ST. THOMAS JOURNAL OF COMPLEX LITIGATION

Volume 6 Fall 2019

THE DATA DILEMMA IN THE 21st CENTURY COURT SYSTEM

Lawrence Suarez

THE DATA DILEMMA IN THE 21st CENTURY COURT SYSTEM

Lawrence Suarez*

Technology has made modern life more efficient and convenient for those who have access to it. However, life in the time of Alexa is not without its pitfalls, especially with respect to privacy.[1] Willingly or reluctantly, customers find themselves exposing elements of their lives, which traditionally held a subjective expectation of privacy from third parties.[2] Companies such as Amazon, Google, Facebook, Apple, and countless others, know individuals' bank and credit card information, political views, geographic location and much more, all in real-time.[3] The immense amount of data that companies collect and store poses three problems: (1) the potential for unwarranted government intrusion; (2) the potential for identity theft through data breaches; and (3) the actual use and sale of personal information in a form of uncompensated taking with or without consent.[4]

Technology is the ultimate glass house, and has become an integral and essential part of everyone's daily life. It is unreasonable to think that technology will de-evolve in order to simplify life and mitigate consumers' concerns, or that consumers will have more of a choice whether to engage in some relation with third-party technology companies in the future. While "do not track" lists, similar to "do not call" registries, may provide some respite, customers may not be adequately protected unless Congress or the courts recognize a property right in the data individuals generate.[5] This can be achieved by creating a specialized court within the Court system to address technological matters since today's courts do not normally have the requisite knowledge necessary to adjudicate these complex issues.

Therefore, Part I of this note will explore historical issues of privacy from the government, directly and indirectly. Then, Part II will touch on the relationship between privacy and property, including proposed legislation and political objectives. Part III will proceed to explain how the judicial adjudication of technology issues can be resolved. Finally, Part IV will conclude by stating why privacy rights consisting of personal data generated by individuals should be protected as an

---

* Lawrence Suarez, Juris Doctor Candidate May 2020, St. Thomas University School of Law, ST. THOMAS JOURNAL OF COMPLEX LITIGATION, *Member*. To my wife Jie, the love of my life, and our daughter Katherine, the most beautiful miracle I have ever witnessed. Thank you for your love, support, and encouragement.

[1] *See* Megan Wollerton, Andrew Gebhart, *What is Alexa?,* CNET (June 2, 2019, 4:00 AM), https://www.cnet.com/news/what-is-alexa/.

[2] *See* Melanie De Klerk, *Amazon Ring: Explaining concerns about the smart, controversial doorbell, from privacy to hacking*, GLOBAL NEWS (Mar. 5, 2020, 7:00 AM), https://globalnews.ca/news/6633045/amazon-ring-privacy-security-explained/.

[3] *See* Omer Tene, *Privacy: The New Generations,* 1 INT'L DATA PRIVACY LAW 15 (2011), http://idpl.oxfordjournals.org/content/1/1/15.full.

[4] *See* U.S. CONST., amend. V (stating "nor shall private property be taken for public use, without just compensation[,]" and analogizing that Tech companies are as powerful as the Government in this area, and that the use of personal data is a form of "taking" entitling the individual to just compensation); *see also* Joe Mullin, *How Much Do Google and Facebook Profit from Your Data?*, ARS TECHNICA (Aug. 6, 2019), http://arstechnica.com/tech-policy/2012/10/how-much-do-google-and-facebook-profit-from-your-data (analogizing that technology companies are as powerful as the Government in this area and the use of data is a form of "taking," entitling the individual to just compensation).

[5] *See FTC Testifies on Do Not Track Legislation*, FEDERAL TRADE COMMISSION (Dec. 2, 2010), https://www.ftc.gov/news-events/press-releases/2010/12/ftc-testifies-do-not-track-legislation; *see also* Do Not Track Act of 2019, *infra* note 93.

unalienable universal right, and that as with any area of law that requires specialized knowledge, a separate court should be created to deal with such technological matters.

