Objects, Places and Cyber-Spaces Post-*Carpenter*: Extending The Third-Party Doctrine Beyond CSLI: A Consideration of IoT and DNA

Eunice Park*

21 YALE J.L. & TECH. 1 (2019)

At the November 2017 oral arguments in the case Carpenter v. United States, Justice Sotomayor commented that many individuals even carry their cell phones into their beds and public restrooms: "It's an appendage now for some people."[1] *On June 22, 2018, in a 5-4 opinion written by Chief Justice Roberts and joined by Justices Ginsberg, Breyer, Sotomayor, and Kagan, the Supreme Court held that the government will generally need a warrant to access cell-site location information (CSLI).*[2] *Ostensibly, Carpenter is only about CSLI, and the language of the decision carefully limits its application. However, the Court's reasoning behind why the third-party doctrine should not apply is broadly applicable: the information was involuntarily exposed, incidental to merely having a cell phone, which is an item necessary for functioning in modern society.*[3] *Indeed, technology's constant forward march leads one to wonder, what privacy issue awaits around the next corner? What technological innovation will pose yet another Fourth Amendment challenge? Our cell phones commonly have health apps that monitor our activity, sleep, mindfulness, and nutrition.*[4] *Internet of Things (IoT) de-*

* Associate Professor of Lawyering Skills, Western State College of Law. A special thank you to Western State College of Law Librarian Scott Frey for his invaluable research assistance; Professor Emeritus Neil Gotanda for his cogent insights; and the editors of the *Yale Journal of Law and Technology*, particularly Kelsey Stimson, Phil Yao and Adam Pan, for their thoughtful suggestions. The views expressed in this article are my own. I am grateful always to my parents, husband and children. I dedicate this article to my mom, Kyung S. Park, and to the memory of my dad, Jong M. Park.

[1] Greg Stohr, *Supreme Court Justices Hint at More Digital-Privacy Protections*, BLOOMBERG NEWS (Nov. 29, 2017), https://www.bloomberg.com/news/articles/2017-11-29/supreme-court-justices-hint-at-new-digital-privacy-protections.

[2] Carpenter v. United States, 138 S. Ct. 2206 (2018).

[3] *Id*. at 2220.

[4] APPLE, https://www.apple.com/ios/health; *see also* Nadine Bol, Natali Helberger & Julia C. M. Weert, *Differences in Mobile Health App Use: A Source of New Digital Inequalities?*, 34 INFO. SOC'Y 183, 183 (2018),

vices, which have the ability to connect to and interface with a network,[5] *include "smart" light bulbs, refrigerators, and even a mattress cover that starts your Bluetooth or WiFi-enabled coffee maker when you wake up in the morning.*[6] *The private genomic testing industry, too, in which intimate genealogical and genetic health information is sent to third-party laboratories, medical researchers, and even sold to pharmaceutical companies for profit, has seen tremendous growth recently.*

IoT devices and private DNA testing seem vastly different from each other and from cell phones, and yet both are increasingly popular consumer technologies whose functioning, by design, necessitates a third party. Like CSLI, the data sent to third parties by smart devices and genomic testing services involves no voluntary act, let alone affirmative sharing. This lack of voluntariness was a significant part of the Carpenter *Court's basis for holding—in a decision lauded by privacy advocates—that the cell phone owner has an expectation of privacy in CSLI, despite the fact that the data is owned by a third party. Thus, notwithstanding its limiting language,* Carpenter *opens the door to a slew of questions about consumers' privacy expectations in multitudes of other burgeoning technologies that, like cell phones and the location data they produce, also necessitate a third party. This Article, therefore, proposes extending the third-party doctrine in* Carpenter*'s wake to reflect the realities of the digital age, both to protect privacy and provide some limits to the third-party doctrine. Given that a third party has control over a consumer's personal data, a meaningful test for whether an expectation of privacy remains or has been forfeited should include two inquiries: first, whether the consumer understands that the technology's*

---

https://www.tandfonline.com/doi/pdf/10.1080/01972243.2018.1438550 ("Mobile health apps are increasingly gaining popularity. . . .").

[5] Karen Rose, Scott Eldridge & Lyman Chapin, *The Internet of Things: An Overview,* INTERNET SOC'Y 4 (Oct. 2015), https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC-IoT-Overview-20151221-en.pdf ("The Internet of Things is an emerging topic of technical, social, and economic significance. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities."); *Smart Device*, TECHOPEDIA, https://www.techopedia.com/definition/31463/smart-device.

[6] Melia Robinson, *This Mattress Cover Can Wake You Up, Change Temperature, and Start Your Morning Coffee*, BUS. INSIDER (Mar. 8, 2016, 2:20 PM), http://www.businessinsider.com/luna-smart-mattress-cover-by-eight-2016-3.

very design necessitates a third party; and second, whether the consumer has a meaningful opportunity to opt out of sharing data with that third party.

This Article begins by describing the common law background that prefaced Carpenter*, explains why the* Carpenter *analysis is incomplete, and offers the new, extended test for the third-party doctrine as one that balances decisional analysis with technological reality and provides a principled framework to encompass technologies beyond CSLI. Next, this Article offers normative explanations for why digital data is a square peg in the round hole of the third-party doctrine but explains that privacy in the digital era should nonetheless survive the disconnect. Finally, this Article applies the newly extended third-party doctrine test to two specific examples of increasingly popular technologies in which private data is necessarily shared with third parties: IoT devices and private DNA testing. This Article illustrates the inability of smart devices and private genomic testing services to pass the two inquiries of the proposed extended test, and affirms the consumer's expectation of privacy in the absence of any voluntary act.*

I. INTRODUCTION 5

II. TRADITIONAL TENSIONS, CARPENTER DECONSTRUCTED, AND THE CALL FOR A NEW EXTENSION OF THE THIRD-PARTY DOCTRINE IN THE DIGITAL AGE 8

