required a finding that [the plaintiff's] losses exceeded the '$5,000 statutory threshold requirement' before it granted summary judgment." *Id.* (citing *America Online, Inc. v. LCGM*, 46 F. Supp. 2d 444, 450 (E.D. Va. 1998)).

[125]. *See, e.g.*, *Thyroff*, 460 F.3d at 405 (holding that under New York law, "an action for conversion will not normally lie over intangible

B. DEFINING OWNERSHIP

Oxford's proposal that information, "[c]ontrasted with data[, is] that which is obtained by the processing of data"[126] implies that the existence of information depends on its being produced. The majority in *International News* critiqued the defendant's stance that information not contained "becomes the common possession of all to whom it is accessible; and . . . [anyone who gains knowledge of it] has the right to communicate [it] to anybody and for any purpose, even for the purpose of selling it for profit"[127] by distinguishing among the purposes of the communication. "The right of the purchaser of a single newspaper to spread knowledge of its contents gratuitously, for any legitimate purpose not unreasonably interfering with complainant's right to make merchandise of it, may be admitted; but to transmit that news for commercial use, in competition with

---

property." The exception to the rule, the court recognized, is that "documents that embody an intangible right, like stock certificates . . . may be the subject of conversion"); *Del Vecchio*, No. 11-366, 2012 WL 1997697 (finding "plaintiffs alleged sufficient injury to have standing when they alleged the dissemination and use of personal information belonging to them, including sensitive information about their web browsing and shopping habits, purchases, and related transaction information, combined with their financial information such as credit and debit card information, and their mailing and billing addresses.").

126. *See* OED, *supra* note 8.

127. *International News*, 248 U.S. at 239.

complainant—which is what defendant has done and seeks to justify—is a very different matter." This distinction further suggests that intangible property rights must correspond with the business enterprise model; this paper attempts to extend the business enterprise model by tying an individual's personal information with his ability support his own livelihood. While the individual's use of his own information does not always translate to a commercial enterprise, every commercial enterprise he endeavors to undertake implicates his personal information, and when that information has been tampered with, his commercial undertakings are hindered.

1. THE EXCLUSIVE RIGHT TO PROFIT

Under current judicial constructions, information generally belongs to the individual who "produces" it,[128] so consumers trying to sue information-traders on property grounds have consistently struck out. For example, where iPhone customers sued Apple for conversion of personal information (among other things), District Court Judge Koh complained the plaintiffs "failed to establish that the broad category of information referred to as 'personal information'

---

128. *See* Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 17 (1996). "The consequence of the increased institutional need for information made its possession the determining factor in the right to use the information. With few exceptions, the individual's ability to prevent collection and disclosure of the information ended once the information was in the hands of a third party." *Id.*

is an interest capable of precise definition." [129] In contrast to the observations Justice Stevens presented in *Reporter's Committee*, Judge Koh maintained, "Moreover, it is difficult to see how this broad category of information is capable of exclusive possession or control."[130]

International News indicates, however, that while information may not be capable of exclusive possession, an individual maintains property rights to information by lawfully controlling how the information will be disseminated: "Defendant insists that . . . by issuing [the news] to newspapers and distributing it indiscriminately, complainant no longer has the right to control the use to be made of it. . . . The fault in the reasoning lies in applying as a test the right of the complainant as against the public, instead of considering the rights of complainant and defendant, competitors in business, as between themselves."[131] This statement suggests that the law recognizes exclusive control of information by recognizing the exclusive right to profit commercially by its publication. Thus, the law comprehends that the primary incentive for producing information is profit, so the fact that information is incapable of exclusive possession does not impede its potential to classify as property.

In *Google*, the court dismissed four counts in a class action against Google, where Google had collected users' personally-identifiable information to later trade and sell

---

129. *iPhone*, 844 F. Supp. 2d at 1075.

130. *Id.*

131. *International News*, 248 U.S. at 239–40.

that information. Here, the plaintiffs cited numerous articles supporting their assertion that personal information is a valuable commodity.[132] The court found the plaintiffs lacking Article III standing[133] to bring the case: "[W]hile the plaintiffs . . . offered some evidence that the online personal information . . . has some modicum of identifiable value to [themselves], [they] have not sufficiently alleged that the ability to monetize their [PII] has been diminished or lost by virtue of Google's previous collection of it."[134] Conversely, in *Del Vecchio v. Amazon.com, Inc.*,[135] a district court in Washington found the plaintiffs' allegations of Amazon's "dissemination and use of personal information belonging to [the plaintiffs], including sensitive information about their web browsing and shopping habits, purchases, and related transaction information, combined with their financial information such as credit and debit card information, and their mailing and billing addresses"[136] sufficient for the plaintiffs to have standing.

---

132. *Google*, 988 F. Supp. 2d at 441.

133. *Id* at 440. "Article III standing requires: (1) an injury-in-fact . . . ; (2) a causal connection between the injury and the conduct complained of; and (3) that it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Id.*

134. *Id.*

135. No. 11-366, 2012 WL 1997697 (W.D. Wash. June 1, 2012)

136. *Del Vecchio*, No. 11-366, 2012 WL 1997697 *2).

2. BALANCING PRIVACY AND PROPERTY

The intrinsic problem for property analyses in these cases is that people don't necessarily *want* to publish, produce, or disseminate all the information that is generated about them—even for a profit—so data brokers are not competing in business with the individuals whose information they produce. Plaintiffs cannot, then, rely on *International News* to support their cause. This explains why privacy cases, including *Reporter's Committee*, rely on the balancing test when comparing a plaintiff's "interest" in keeping his information private with a commercial entity's "interest" in publishing the information.[137] Within this framework, for the commercial entity, property equals the market value of the information, but for the individual, property equals privacy. Courts cannot compare apples to oranges, and monetary damages drive civil law, so the plaintiffs lose unless they can put a price on their identity—and not only their identity, but the misrepresentation of their identity. To discourage mass surveillance and information trade, the law must remove the profit incentive, either with punitive damages or criminal fines.

---

[137]. This argument acknowledges that the FBI in *Reporter's Committee* had no commercial interest in disseminating its records of individuals' criminal history records and that privacy, not property, was at issue in that case. However, because the individuals' privacy was implicated, the Court had to use the balancing test, which this paper attempts to elucidate.

IV. CONCLUSION

Privacy laws provide insufficient protection of personal information for two reasons. First, regardless of the Stored Communications Act being introduced as serving to fill constitutional gaps created by the internet, the act ultimately regulates activity by private actors, and it incorporates ill-suited, misguided Fourth Amendment standards to do so. The act focuses on information access and surveillance, and it fails to address the implications arising from third parties' dissemination of the information they access. While the law purports to limit government officials' access to information conveyed to technological service providers, it gives providers broad dominion over whatever information they acquire. Second, common law tort theories rely on measurable damages, and the intangible, abstract nature of the identity lacks a clear formula for quantification. Until the law regards the *identity* as either the person or property of the individual whom it concerns, and as long as the law refuses to protect "shared" information, the public outcry for greater privacy protection will remain futile.

By shifting its focus to the *enterprise* at issue in *International News*, and recognizing that the individual requires autonomy over his identity to conduct the *enterprise* of living and being in the modern world, the law could restrict information appropriation to the extent that it interferes with the individual's necessary use of his own identity.