I. The History of the Right to Privacy and the Technology Trap

The Fourth Amendment to the Constitution of the United States is intended to protect citizens against the possibility of unreasonable government intrusion and it affirms "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[6] The Fourth Amendment was undoubtedly influenced by notions of property rights under English common law such as ownership and trespass, a rationale that stands to this day.[7]

In the first major case to discuss electronic surveillance, *Olmstead v. United States*, the Supreme Court had to decide whether the defendant's Fourth Amendment rights were violated when private telephone conversations between the defendants and others were intercepted by means of wire-tapping.[8] The evidence leading to Olmstead's conviction was largely obtained with the use of wiretaps by tapping into the phone lines outside of the suspects' residences.[9] The Court concluded that, "[t]he intervening wires are not part of [defendant's] house or office, any more than are the highways along which they are stretched."[10] Thus, the Court held that the wiretapping of the phones did not constitute a search and did not violate the Fourth Amendment.[11] However, Justice Brandeis' dissent argued that the Fourth Amendment should be understood as prohibiting "every unjustifiable intrusion by the government upon the privacy of the individual."[12] Brandeis reasoned that "[w]ays may someday be developed by which the government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home."[13] Ultimately, Brandeis feared that technological advancements would one day make it possible to discretely and covertly unearth "unexpressed beliefs, thoughts and emotions."[14]

The Supreme Court first departed from the purely property-based rationale that was the backbone of the Fourth Amendment jurisprudence for almost two centuries in *Katz v. United States*.[15] Katz was convicted of interstate transmittal of wagering information in violation of federal law.[16] During trial, the government introduced evidence of Katz's conversations, which were gathered by attaching an electronic listening and recording device to the outside of the public telephone booth Katz was known to use to place calls.[17] The Government contended that *Olmstead*

---

[6] *See* U.S. CONST., amend. IV.
[7] *See* Richard Chen, *An Original Fourth Amendment Based on Property not Privacy*, MEDIUM (Nov. 3, 2018), https://medium.com/@rchen8/an-original-fourth-amendment-based-on-property-not-privacy-90427db5f202; *see also* United States v. Jones, 565 U.S. 400 (2012).
[8] *See* Olmstead v. United States, 277 U.S. 438, 455-57 (1928) (describing information which led to the discovery of the conspiracy and its nature and extent was largely obtained by intercepting messages on the telephones of the conspirators by four federal prohibition officers).
[9] *See id.* at 457, 564-65.
[10] *Id.* at 465.
[11] *Olmstead,* 277 U.S. at 466.
[12] *Id.* at 478 (Brandeis, J., dissenting).
[13] *Id.* at 474.
[14] *Id*.
[15] *See* Katz v. United States, 389 U.S. 347, 352-53 (1967).
[16] *Id*. at 348.
[17] *Id*.

deemed the procedure valid,[18] and the phone booth was in plain view and constructed partly of glass, so Katz was visible when using it.[19] However, the Court found that "what [Katz] sought to exclude when he entered the booth was not the intruding eye—it was the uninvited ear."[20] Thus, placing a call from a public phone booth does not waive the private nature of the conversation.[21] "One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[22]

As Justice Harlan conveyed in his concurrence, "'the Fourth Amendment protects people, not places.' The question, however, is what protection it affords to those people."[23] He then detailed his understanding of the rule that had emerged from prior decisions as "a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[24] Therefore, under *Katz*, a person neither forfeits all expectations of privacy while in public, nor is completely secure while at home.[25] However, Justice Harlan's test involves a certain degree of circularity that may be counterproductive: as society is willing to lower its standards for personal privacy, proportional damage is caused to the Fourth Amendment.[26]

In *United States v. Miller*, the Court decided that a bank depositor had "no legitimate 'expectation of privacy' on matters which he handles using a bank because "checks are not confidential communications but negotiable instruments to be used in commercial transactions."[27] Moreover, because the documents were voluntarily conveyed to the banks and bank employees, "[t]he Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities."[28] The Court explained that a depositor assumes the risk, in revealing his affairs to another, that the information will be conveyed by that person to others, including the government.[29] Furthermore, the Court held that the items subpoenaed were business records of the banks, not respondent's private papers.[30] Therefore, the Fourth Amendment was not violated under either a reasonable expectation of privacy approach or a property-based approach.