A. The Fourth Amendment: Property or Privacy? 8

B. Carpenter Deconstructed: A Direct Strike at the Third-Party Doctrine 11

C. The Call for a New Extension of the Third-Party Doctrine: A Proposal for a Retrospective Test 13

III. FITTING THE SQUARE PEG OF DIGITAL DATA IN THE ROUND HOLE OF THE THIRD-PARTY DOCTRINE 17

A. Why Privacy Should Survive the Disconnect with Traditional Decisional Analysis: "We're Not in Kansas Anymore" 17

B. Consumers' Contradictory Behavior: An Explanation 22

1. Dissociative appeal dilutes apprehension 24

2. Social mandate contributes to an illusion of indifference 26

IV. THE NEW TEST APPLIED: PERSONAL DATA OF SMART DEVICES AND DNA TESTING 28

C. Smart Technology: Wearable and Voice-Activated 29

1. IoT devices necessitate a third party, but not necessarily consumer awareness 29

2. IoT devices lack meaningful ability to opt out 38

D. Private DNA and Genetic Testing Companies 40

1. Private DNA testing services necessitate a third party, but not necessarily consumer awareness 40

2. Testing services lack meaningful ability to opt out 45

V. CONCLUSION 55

I. INTRODUCTION

On June 22, 2018, the Supreme Court held that the Government will generally need a warrant to access historical cell-site location information ("CSLI").[7] In arriving at its decision, *Carpenter* held that CSLI was not subject to the "third-party doctrine"—the general rule that an individual lacks a reasonable expectation of privacy in information he or she has voluntarily disclosed to a third party, and that "the Government is typically free to obtain such information from [the third party] without triggering Fourth Amendment protections."[8] Ostensibly, *Carpenter* is only about CSLI, and the language of the Court's decision is careful to limit its application.[9] However, the constant forward march of technology leads one to wonder, what privacy issue awaits around the next corner? What technological innovation will pose yet another Fourth Amendment challenge? Our cell phones commonly have health apps that monitor our activity, sleep, mindfulness, and nutrition.[10] "Smart" devices, with the ability to connect and interface with a network,[11] include light bulbs, refrigerators, even a smart mattress cover that starts your Bluetooth or WiFi-enabled coffee maker when you wake up in the morning.[12] Private genomic testing, too, with intimate genealogical and genetic health information sent to third-party laboratories, medical researchers, and even sold to pharmaceutical companies for profit, has seen tremendous recent growth.

IoT devices and private DNA testing seem vastly different from each other and from cell phones, yet both are increasingly popular consumer technologies whose functioning, by design, necessitates a third party. Like CSLI, the data sent to third parties by smart devices and DNA requires no voluntary act, let alone an act of affirmative sharing. This lack of voluntariness was a significant part of the *Carpenter* Court's basis for holding that the cell phone owner has an expectation of privacy in CSLI, despite the fact that the data is

---

[7] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[8] *Id.* at 2216; *see also* Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age*, 28.2 ALB. L.J. SCI. & TECH. 73, 110-11 (2017) (citations omitted).
[9] *Carpenter*, 138 S. Ct. at 2220.
[10] APPLE, https://www.apple.com/ios/health, *supra* note 4; Bol, Helberger & Weert, *supra* note 4.
[11] Rose, Eldridge & Chapin, *supra* note 5; TECHOPEDIA, *supra* note 5.
[12] Robinson, *supra* note 6.

owned by a third party. Thus, notwithstanding its limiting language, *Carpenter* opens the door to a slew of questions about consumers' privacy expectations in multitudes of other burgeoning technologies that, like cell phones and the location data they produce, also necessitate a third party.

This Article, therefore, proposes extending the third-party doctrine in *Carpenter*'s wake to reflect the realities of the digital age, both to protect privacy and provide some boundaries to the third-party doctrine. Given that third parties control consumer data, a meaningful test for whether an expectation of privacy remains or has been forfeited must include two inquiries: first, whether the consumer understands that the technology's very design necessitates a third party; and second, whether the consumer has a meaningful opportunity to opt out of sharing data with that third party. This Article examines smart devices and private genomic testing services as examples of technologies in which private data necessarily is shared with third parties, illustrates their inability to pass these two inquiries, and affirms the consumer's expectation of privacy in the absence of any voluntary act under such circumstances.

Part II of this Article first describes the Fourth Amendment expectation of privacy and the traditional tension between the property and privacy analytical approaches. Section II.B then deconstructs *Carpenter*'s reasoning for finding a privacy interest in CSLI. Section II.C proposes a new extension of the third-party doctrine that rejects the first part of the Court's test (pervasiveness) and urges instead that the second part of the test is pivotal: the absence of an affirmative act of sharing. Given the absence of an affirmative act of sharing with a third party, two inquiries should follow: first, whether the consumer understood that the technology necessitated a third party; second, whether a meaningful opportunity to opt out existed. This extended two-part test maintains focus on the decisionmaker, yet recognizes that the landscape upon which the doctrine is predicated has become altered in the digital era. By operating retrospectively, the new test provides a principled framework to encompass technologies beyond *Carpenter*'s cell phones and the CSLI they produce.

Part III offers normative explanations for why digital data is a square peg in the round hole of the third-party doctrine. Section III.A discusses why privacy in the digital era should nonetheless survive the disconnect with traditional decisional analysis, and why both the majority and dissenting opinions of *Carpenter* are incomplete. Section III.B then offers explanations for consumers' seemingly contradictory behavior as to privacy concerns that are, nonetheless, consistent with a privacy expectation.

Part IV applies the newly extended third-party doctrine test to two examples of increasingly popular technologies: IoT devices and DNA testing. Both technologies, by design, necessitate a third party and even create opportunities for secondary third parties. Moreover, even if the consumer is aware that personal data will be shared with a third party, no meaningful opportunities are available to opt out of the arrangement, since the choice presented is either use with these conditions or no use at all.

Part V concludes with some thoughts about the urgent need for the Court to extend the third-party doctrine for the growing assembly of technologies whose designs necessitate a third party, if the expectation of privacy is to have any continued resonance.

II. TRADITIONAL TENSIONS, CARPENTER DECONSTRUCTED, AND THE CALL FOR A NEW EXTENSION OF THE THIRD-PARTY DOCTRINE IN THE DIGITAL AGE

A. The Fourth Amendment: Property or Privacy?[13]

The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers and effects" and mandates that a search or seizure conducted by a government agent must be "reasonable."[14] Although no general constitutional right to privacy exists, and it is not expressly written into the amendment's language, [15] Fourth Amendment jurisprudence encompasses an expectation of privacy.[16] The Fourth Amendment originally "was understood to embody a particular concern for government trespass,"[17] but, since *Katz v. United States* was decided in 1967, has also been held to implicate a reasonable expectation of privacy.[18] To invoke Fourth Amendment protection against unreasonable or warrantless searches based on a "*Katz* invasion of privacy,"[19] the area searched must be one in which there is a "constitutionally protected reasonable expectation of privacy."[20] This consists of both a subjective and objective 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.'"[21]

---

[13] Portions of this passage are adapted from Eunice Park, *Traffic Ticket Reasonable, Cell Phone Search Not: The Cell Phone as 'Hybrid' and the Search Incident-to-Arrest Exception*, 60 DRAKE L. REV. 429 (2012).

[14] U.S. Const. amend. IV.

[15] *See* Katz v. United States, 389 U.S. 347, 350 (1967) ("[T]he Fourth Amendment cannot be translated into a general constitutional 'right to privacy.'"); *see also* Newhard v. Borders, 649 F. Supp. 2d 440, 449-50 (D. W.Va. 2009) ("[A]ny plausible claim would [not] arise . . . under privacy rights protected by the Constitution.") (citing Carroll v. Parks, 755 F.2d 1455 (11th Cir. 1985)).