In *Smith v. Maryland*, the Court was presented with the question of whether the use of a mechanical device to detect a caller's phone number constitutes a "search" for purposes of the

[18] *See id*. at 349 (arguing under Olmstead, that no violation could occur in the absence of a physical intrusion).
[19] *See Katz*, 389 U.S. at 352; *see also* Ric Simmons, *From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies*, 53 Hastings L.J. 1303, 1307 (2002) (explaining that Justice Harlan's "reasonable expectation of privacy" test in his concurrence in Katz became the test used by subsequent courts).
[20] *See Katz*, 389 U.S. at 352.
[21] *Id.*
[22] *Id*.
[23] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).
[24] *Id.*
[25] *See generally* Katz v. United States, 389 U.S. 347 (1967).
[26] *See* Kyllo v. United States, 533 U.S. 27 (2001) (explaining that the government could pass laws that would lower the expectation of privacy, and similar to society's use of social media, for example, would indicate that expectations of privacy have decreased since the time of Katz).
[27] United States v. Miller, 425 U.S. 435, 442 (1976).
[28] *Id*
[29] *Id.*
[30] *Id*. at 440.

Fourth Amendment.[31] In *Smith*, the police, without a warrant, requested a telephone company to remotely operate a mechanical device to record the numbers dialed from a suspect's home telephone.[32] Smith appealed his conviction on grounds that the use of the mechanical device was a warrantless search; however, the Court of Appeals affirmed the trial court's judgment by holding that "there is no constitutionally protected reasonable expectation of privacy in the numbers dialed into a telephone system and hence no search within the fourth amendment is implicated by the use of a pen register installed at the central offices of the telephone company."[33] Thus, no "search" took place, and no warrant was required. Grounded on its decision in *Miller*, the Court held Smith "assumed the risk" of disclosure by the telephone company of the numbers he dialed, and it would be unreasonable for him to expect his phone records to remain private.[34]

In his dissent, Justice Marshall identified the problem that would become more prevalent as technology continued to evolve when stating "[t]he Court determines that individuals who convey information to third parties have 'assumed the risk' of disclosure to the government."[35] However, Marshall noted that the concept of assumption of risk implies the existence of choice, because "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."[36] Conversely, Marshall noted there exist aspects of modern life in which choice is academic but unrealistic.[37]

In *United States v. Knotts*[38] and *United States v. Karo*[39], the Supreme Court had to decide whether the use of a beeper violated the Fourth Amendment. In *United States v. Knotts*, with the consent of the third-party vendor, a beeper was placed in a drum and reserved for Knotts, who was suspected of manufacturing illegal drugs.[40] Agents then followed the buyer using a combination of visual surveillance and monitoring the beeper signal until it reached Knotts' residence.[41] In deciding that Knotts was not subject to a search, the Court found that "[a] car has little capacity for escaping public scrutiny" and that "[a] person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another".[42] Moreover, the Court agreed, as expressed in Petitioner's Brief, that "beepers are merely a more effective means of observing what is already public."[43] Further, the use of the beeper merely amounted to an enhancement of the visual surveillance.[44] However, in *United States v. Karo*, the Court ruled that monitoring of a beeper inside of a private residence, because a private residence is a location not opened to visual surveillance, violates the Fourth Amendment rights of those who have a justifiable interest in the privacy of their residence.[45] The Court

[31] Smith v. Maryland, 442 U.S. 735, 736 (1979).
[32] *Id*. at 737.
[33] *Id*. at 738 (citing Smith v. State, 283 Md. 156, 173 (1978)).
[34] *Id.* at 744.
[35] Smith, 442 U.S. at 749 (Marshall, J., dissenting).
[36] *Id.* at 749-50 (citation omitted).
[37] *Id.*
[38] *See generally* United States v Knotts, 460 U.S. 277 (1983).
[39] *See generally* United States v Karo, 468 U.S. 705 (1984).
[40] *See Knotts*, 460 U.S. at 278.
[41] *Id.*
[42] *Id*. at 281 (citing Cardwell v. Lewis, 417 U.S. 583, 590 (1974)).
[43] *Knotts*, 460 U.S. at 284 (citing Petitioner's Brief at 6a).
[44] *Id.* at 285.
[45] *Karo*, 468 U.S. at 727-28.

reasoned that monitoring a beeper inside a residence is tantamount to a warrantless entry by the government actor upon that residence, a trespass in direct violation of the Fourth Amendment.[46]

In *United States v. Jones*, a GPS tracking device was physically attached to Jones' vehicle, and his movements were tracked for twenty-eight days, all without a valid warrant.[47] Justice Scalia, writing the majority opinion, declared the unconsented attachment of a GPS device to monitor the car's movements was a search.[48] Justice Scalia noted the car was an "effect" of Jones, an enumerated protected area and thus protected from trespass under the property-based approach.[49] The opinion makes it clear that "Jones's Fourth Amendment rights do not rise or fall with the Katz formulation"; the Court expressly refrained from deciding the case under a reasonable expectation of privacy test due to the basic property rights violations at issue in the case.[50]

Justice Alito, in his concurrence, questioned the wisdom of deciding a high-tech case with a several hundred-year-old approach instead of the *Katz* test, which had become the mainstay of Fourth Amendment jurisprudence for half a century.[51] Justice Alito would instead "analyze the question presented in [the] case by asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[52] Justice Alito worried that "long-term monitoring [could] be accomplished without committing a technical trespass—suppose, for example, that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car—the Court's theory would provide no protection" under its rationale.[53]

The Supreme Court then decided *Carpenter v. United States* in 2018.[54] Carpenter challenged the warrantless search, through his wireless phone providers, of 127 days of Cell-Site Location Information ("CSLI") totaling almost 12,898 location points—an average of 101 data points per day.[55] As Justice Gorsuch points out in his dissent, the case could have been decided in one of three ways.[56] The first way was to ignore the problem and rule consistently with and in reliance on *Smith* and *Miller*.[57] This outcome appeared unpalatable to Chief Justice Roberts and the Court's four "liberals."[58] They even went so far to say "[i]f the confluence of these decisions and modern technology means our Fourth Amendment rights are reduced to nearly nothing, so be it."[59] The second way was to overrule *Smith* and *Miller* and resolve the case using the *Katz* 'reasonable expectation of privacy' test and jurisprudence.[60] This would appear to be the most

[46] *Id.* at 717.
[47] United States v Jones, 565 U.S. 400, 402-03 (2012).
[48] *Id.* at 402, 404.
[49] *Id*. at 404.
[50] *Jones*, 565 U.S. at 406.
[51] *Id.* at 418 (Alito, J., concurring).
[52] *Id.* at 419.
[53] *Id.* at 425.
[54] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).
[55] *See* Transcript of Record at 1, Carpenter, 138 S. Ct 2206 (No. 16-402) (explaining that cell phones work in conjunction with cell sites and every time a phone connects to a nearby cell site a time-stamped record known as CLSI is generated and stored by carriers for several years; thus, accessing CSLI can potentially provide detailed information of someone's whereabouts over a period of several years).
[56] *See Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).
[57] *Id.*
[58] *Id*. at 2206.
[59] *Id.*
[60] *Carpenter*, 138 S. Ct. at 2262.

reasonable option in a world where individuals' pictures, texts, word documents, spreadsheets, and emails, filled with individuals' most embarrassing and darkest secrets, and individuals' dearest and deepest feelings are held, serviced, or monitored by websites, applications, and digital providers. This was the great leap the Court should have taken but did not.