[16] *See Katz*, 389 U.S. at 351 ("[T]he Fourth Amendment protects people, not places.").

[17] United States v. Jones, 565 U.S. 400, 406 (2012).

[18] *Id.* at 406-08. *But see id.* at 422 (Alito, J., concurring) (interpreting *Katz* as "finally [doing] away with the old approach, holding that a trespass was not required for a Fourth Amendment violation").

[19] *Id.* at 408 n.5.

[20] *Katz*, 389 U.S. at 360 (Harlan, J., concurring).

[21] *Id.* at 361. The Court held that a person in a telephone booth could rely upon the protection of the Fourth Amendment. "One who occupies [a telephone booth], 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." *Id.* at 352 (majority opinion).

Once a reasonable expectation of privacy has been established, the burden is on the government to justify a warrantless search.[22] "[T]he Constitution requires 'that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police.'"[23] A warrantless search is per se unreasonable, "subject only to a few specifically established and well-delineated exceptions."[24] Under the exceptions, certain types of searches and seizures are per se valid even in the absence of probable cause or a warrant.[25]

Against this backdrop, a tension has developed between two different approaches to Fourth Amendment privacy issues, with one approach invoking theories of physical trespass, and another emphasizing privacy rights of a more intangible nature.[26]

For example, in the 2012 case *United States v. Jones*, the Supreme Court held that a Global Positioning System (GPS) attached to the undercarriage of a vehicle to track its movements constituted a search.[27] In his majority opinion, Justice Scalia reasoned that attaching the tracking device to the vehicle was a physical trespass, and said the Court did not need to address whether the defendant had a reasonable expectation of privacy, since that test added to, but did not substitute for, the common law trespassory test.[28] The end result, nonetheless, is that a warrant is now required if the government wants to attach a GPS to an individual's vehicle.

In contrast to *Jones*, which viewed the privacy issue as secondary to the property rationale, *Riley v. California* focused on the immense privacy implications of warrantless cell phone searches.[29] In holding

---

[22] *Id.* at 357.
[23] *Id.* (quoting Wong Sun v. United States, 371 U.S. 471, 481-82 (1963)).
[24] *Id.*
[25] *See Katz*, 389 U.S. 347, 357 (citing examples of cases reinforcing the principle that warrantless searches may be valid in exceptional situations).
[26] The discussion of *United States v. Jones*, *Riley v. California*, and *Katz v. United States* in this passage is adapted from Eunice Park, *Protecting the Fourth Amendment After Carpenter in the Digital Age: What Gadget Next?*, 60 ORANGE COUNTY LAW. MAG. 34, 35 (2018).
[27] 565 U.S. 400 (2012).
[28] *Id.* at 406-08.
[29] The discussion about Riley is adapted from Eunice Park, *The Elephant in the Room: What Is a 'Nonroutine' Border Search, Anyway?: Digital Device Searches Post-Riley*, 44 HASTINGS CONST. L.Q. 277, 278-79 (2017).

that a warrant is required to search a cell phone, even in a search incident to arrest, Chief Justice Roberts explained, "Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person" in part because of "their immense storage capacity."[30] The answer "to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant."[31] While the rationale that a cell phone has unique quantitative and qualitative properties seems almost simplistic now, the decision was only rendered in 2014, resolving the then-tenacious circuit split as to whether a cell phone was a traditional container requiring a warrant to search.[32] The emphasis on privacy represented a return to the reasonable expectation of privacy test articulated in *Katz*.[33] In so doing, the Court also "[took] clear aim at the third-party rule—that 'non-content' records like call logs, location data, and other metadata held by third parties can be collected by the government without a warrant."[34]

Thus, whether an individual has a "reasonable expectation of privacy" has been framed, since *Katz*, as a two-part test and viewed as a discrete, measurable expectation. While not built into the Constitution, this concept has become an accepted, critical component of Fourth Amendment jurisprudence, consistent with the American ethos of individuality and choice. In assailing the container construct and asserting the primacy of privacy even in the absence of physical objects, the *Riley* Court reaffirmed this ethos, opening the door for the intangible data of CSLI to pose its Supreme Court challenge. A critique of the *Carpenter* decision, however, exposes the inadequacy of the traditional analytic framework in the digital era, as discussed in the next Section.

---

[30] Riley v. California, 134 S.Ct. 2473, 2489 (2014).
[31] *Id.* at 2495.
[32] Portions of this article are adapted from Park, *supra* note 13.
[33] 389 U.S. 347 (1967).
[34] Marc Rotenberg & Alan Butler, *Symposium: In* Riley v. California*, A Unanimous Supreme Court Sets Out Fourth Amendment for Digital Age*, SCOTUSBLOG (June 26, 2014), http://www.scotusblog.com/2014/06/symposium-in-riley-v-california-a-unanimous-supreme-court-sets-out-fourth-amendment-for-digital-age; *see also* Park, *supra* note 13, at 460.

B. Carpenter Deconstructed: A Direct Strike at the Third-Party Doctrine

The "clear aim"[35] the Court took at the third-party rule in *Riley* became a direct strike in *Carpenter*. After the FBI identified the cell phone numbers of several robbery suspects, the Government obtained the petitioner Timothy Carpenter's cell phone records under the Stored Communications Act.[36] Wireless carriers produced Carpenter's CSLI, including 12,898 location points cataloging his movements over 127 days.[37] "In the Government's view, the location records clinched the case" by confirming that Carpenter was "right where the . . . robbery was at the exact time of the robbery."[38]

The Court held that the Government's acquisition of Carpenter's CSLI was a Fourth Amendment search requiring a warrant supported by probable cause.[39] While "[t]he Government's primary contention . . . is that the third-party doctrine governs this case," the Court drily noted that "[t]he Government . . . recognizes that this case features new technology."[40] Thus, the Government's "assert[ion] that the legal question nonetheless turns on a garden-variety request for information from a third-party witness . . . fails to contend with the seismic shifts in digital technology" that include "the exhaustive chronicle of location information casually collected by wireless carriers today."[41]

The decision that Carpenter had a privacy interest in his CSLI was informed by "the intersection of two lines of cases."[42] The first line involves "a person's expectation of privacy in his physical location and movements."[43] The second line involves the distinction "between what a person keeps to himself and what he shares with others"[44]: the third-party doctrine. The third-party doctrine, in turn, re-

---

[35] *See* Rotenberg & Butler, *supra* note 34.
[36] *Carpenter*, 138 S. Ct. at 2212.
[37] *Id.*
[38] *Id.* at 2213.
[39] *Id.* at 2221.
[40] *Id.* at 2219.
[41] *Id.*
[42] *Id.* at 2214-15.
[43] *Id.* at 2215.
[44] *Id.* at 2216.

lies on two rationales: first, since business records are not confidential communications, the defendant can "assert neither ownership nor possession" and the nature of the records itself confirms a limited expectation of privacy.[45] Second, under the rationale of voluntary exposure, a defendant who has shared information with another forfeits an expectation of privacy in that information.[46]

The Court asserted that the rationale of voluntary exposure is unsustainable when it comes to CSLI, offering another subset of reasons.[47] First, the technology is pervasive. "[C]ell phones and the services they provide are 'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[48] Second, information cannot be said to be voluntarily exposed in the absence of an affirmative act. A "cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up . . . . [I]n no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements."[49]

By its decision, the Court reinforced the *Katz* principle that the Fourth Amendment protects not only property interests but certain expectations of privacy as well.[50] While acknowledging the property-privacy tension in Fourth Amendment jurisprudence, the Court, rather than adhering to an originalist property-based interpretation, looked to history to underscore the Framers' concerns with government intrusion. It saw the Fourth Amendment as aiming to "secure the 'privacies of life' against 'arbitrary power,'" and "'place obstacles in the way of a too permeating police surveillance.'"[51] The Court found itself "obligated . . . to ensure that the 'progress of science' does not erode Fourth Amendment protections."[52] It is this

---

[45] *Id.* (citing United States v. Miller, 425 U.S. 435, 440, 442 (1976)).
[46] *Id.* at 2220 ("The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another.").
[47] *Id.*
[48] *Id.* (citing Riley v. California, 134 S.Ct. 2473, 2484 (2014)).
[49] *Id.* (citing Smith v. Maryland, 442 U.S. 735, 745 (1979)).
[50] *Id*. at 2213 (citing Katz v. United States, 389 U.S. 347, 351 (1967)).
[51] *Id.* at 2214 (citations omitted).
[52] *Id.* at 2223 (citing Olmstead v. United States, 277 U.S. 438, 474 (1928) (Brandeis, J., dissenting)).

very "progress of science" that lends *Carpenter* portent beyond CSLI, despite its purported narrowness.[53]

C. The Call for a New Extension of the Third-Party Doctrine: A Proposal for a Retrospective Test

The limiting language of *Carpenter* is telling: "We do not disturb the application of *Smith* and *Miller* or call into question conventional, surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information."[54] This attempt at limitation, however, calls into question the vastness of information residing outside the obsolete pen registers of *Smith v. Maryland*[55] and the traditional bank statements of *United States v. Miller*.[56]

Indeed, the wide swath of popular consumer products and services beyond CSLI that *Carpenter* implicates is as endless as technological innovation. The broad applicability of the reasoning, despite the decision's limiting language, invites relentless future arguments before the Supreme Court. Specifically, in our digitally plugged-in society, how is one to approach the information collected by smart devices and private genetic testing companies? One way to avoid litigation as endless as technological innovation itself is to limit the third-party doctrine for technologies that require sharing personal information with third parties.

---

[53] *See, e.g.*, Ian Lopez, *When Privacy Prevails: ACLU Lawyer Dishes on SCOTUS'* Carpenter *Decision*, LAW.COM: LEGALTECH NEWS (June 29, 2018), https://www.law.com/legaltechnews/2018/06/29/when-privacy-prevails-aclu-lawyer-dishes-on-scotus-carpenter-decision ("[T]he court has created space for future cases to address what protections are necessary for all the other kinds of highly sensitive digital age data that's held by third-party companies. That's everything from the content of our emails to information generated by GPS on our phones, whether it's medical information or a record of everything we read on newspaper apps or fertility tracking or so much more. Information about the state of our bodies being collected by a smartwatch or another wearable medical device, information about the interior of our home from internet of things devices, like a smart thermostat that knows when you're home and maybe what room you're in.").

[54] *Carpenter*, 138 S. Ct. at 2220.

[55] 442 U.S. 735 (1979).

[56] 425 U.S. 435 (1976).

This Article does not focus on reinforcing the Court's first reason for why the third-party doctrine does not apply—the qualitative distinctions between "business records" and CSLI. Instead, this Article's primary interest is in the applicability of the Court's second reason, involuntary exposure, which was broken down into pervasiveness and the absence of affirmative sharing. This Article urges rejecting the first part of *Carpenter*'s involuntary exposure test—the pervasiveness of the technology—and proposes that the key focus of the third-party doctrine should instead be the existence, or absence, of an affirmative act of sharing.

A proposal for balance. Whether an affirmative act of sharing has taken place requires a subtler look than the Court has given it. An expectation of privacy—subjective and objective, under the *Katz* test—should not be forfeited simply because a third party owns or controls a consumer's personal data, as the *Carpenter* dissent would have it. Nor should an expectation of privacy be assumed simply because the consumer did not voluntarily share the data, which would encompass virtually all current technology. Rather, when there is no affirmative act of sharing, the new third-party doctrine test should be a retrospective one, involving two inquires: first, whether the consumer understood that the technology necessitated sharing data with a third party; and second, whether the consumer had a meaningful opportunity to opt out of that sharing.

Pervasiveness should not be a prerequisite. It is hard to imagine a technological device or service as pervasive as the cell phone. As the Supreme Court noted in *Riley*, it is "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[57] Certainly, IoT devices and genomic testing, at least currently, are not. The purpose and design of these other technologies circumvent the cell phone's prescription for constant physical attachment.[58] Smart devices and private DNA testing are not indispensable; they may even be considered luxuries. However, this should not matter. The cell phone, too, initially could have been considered a luxury, until society gradually and increasingly

[57] *Carpenter*, 138 S. Ct. at 2220 (citing Riley v. California, 134 S. Ct. 2473, 2484 (2014)).

[58] *Cf. supra* note 1 (recall Justice Sotomayor's comment at oral argument in *Carpenter* that many people even carry their cell phones into their beds and public restrooms: "It's an appendage now for some people").

incorporated the technology. Also like the cell phone, these technologies are affordable, accessible, and rapidly growing in popularity.

More fundamentally, however, a technology's pervasiveness should not be a prerequisite for determining whether personal data may be involuntarily exposed. When a technology is pervasive in the digital era, the cow has already left the barn and, indeed, has flown into cyberspace. Personal data, once in cyberspace, cannot be retrieved, and can be disseminated at an exponential rate. One example is email. Because email is cloud-based, allowing constant access from any device, "there have to be redundant copies."[59] Even the trash can of deleted email is only figurative, as providers may keep copies on back-up servers.[60] Moreover, global surveillance programs may sweep in some of the many emails routed across international borders.[61]

In another example, Cambridge Analytica's data on thousands of Facebook users in Colorado is still circulating, despite the company's assurances that it had been deleted.[62] Indeed, a Cambridge Analytica spokesperson had declared that "[a]fter Facebook contacted us in December 2015 we deleted all GSR data and took appropriate steps to ensure that any copies of the data were deleted." Yet the fact that a Colorado dataset still exists, as well as a similar one on Oregonians, creates concern about what other Facebook-derived data remains in circulation.[63] As residents in Colorado were told, if "[Channel 4 News] can get a copy of [the data], users would be naive to assume that someone else can't as well."[64]