Finally, the last choice in deciding *Carpenter* was to "look for answers elsewhere,"[61] resulting in an expressly narrow opinion, against the government, that deemed the targeted collection of at least seven days of CLSI to be a search.[62] The Court correctly found that CSLI is information that in the aggregate ought to be protected under the Fourth Amendment, but the Court's conclusion appears at odds with *Miller* and *Smith.* Carpenter, like Miller, could "assert neither ownership nor possession" of the documents or information[63]; the documents were deemed business records of the cellphone carrier, just like Miller's were "business records of the banks."[64] Thus, these are not Carpenter's "papers and effects," entitled to property-based protection. Despite that neither *Miller* nor *Smith* were decided utilizing the *Katz* test, but on voluntary conveyance and assumption of risk, the Court engages in a lengthy discussion as to why CSLI should be deemed worthy of higher privacy protection than financial information and phone numbers dialed.[65] Even assuming, *arguendo*, that CSLI are both "papers and effects" under the Fourth Amendment, and that Carpenter had a subjective expectation of privacy on the CSLI that society is willing to recognize, under a plain reading of the Third Party Doctrine, "[o]nce you disclose information to third parties, you forfeit any reasonable expectation of privacy you might have in it."[66] That is precisely the problem with a doctrine that was conceived at a time when the United States was sending men to the Moon with technology generating less calculating power than an iPhone.[67]

II. Privacy, Property, or Both?

Notions of privacy have developed from, and to a certain extent continue to be associated with, notions of property.[68] The ethereal nature of data causes classification problems for many lawyers and judges.[69] In attempting to solve the data problem, it is helpful to understand the origins of property. James Madison, founding father and fourth President of the United States, expressed that, "as a man is said to have a right to his property, he may be equally said to have a property in his rights."[70] Moreover, that "[i]f the United States mean to obtain or deserve the full praise due to wise and just governments, they will equally respect the rights of property, and the property in rights."[71] As expressed by Supreme Court Justice James Wilson in his unfinished work titled *On the History of Property*, "[p]roperty is the right or lawful power, which a person has to a thing. Of

[61] *Id. at* 2262 (Gorsuch, J., dissenting).
[62] *Id.* at 2220.
[63] United States v. Miller, 425 U.S. 435, 440 (1976).
[64] *Id.*
[65] *Carpenter*, 138 S. Ct. at 2217.
[66] *Id.* at 2262 (Gorsuch, J., dissenting).
[67] *See* David Grossman, *How Do NASA's Apollo Computers Stack Up to an iPhone?,* POPULAR MECHANICS (Mar. 13, 2017), https://www.popularmechanics.com/space/moon-mars/a25655/nasa-computer-iphone-comparison/.
[68] U.S. CONST. amend. IV.
[69] Melisa Whitney, *How to improve technical expertise for judges in AI-related litigation*, THE BROOKINGS INSTITUTION (Nov. 7, 2019), https://www.brookings.edu/research/how-to-improve-technical-expertise-for-judges-in-ai-related-litigation.
[70] James Madison, *The Writings of James Madison, vol. 6 [1906]* at 101*,* ONLINE LIBRARY OF LIBERTY, https://oll.libertyfund.org/titles/madison-the-writings-vol-6-1790-1802 (last visited Oct. 27, 2019).
[71] *Id.* at 103.

this right, there are three different degrees."[72] He further differentiated between degrees of ownership: the lowest being the right to possess, an intermediate right to possess and to use, and highest degree being the right to possess, to use, and to dispose of the thing owned.[73]

Wilson also discussed what creates ownership rights, articulating that "[m]an is intended for action. Useful and skillful industry is the soul of an active life. But industry should have her just reward. That reward is property; for of useful and active industry, property is the natural result."[74] Thus, in Wilson's view, exclusive property is preferred over communal property. This view is consistent with John Locke's in that "every [m]an has a *[p]roperty* in his own *[p]erson*. This no [b]ody has any [r]ight to but himself. The *[l]abour* of his [b]ody, and the *[w]ork* of his [h]ands, we may say, are properly his."[75]