---

[59] Kevin Mitnick, *Famed Hacker Kevin Mitnick Shows You How to Go Invisible Online*, WIRED (Feb. 24, 2017), https://www.wired.com/2017/02/famed-hacker-kevin-mitnick-shows-go-invisible-online.
[60] Cora Borradaile, *What Happens to Deleted Emails?*, C.L. DEF. CTR. (Aug. 7, 2017), https://cldc.org/security/what-happens-to-deleted-emails.
[61] *Id*. (Thus, ominously, "if you didn't go to the trouble of encrypting that email, there is probably a copy of it somewhere.").
[62] *Revealed: Cambridge Analytica Data on Thousands of Facebook Users Still Not Deleted*, CHANNEL 4 NEWS (Mar. 28, 2018), https://www.channel4.com/news/revealed-cambridge-analytica-data-on-thousands-of-facebook-users-still-not-deleted.
[63] *Id.* ("The data is . . . known to have been passed around using generic, non-corporate email systems, outside of the servers of Cambridge Analytica.").
[64] *Id.*

Ordinary consumers utilize technology-based conveniences and services without fully understanding how the technologies work or the consequences of using them. Given the rapidity of technology's relentless march, a purely reactionary test requiring established pervasiveness will fail to provide needed privacy protections. For these reasons, this Article urges that the technology's pervasiveness should not be a determinant of users' privacy expectations. The examples of IoT devices and DNA testing demonstrate that privacy can be breached without pervasiveness. Instead, the third-party doctrine should employ a retrospective test examining the individual's understanding and choices. It is impossible to predict what new classes of technology have yet to emerge and the kinds of personal data that may be compromised, let alone when or how. What can be done, however, is to identify technologies susceptible to privacy violations, such as IoT devices and DNA testing. Once the technology has been so identified, the new test proposed by this Article should be applied.

Absence of affirmative sharing is the key. The absence of an affirmative act of sharing is the *Carpenter* Court's second reason for why CSLI is involuntarily exposed and therefore not encompassed by the third-party doctrine. Smart devices and private genomic testing, by design, require involuntary exposure to third parties of users' personal data. Like CSLI, both technologies "lo[g] a . . . record by dint of . . . operation, without any affirmative act on the part of the user beyond powering up."[65] Nor does the consumer have any meaningful opportunity to opt out, beyond not using the technology itself, which would mean excising oneself from mainstream, modern conveniences and popular services. This Article urges that this absence of affirmative sharing should be the crux of the third-party doctrine. *Carpenter* should apply this test to law enforcement's efforts to access any such data, just as it did with CSLI. The test should apply regardless of whether the third party is a government entity or a private party possessing information the government seeks, for the same reasons obtaining CSLI requires a warrant under *Carpenter*: the technology necessitates involuntary exposure of data without an affirmative act of sharing by the user.

[65] *Carpenter*, 138 S. Ct. at 2220.

The proposed new test—which asks first if the consumer understood that the technology necessitated the sharing of personal data with a third party, and second if the consumer had a meaningful opportunity to opt out—preserves the decisional analysis intrinsic to the third-party doctrine. Under this test, the third-party doctrine involves a retrospective test pivoting on the understanding and choices of the individual. The next Section explains why this decisional analysis should be preserved notwithstanding modern consumers' contradictory behavior on matters of personal privacy.

III. FITTING THE SQUARE PEG OF DIGITAL DATA IN THE ROUND HOLE OF THE THIRD-PARTY DOCTRINE [66]

A. Why Privacy Should Survive the Disconnect with Traditional Decisional Analysis: "We're Not in Kansas Anymore"[67]

The digital world is not a tangible place. As one scholar noted, "[p]rivacy used to be a black-and-white matter. Your information was private if you kept it to yourself, and it was not private if you provided it to others," a view that led the Court to seek bright-line rules in its Fourth Amendment jurisprudence.[68] It also led the Court to focus its reasoning on decisional privacy, and specifically "the right of individuals to make decisions free of government intervention."[69]

Carpenter revives questions about the validity of the *Katz* test in the digital age. Along with Justices Thomas and Gorsuch,[70] many have challenged its continued value. Evolving technologies change which expectations of privacy are considered "reasonable," as scholars have noted.[71] With tangible items such as pen registers, forfeiting

---

[66] *See generally* Park, *supra* note 26.
[67] WIZARD OF OZ (Warner Bros. 1939).
[68] Kevin P. McLaughlin, *Sharing You with You: Informational Privacy, Google, & the Limits of Use Limitation*, 23 ALB. L.J. SCI. & TECH. 55, 56 (2013).
[69] Jay P. Kesan et al., *A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy*, 91 IND. L.J. 267, 277 (2016).
[70] *Carpenter*, 138 S. Ct. at 2235-46 (Thomas, J., dissenting), 2261-72 (Gorsuch, J., dissenting).
[71] *See, e.g.*, Margaret Hu, *Cybersurveillance Intrusions and an Evolving* Katz *Privacy Test*, 55 AM. CRIM. L. REV. 127, 129, 139 (2018) ("The heart of this problem is that the *Katz* test does not appear to be offended by cybersurveillance tools . . . that can subject both citizens and noncitizens to mass, suspicionless, criminal, and national security profiling through the collection and analysis of comprehensive databases of personally identifiable information. And as such, the *Katz* standard

the *Katz* reasonable expectation of privacy under the third-party doctrine made sense. In *Smith*, the Supreme Court held that one has "no legitimate expectation of privacy in information he voluntarily turns over to third parties," defining the classic third-party doctrine.[72] Transferring this doctrine from pen registers to digital technology, however, poses challenges. As Justice Sotomayor expressed in her concurrence in *Jones*:

> [I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks . . . . I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection.[73]

Indeed, the issue of digital data privacy adds a challenging layer of complexity to evaluating privacy expectations. Traditional assumptions underlying scholars' debates on the expectation of privacy—about physical objects, enclosures, time, and space, involving houses, curtilage, cars, sealed letters and the like—do not translate so easily to the amorphous digital realm.[74] Unlike physical objects, "[d]ata is . . . non-terrestrial and borderless. Bits and bytes populate an alternative world. They may be held on a server, but their generation, transfer, and availability are not tied to territory, undermining

---

appears inadequate for protecting Fourth Amendment values in the context of suspicionless seizures of data and subsequent analysis of that data.").

[72] Smith v. Maryland, 442 U.S. 735, 743-44 (1979).

[73] United States v. Jones, 565 U.S. 400, 417 (2012).