The notion of the exclusive nature of property is not a new concept, it has been around for millennia.[76] The Old Testament and the document it was based on, the Hebrew Bible (or Tanakh), have been read and followed for almost three thousand years, and form the moral code of Western Civilization.[77] The Bible is replete with examples of the express acceptance of exclusive property.[78] For example, Exodus tells the story of how Moses was directed by God to deliver the Israelites from slavery in Egypt.[79] As the group was camped by Mount Sinai, God handed Moses the Ten Commandments as a moral and spiritual guide.[80] The Eighth Commandment states "[y]ou shall not steal."[81] The Tenth Commandment states "[y]ou shall not covet your neighbor's house; you shall not covet your neighbor's wife, nor his male servant, nor his female servant, nor his ox, nor his donkey, nor anything that is your neighbor's."[82] This divine guidance, handed down at times of conflict and tribulations, makes it clear that property can be private and exclusive. One should not steal or covet from someone something that does not belong to that someone. Even for a collection of people escaping oppression, exclusive property did not become communal property and this is a concept that should be respected even now.[83]

On December 10, 1948, The United Nations General Assembly unveiled The Universal Declaration of Human Rights.[84] The declaration espoused traditional Judeo-Christian values prevalent in the West, along with notions of fairness engraved in the U.S. Constitution.[85] The declaration states that "the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world."[86] Among those rights the following are listed:

---

[72] James Wilson, *Collected Works of James Wilson, vol. 1 [2007]* at 387, ONLINE LIBRARY OF LIBERTY, https://oll.libertyfund.org/titles/2072#Wilson_4140_1872 (last visited Oct. 15, 2019).
[73] *Id.*
[74] *Id.* at 396.
[75] John Locke, Second Treatise, §§ 25-51, 123-26 at 27.
[76] *See generally Exodus* 1-40 (King James).
[77] *See* Mark Silk, *Notes on the Judeo-Christian Tradition of America*, AMERICAN QUARTERLY, Vol. 36, No. 1, (Spring 1984), 65-85.
[78] *See Exodus* 20:15, 17, (King James); *see also Deuteronomy* 5:19, 21 (King James).
[79] *See generally Exodus* 1-40 (King James).
[80] *Id.* at 24:12-13.
[81] *Exodus* 20:15 (King James).
[82] *Exodus* 20:17 (King James).
[83] *See generally Exodus* 1-40 (King James).
[84] *See* The Universal Declaration of Human Rights, G.A. Res. 217 (III), at 71 (Dec. 10, 1948).
[85] *See* Silk, *supra* note 77; *see also* U.S. CONST., amend. I-VIII, XIII-XV, XIX.
[86] The Universal Declaration of Human Rights, G.A. Res. 217 (III), at 71.

> Article 12.
> No one shall be subjected to arbitrary interference with his privacy …
> …
> Article 17.
> (1) Everyone has the right to own property alone as well as in association with others.
> (2) No one shall be arbitrarily deprived of his property.
> …
> Article 30.
> Nothing in this Declaration may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein.[87]

A grand achievement at the time, this Declaration drafted over 70 years ago would benefit from updates and revisions. Not because the issues raised in it are no longer applicable, but because technology has advanced so dramatically that new areas impacting human life deservedly have a place in such an important document. In more recent times, politicians on both sides of the aisles in the United States have attempted to bring awareness and limit the overreach of technology companies.[88] In 2012, the Obama Administration unveiled the Privacy Bill of Rights.[89] Under this blueprint:

> [c]onsumers have a right to exercise control over what personal data organizations collect from them and how they use it[,] [c]onsumers have a right to easily understandable information about privacy and security practices, [c]onsumers have a right to expect that organizations will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data[,]consumers have a right to secure and responsible handling of personal data, [c]onsumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data are inaccurate, [c]onsumers have a right to reasonable limits on the personal data that companies collect and retain,[c]onsumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.[90]

However, these guidelines are unenforceable because Congress has never granted authority to the Federal Trade Commission to enforce them.[91] During the 116TH Congress, Senator Josh

[87] *Id.* at 73-74, 77.
[88] *See* We Can't Wait, *infra* note 89; *see also* Do Not Track Act of 2019, *infra* note 92; *see also* Yang, *infra* note 95.
[89] *See We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online*, THE WHITE HOUSE PRESS RELEASE (Feb. 23, 2012), https://obamawhitehouse.archives.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights.
[90] *Id*.
[91] *See* Cameron F. Kerry and Daniel J. Weitzner, *Rulemaking and its discontents: Moving from principle to practice in federal privacy legislation,* TECHTANK (June 5, 2019), https://www.brookings.edu/blog/techtank/2019/06/05/rulemaking-and-its-discontents-moving-from-principle-to- practice-in-federal-privacy-legislation/.

Hawley (R-MO) introduced the Do Not Track Act of 2019.[92] The purpose of the Act is "[t]o protect the privacy of internet users through the establishment of a national Do Not Track system[.]"[93] The bill deems "a covered website, service, or application that collects data for the purpose of designing or displaying targeted advertisements shall be considered to be collecting more data than is necessary to operate such website, service, or application."[94] Andrew Yang, a former 2020 Democratic presidential candidate, made data ownership a key element of his political philosophy.[95] In his words, "[d]ata generated by each individual needs to be owned by them, with certain rights conveyed that will allow them to know how it's used and protect it."[96] Just like the ox and donkey, the Tenth Commandment urges us not to covet; however, technology companies do not simply covet but outright steal our modern-day belongings – our data.[97] Unsurprisingly, both Hawley and Yang are much younger than the average Senator, member of Congress, or presidential candidate, as well as younger than the average federal judge.[98]

III. A Different Type of Court

The time for a more informed court is fast approaching. As previously discussed, in *Jones,* Justice Alito's criticism in his concurrence is well-founded, however, it is arguably insufficient in that it only directs the attention to the theories involved in the resolution of the case, and not on the capacity of the judges to understand the issues.[99] Article III of the Constitution states, in part, that "[t]he judicial Power of the United States, shall be vested in one supreme court, and in such inferior courts as the Congress may from time to time ordain and establish."[100] Additionally, the Legislature under Article I, and even the Executive under Article II, are able to create special-purpose courts if necessary.[101] Article II Courts are tribunals established: (1) pursuant only to the President's war-making power under Article II of the Constitution; (2) which exercises either civil jurisdiction or criminal jurisdiction over civilians in peacetime; and (3) was constituted without an Act of Congress or any other legislative concurrence.[102] Article II Courts have very limited applicability and jurisdiction; thus, have been used sparingly throughout history.[103]

Article I Courts, on the other hand, are plentiful and serve to meet the needs of the District of Columbia, the military, government agencies, and other important purposes.[104] In particular,

[92] *See* Do Not Track Act of 2019, S. 1578, 116TH CONG. (2019).
[93] *Id.* at 1.
[94] *Id.* at § 4(a)(2)(C).
[95] *See* Andrew Yang, *Data as A Property Right*, YANG 2020, https://www.yang2020.com/policies/data-property-right (last visited Sept. 13, 2019).
[96] *Id.*
[97] *See* Exodus*, supra* note 83; *see also* Bernard Marr, *Big Data Facts: How Many Companies Are Really Making Money From Their Data?,* FORBES (Jan. 13, 2016), https://www.forbes.com/sites/bernardmarr/2016/01/13/big-data-60-of-companies-are-making-money-from-it-are-you/#4c7257b32d8f.
[98] *See Membership of the 116th Congress: A Profile*, CONGRESSIONAL RESEARCH SERVICE (updated Oct. 17, 2019), https://crsreports.congress.gov; *see also Demography of Article III Judges, 1789-2017*, FEDERAL JUDICIAL CENTER, https://www.fjc.gov/history/exhibits/graphs-and-maps/age-and-experience-judges (last visited Nov. 1, 2019).
[99] United States v Jones, 565 U.S. 400, 418-19 (2012) (Alito, J., concurring).
[100] *See* U.S. CONST. art. III.
[101] *See generally* David J. Bederman, *Article II Courts*, 44 MERCER L. REV. 825 (1993).
[102] *Id.* at 832.
[103] *Id.* at 837-38.
[104] *See Court Role and Structure*, UNITED STATES COURTS, https://www.uscourts.gov/about-federal-courts/court-role-and-structure (last visited Aug. 1, 2019).