[74] *See* Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1908 (2013) ("The way forward for privacy theory in the liberal tradition requires engaging with other scholarly traditions that acknowledge the emergent and relational character of subjectivity. One place to begin is with literatures in the fields of cognitive science, sociology, and social psychology, which establish empirical foundations for an understanding of subjectivity as socially constructed. These literatures . . . illuminate the various physical, spatial, and informational strategies that people deploy to manage their personal boundaries dynamically over time.").

doctrines that rely on three-dimensional space."[75] However, *Katz* presciently recognized that "the Fourth Amendment protects people, not places"[76] in striving to meet its underlying purpose of curbing excessive governmental power.[77] The concept of protecting people, not places, has never been more fitting than now, where "places" may very well be cyberspaces. The solution to the challenge of measuring the expectation of privacy should be not to abandon it, nor to abandon the *Katz* test, but to recalibrate how to gauge the presence of a subjectively and objectively reasonable expectation of privacy.

Given the new ways in which personal data may be produced, owned, or otherwise in the hands of third parties without the individual's knowledge or control, limiting the third-party doctrine to the physical landscape from which it originated turns a blind eye. The *Carpenter* dissent, by being unable to move away from the originalist perspective of privacy as property, and therefore saying that digital data does not differ from traditional business records, is bound unimaginatively to a mechanical pre-digital world. Kennedy's lament that "the Court unhinges Fourth Amendment doctrine from the property-based concepts that have long grounded the analytic framework that pertains in these cases"[78] does have a certain appeal, as Justices Thomas, Alito and Gorsuch would agree. Indeed, if one views privacy strictly from a literal property perspective, then the dissent wins. However, the majority argued that CSLI is not property in the sense that the banking records were in *Miller* or the phone numbers were in *Smith*: "At some point, the dissent should recognize that CSLI is an entirely different species of business record—something that implicates basic Fourth Amendment concerns about arbitrary government power much more directly than corporate tax or payroll ledgers."[79]

Moreover, Justice Kennedy ascribes to the average consumer a level of mastery of technology and awareness of the consequences of en-

---

[75] Laura K. Donohue, *The Fourth Amendment in a Digital World*, 71 N.Y.U. ANN. SURV. AM. L. 553, 554 (2017).
[76] Katz v. United States, 389 U.S. 347, 351 (1967).
[77] *See id.* at 357.
[78] *Carpenter*, 38 S. Ct. at 2224 (Kennedy, J., dissenting).
[79] *Id.* at 2222 (majority opinion).

gaging with it that is belied by the realities of the rapid pace of technological evolution. He argues, "Because Carpenter lacks a requisite connection to the cell-site records, he also may not claim a reasonable expectation of privacy in them. He could expect that a third party—the cell phone service provider—could use the information it collected, store, and classified as its own for a variety of business and commercial purposes."[80] However, on what basis does Kennedy conclude that Carpenter, or any lay consumer, would have had this expectation? If a consumer has this expectation about CSLI, by extension would a consumer be expected to also have this expectation about other types of digital data arising from technology that necessitates third-party control? Finally, even if a consumer has this awareness, does he or she have any meaningful choice about whether or not to use the technology? Justice Gorsuch, in his dissent, made this observation, stating, "At least some of this Court's decisions have already suggested that use of technology is functionally compelled by the demands of modern life, and in that way the way that we store data with third parties may amount to a sort of involuntary bailment too."[81]

On the other hand, while the *Carpenter* majority repudiated the dissent's test for the third-party doctrine as being based simply on whether a third party owns or has control over the CSLI,[82] simply basing the doctrine's applicability on an absence of the user's affirmative sharing of data may too broadly absolve the individual of any responsibility. As less and less data is actually shared but rather, like CSLI, simply left behind as a digital trail from having used a

[80] *Id*. at 2230 (Kennedy, J., dissenting).
[81] *Id.* at 2270 (Gorsuch, J., dissenting).
[82] Justice Kennedy disputed that a search took place at all. *Id.* at 2224 (Kennedy, J., dissenting). In his dissent, he argued that in obtaining Carpenter's CSLI, the government simply used a "compulsory process to obtain records of a business entity." *Id.* Justice Kennedy noted that "individuals have no Fourth Amendment interests in business records which are possessed, owned, and controlled by a third party. This is true even when the records contain personal and sensitive information." *Id.* at 2223 (citations omitted). He saw CSLI as "a now-common kind of business record . . . no different from the many other kinds of business records the Government has a lawful right to obtain by compulsory process," such as "bank records, telephone records, and credit card statements." *Id*. at 2224.

technology,[83] *Carpenter*'s reasoning may not leave room for any digital data to be unprotected by the third-party doctrine.

In *Carpenter*'s wake, this Article calls for an extension of the third-party doctrine in the digital era. Digital technology is an unavoidable part of living in modern society.[84] It is an inconvenient truth that society itself is struggling to understand this technology—what kinds of data are being distributed, how and to whom, and how respond to that understanding—even as it embraces the technology's wizardry. This should not translate, however, to render the notion of an expectation of privacy obsolete. Nor should all data necessarily be protected by the third-party doctrine merely because, as in *Carpenter*, the consumer did not affirmatively share the data. A gap may exist between the everyday consumer's handling of technology and the desire to maintain privacy; this, however, should leave the individual neither less nor more protected under the Fourth Amendment. The rapid, continuous emergence of technologies that has thus far outpaced society's ability to respond may very well continue for the foreseeable future, as we leave the mechanical world behind and become immersed in an increasingly digital world. However, the expectation of privacy cannot simply be dispensed with merely because digital data is a square peg in the round hole of the third-party doctrine. Courts should adapt the decisional privacy upon which the doctrine is predicated in circumstances in which the technology does not afford the consumer an ability to decide, while preventing a strict reading of the doctrine from indiscriminately protecting all digital technology use.

Some scholars have thoughtfully suggested an alternate framework in which the third party's role is more closely scrutinized: differentiating between an intermediary and a direct participant.[85] Others

---

[83] *Id.* at 2220 ("[A] cell phone logs a cell-site record by dint of its operation, without any affirmative act on the part of the user beyond powering up. Virtually any activity on the phone generates CSLI . . . . Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data.").

[84] *See* Donohue, *supra* note 75, at 554 ("Digital information is ubiquitous. Individuals cannot go about their daily lives without generating a footprint of nearly everything they do. The resulting data is accessible, recordable, and analyzable. And because it is digital, it can be combined with myriad sources, yielding deeper insight into our lives.").

[85] Ormerod & Trautman, *supra* note 8, at 141.

have already suggested maintaining Fourth Amendment protection for smart devices by redefining "effects" to include "digital curtilage."[86] Yet another suggestion is to create an exclusion framework that presumes an objective unreasonableness in any warrantless penetration by the state into the smart home.[87]

This Article proposes instead that the focus continue to remain on the decision-maker, consistent with the *Katz* tradition. Given the absence of an affirmative act of sharing personal data with a third party, an extended test that inquires whether the consumer understood that the technology's very design necessitated a third party, and, if so, whether the consumer had a meaningful opportunity to avoid sharing data with that third party, allows for balance between strict decisional jurisprudence and the reality that the digital world is Oz, and not Kansas anymore.[88] The Sections that follow offer reasons for consumers' seemingly contradictory, yet ultimately consistent, behavior.

B. Consumers' Contradictory Behavior: An Explanation

The current state of scholarship about society's expectation of privacy is as convoluted as the cyber-landscape it attempts to describe. Scholars disagree as to whether the digitally-driven are acutely aware of privacy risks, lack basic information/awareness, or are indifferent.

One scholar notes the difference between "digital natives" who are both more active on social media sites and "more active in managing their online reputation than older users,"[89] versus "'digital immigrants,' i.e., those who have had to assimilate to a post-World Wide Web universe."[90] Researchers have found that active social media users between the ages of 18 and 29 are more likely to update their

---

[86] See, e.g., Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L.R. 805, 864 (2016).
[87] Stefan Ducich, *These Walls Can Talk! Securing Digital Privacy in the Smart Home Under the Fourth Amendment*, 16 DUKE L. & TECH. REV. 278, 280, 299 (2018).
[88] WIZARD OF OZ (Warner Bros. 1939).
[89] Mary Graw Leary, *Reasonable Expectations of Privacy for Youth in a Digital Age*, 80 MISS. L.J. 1033, 1044-45 (2011).
[90] *Id.* at 1039.

profiles and carefully curate their online image.[91] Knowing that privacy risks loom raises the question "why people, particularly young people, compromise their privacy so extensively through social networking sites."[92]

Another scholar observes that risky privacy behavior may be particularly common among "social network users . . . of certain generations," who simultaneously "expect that their information will remain within the network and not be seen by the vast potential audience."[93] The author noted that students in one survey were described as "'technologically savvy, yet somewhat dismissive of potential risks online," because they "believed that they had taken appropriate steps to keep their information within their own set of friends or contacts."[94]

In contrast to the students who may imagine themselves to be more empowered over technology than warranted, another survey observes that consumers may be aware of privacy compromises, but feel a "sense of helplessness . . . with regard to agreements that they must accept in order to use a service."[95] In the same study, the authors also observe that other consumers are unaware of how much personal information they give away on the Internet, or even that they are revealing information that can be tracked.[96] The authors note that "potentially millions of consumers have inadequate knowledge to make meaningful choices about how their data is used online."[97]

Yet another scholar suggests that "privacy-sensitive individuals" are a "relatively small share," and that many consumers are only motivated to demonstrate concern about privacy when faced with economic consequences.[98]

---

[91] *Id.* at 1046.
[92] *Id.* at 1047.
[93] Steven D. Zansberg & Janna K. Fischer, *Privacy Expectations in Online Social Media—An Emerging Generational Divide?*, 28 COMM. LAW. 1, 29 (2011).
[94] *Id.*
[95] Kesan *et al.*, *supra* note 69, at 271.
[96] *Id.* at 293, 294.
[97] *Id.* at 342.
[98] Alan McQuinn, *The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules*, INFO. TECH. & INNOVATION FOUND. (Oct. 6, 2017), https://itif.org/publica-

This Article takes an alternate position: all of the above observations are true. While seemingly contradictory, these patterns are cohesive in the digital realm. Because traditional Fourth Amendment jurisprudence has been concerned with tangible features and treatment of physical objects, false conclusions can be drawn when rigidly applying those standards to consumers in the cryptic world of digital data. Consumers' seemingly careless handling of personal information that may be disclosed as they use digital technology, in contrast to their handling of traditional "persons, houses, papers and effects,"[99] defies easy categorization as a rejection of privacy, despite the appeal of doing so in order to fit traditional privacy analysis.

This Article seeks to demonstrate that digital device users actually do care—a lot—about personal privacy, and offers two reasons despite behavior to the contrary. As an initial matter, when a new technology becomes commonly used, apprehension tends to be replaced by ambivalence, acceptance, and eventually enthusiasm as society becomes accustomed to its conveniences, and the underlying risks do not materialize. Additionally, the social mandate to interact through digital media creates pressure to share information that belies the underlying desire to maintain individual privacy.

1. Dissociative appeal dilutes apprehension

When the world was mechanical, it was easier to understand how tools and machines operated. In our digital world, common sense and observation skills are no longer as helpful to gain insight into the workings of services and devices. Most of us would have difficulty explaining how many of the devices we use daily actually work, starting with cell phones. Despite this cognitive dissociation, we are drawn in by the convenience offered. "Dissociative appeal"

---

tions/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules ("In short, consumers care about prices when they make privacy-related decisions. The reason why public opinion polls show such support for strong privacy laws is because these surveys rarely confront consumers with the price consequences of their choices.").

[99] U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

in this Article refers to this phenomenon of finding devices or services appealing despite limited understanding of the technology and expectations for individual control.

Dissociative appeal is evident in consumers' idealistic attitudes towards digital privacy, at least as they existed before the Cambridge Analytica scandal.[100] Users may have a false sense of security rooted in online anonymity and may fail to realize that they are revealing personal information.[101] Thus, they are likely to overestimate the law's privacy protections.[102] Even when Internet users are concerned about their online privacy and security, they still engage in risky online behaviors.[103] While one explanation of this phenomenon is that these users are carefully weighing the costs and benefits of using a service, "[a]nother possible explanation is that the consumers do not know enough to make meaningful decisions about their online privacy."[104]

Behavioral economics, too, may induce a state of denial. Thus, even the IoT user who understands the networking technology intrinsic to smart devices may possess "unrealistic optimism" that "he is less likely than the average person to experience harm from data loss."[105] A consumer also may disregard the risk because of lacking meaningful choice: "[M]aybe consumers know enough but feel helpless to make a decision that differs from what companies are willing to offer."[106] Indeed, because consumers continue to use technologies that may harm their online privacy and security, companies have little reason to offer meaningful alternatives.[107]

In some cases, the privacy risks of technological features are initially not recognized. By the time they are, society becomes accustomed to them. One example is cookies, "a small piece of code"

---

[100] *See infra* text accompanying note 267.
[101] Kesan et al., *supra* note 69, at 293-94.
[102] *Id.* at 343.
[103] *See* Melissa W. Bailey, *Seduction by Technology: Why Consumers Opt Out of Privacy by Buying Into the Internet of Things*, 94 TEX. L. REV. 1023, 1024, 1036 (2016).
[104] Kesan et al., *supra* note 69, at 343.
[105] Bailey, *supra* note 103, at 1024.
[106] Kesan et al., *supra* note 69, at 343.
[107] *Id.* at 267.

placed on one's computer when visiting a website that enables a company to track information about the visitor, which "were used for so long before anybody understood how they worked that they are now an integral part of contemporary e-commerce."[108]

Even when privacy risks are recognized from the moment of a technology's introduction, familiarity eventually leads to desensitization of those concerns. An early example of a technology met with resistance is caller ID, initially seen as a violation of the caller's privacy; today, many people will not answer calls from unknown numbers.[109] Thus, "[w]hat was initially considered a privacy violation is now considered a privacy-enhancing technology."[110]

Google Street View is another technological feature that has become an accepted modern tool, despite the fact that it shows images of people and homes without giving notice or asking for consent.[111] Therefore, "[a]t least in some cases, even the most avid privacy advocate might concede that the public has accepted [these as] social norms."[112]

Accepting technology and potential privacy compromises as a norm, even when consumers harbor apprehensions, offers one explanation for consumers' contradictory behavior. Social mandate, discussed next, is another.