Article I Courts generally have jurisdiction over special disputes between the government and others.[105] Included in the Article I Courts, are the United States International Trade Commission, the Patent Trial and Appeal Board, the Trademark Trial and Appeal Board, the United States Tax Court, and the United States bankruptcy courts.[106] Thus, Congress has had no problem creating courts under Article I, in particular, courts where the expertise of the judges was intensified and protected.[107] Congress is not a stranger to the creation of Article I Courts, so it is proper to question whether the current judiciary has in its rank a sufficient number of technologically savvy judges who can take on the delicate task to determine these matters with the level of expertise the issue requires. If the answer is in the negative, it is an opportunity for Congress and the Judiciary to do what has successfully been done with taxes, patents, and trademarks.

Arguably, the majority of technology-related controversies to be resolved by the courts may likely involve individuals and corporations only, not government entities. Thus, the creation of a specialized court under Article I may be viewed as a usurpation of Article III's jurisdiction and challenged as such.[108] Therefore, Article III courts will continue to capture and adjudicate the majority of these matters. Nevertheless, Article III courts are organized in civil, criminal and bankruptcy divisions.[109]

IV. Conclusion

Technology has outpaced politicians and judges alike. In a world marked by globalization; connectivity; and collaboration, consumers cannot function without the benefit of internet connections, applications, search engines, or smart phones. Tech companies know this, and they take advantage of it by gathering, storing, and making tremendous profits from customer data. However, a man is entitled to his property, and he has a property right to the fruits of his labor. In the digital age, the data generated should be considered the fruits of one's labor. Thus, it follows that one should be entitled to share the benefits.

Under the standards promulgated by *Miller* and *Smith*, the courts would deem the data collected as the exclusive property of the tech companies, as it is collected in the ordinary course of business of these companies.[110] Yet, one major distinction exists: who benefits the most. In *Miller*, Miller undeniably benefited greatly from using the bank. In *Smith*, Smith undeniably benefited greatly from being able to use the Phone Company's services. However, today's customers do not see a benefit from most of their interactions in the digital age, at least not in the same order or magnitude as the companies mining their data.[111]

---

[105] *See* David A. Case, *Article I Courts, Substantive Rights, and Remedies for Government Misconduct*, 26 N. ILL. U. L. REV. 101, 103-04 (2005).
[106] *Id.*
[107] *Id.* at 177–78*; see also* UNITED STATES TAX COURTS, *About the Court,* https://www.ustaxcourt.gov/about.htm (last visited Nov. 1, 2019) (explaining the public benefits of the expertise accumulated and exhibited by Tax Court judges).
[108] *See* Brett Axelrod, *U.S. Supreme Court Dramatically Curtails Bankruptcy Courts' Powers,* FOX ROTHSCHILD LLP (Sep. 2011), https://www.foxrothschild.com/publications/u-s-supreme-court-dramatically-curtails-bankruptcy-courts-powers/.
[109] *See generally* Types of Cases, UNITED STATES COURTS, https://www.uscourts.gov/about-federal-courts/types-cases (last visited Aug. 1, 2019).
[110] *See generally* United States v. Miller, 425 U.S. 435 (1976); *see also* Smith v. Maryland, 442 U.S. 735 (1979).
[111] *See* Bottles, K., Begoli, E. and Worley, B., 2014. *Understanding the pros and cons of big data analytics*, PHYSICIAN EXECUTIVE, 40 Vol. 4, 6-12.

Nevertheless, the recognition of data as a property right may not be a matter for Article III courts. This recognition and shift should be better accomplished by the Legislature, first, by seriously considering the meaningful proposals already on the table,[112] and second, by working with and for the people who they claim to represent in securing their rights and preventing corporate abuse. As society moves forward toward this goal, the judiciary must be updated and upgraded in order to properly serve the people. In this regard, the recruitment and appointment of tech-savvy judges is imperative. In addition, the creation of a specific Court system, similar to the Tax Court, would considerably improve the expertise and consistency in court rulings involving data privacy.

[112] *See* We Can't Wait, *supra* note 89; *see also* Do Not Track Act of 2019, *supra* note 92; *see also* Yang, *supra* note 95.