2. Social mandate contributes to an illusion of indifference

Digital technologies have become a necessary part of functioning in modern society, including cell phones and the CSLI they produce, as *Riley* and *Carpenter* recognized.[113] Even if one tries to avoid the

---

[108] Derek S. Witte, *Bleeding Data in a Pool of Sharks: The Anathema of Privacy in a World of Digital Sharing and Electronic Discovery*, 64 S.C. L. REV. 717, 731-33 (2013).
[109] *See* Omer Tene & Jules Polonetsky, *A Theory of Creepy: Technology, Privacy and Shifting Social Norms*, 16 YALE J.L. & TECH. 59, 72-73 (2013).
[110] *Id.*
[111] *See* Tal Z. Zarsky, *The Privacy-Innovation Conundrum*, 19 LEWIS & CLARK L. REV. 115, 152-53 (2015).
[112] *Id.*
[113] *See Carpenter*, 138 S. Ct. at 2220 (citing Riley v. California, 134 S.Ct. 2473, 2484 (2014); *see also* Donohue, *supra* note 75, at 554 ("It has become a non-option to eschew the digital world, if one wants to live in the modern age."); *see*

technology, it is increasingly difficult in a society where basic activities like making purchases, scheduling appointments, checking your bank account, and receiving delivery-date updates require going online.

Social media provides a salient example of the illusion of indifference to personal privacy. Entire generations are growing up accustomed to sharing their private lives on social media, with an abundant and ever-growing choice of platforms for disclosing and discussing one's whereabouts, activities, and thoughts. Much literature has already been dedicated to society's voracious appetite for social networking, particularly among youth and young adults.[114] Younger users in particular are developing different social norms as they use social networking sites to share their lives and communicate with others.[115] Tacit awareness of the privacy implications of posting pictures or information is likely subsumed by peer pressure and a general inclination to engage in risky behavior.[116] At the same time, teenagers and young adults demonstrate skillfulness at modifying their profile and managing their online reputations.[117]

This savvy suggests that the desire to maintain privacy is not necessarily at odds with the greater willingness to share private information online. The willingness to share information is a reflection of the social media-driven landscape in which the number of "likes," "followers" and "friends" is what matters, while knowing that parents, recruiters, or employers may also have access to one's posts. Teenagers may use fake profiles, names, ages, and "a cloud of other minor lies to keep their profiles safe from prying (usually parental) eyes while also connecting with their peers," and those applying to

---

also Park, *supra* note 13, at 463 ("The cell phone arguably has become an omnipresent and potent force in American communication.").

[114] *See, e.g.*, Leary, *supra* note 89.

[115] *Id.* at 1038.

[116] *See, e.g.,* Devin W. Ness, *Information Overload: Why Omnipresent Technology and the Rise of Big Data Shouldn't Spell the End for Privacy as We Know It*, 31 CARDOZO ARTS & ENT. L.J. 925, 954-55 (2013); *see also* Leary, *supra* note 89, at 1045.

[117] *See, e.g.*, Leary, *supra* note 89, at 1044.

college may use these fake names to escape the scrutiny of admissions officers.[118] Meanwhile, "college students coming back from a night of partying have learned that the first thing they need to do is check Facebook and untag their names from any photos of them doing keg stands, lest their athletic coaches or campus police catch them drinking."[119] Efforts to edit online profiles demonstrate sensitivity to privacy issues and a desire to maintain personal boundaries. Students may also be assuming that the steps they have taken ensure more privacy than they actually do, contributing to their active online presence.[120]

Thus, the social mandate to interact through digital media creates an illusion of indifference to personal privacy, when in fact the expectation of privacy remains intact. This expectation of privacy was the starting point for *Katz*. The next section applies the proposed extended test for the third-party doctrine, which takes into account both the *Katz* tradition and the digital era's realities with its two-part inquiry as to whether the consumer understood that the technology's design necessitated a third party, and, if so, whether the consumer had a meaningful opportunity to avoid sharing data, to two technologies currently surging in popularity: smart devices and genomic testing.

IV. THE NEW TEST APPLIED: PERSONAL DATA OF SMART DEVICES AND DNA TESTING

Given that consumer behavior may superficially be at odds with a desire to maintain privacy, this Article now focuses on two examples of affordable, accessible, and increasingly popular technologies to provide a concrete platform for applying the proposed post-*Carpenter* third-party doctrine. Smart technology and private genomic testing both send the user's data to a third party as a necessary incidental to using the device or service. Like the CSLI that users create simply by using a cell phone, the personal data shared by virtue of using these technologies and services, despite the absence of any

---

[118] Ken Strutin, *Social Networking and the Law: Social Media and the Vanishing points of Ethical and Constitutional Boundaries*, 31 PACE L. REV. 228, 248-49 (2011).
[119] *Id*. (citations omitted).
[120] *See* Zansberg & Fischer, *supra* note 93, at 29.

affirmative act, is a phenomenon not well understood by most consumers. Moreover, this personal data has already proven to be a commodity highly sought after by law enforcement in certain circumstances. Finally, no meaningful alternatives or opportunities exist to opt out of the arrangement. The following Sections examine how smart devices and private genomic testing services intrinsically create third parties and, accordingly, opportunities for the kind of "involuntary exposure" that led the *Carpenter* court to conclude that obtaining CSLI required a warrant.

C. Smart Technology: Wearable and Voice-Activated

1. IoT devices necessitate a third party, but not necessarily consumer awareness

As "smart" devices[121] grow in popularity, many consumers may not yet understand the technology behind the convenience and assistance these devices offer. Consumers have been described as "seduced" by these technologies, with little knowledge of how the technology works.[122] Frequently, little or no information is even available about the privacy policies of various IoT manufacturers, even for the motivated consumer who attempts to investigate them.[123]

---

[121] TECHOPEDIA, *supra* note 5 ("Smart devices are interactive electronic gadgets that understand simple commands sent by users and help in daily activities. Some of the most commonly used smart devices are smartphones, tablets, phablets, smartwatches, smart glasses and other personal electronics. While many smart devices are small, portable personal electronics, they are in fact defined by their ability to connect to a network to share and interact remotely. Many TV sets and refrigerators are also therefore considered smart devices.").

[122] *See* Bailey, *supra* note 103.

[123] Scott R. Peppet, *Regulating the Internet of Things: First Steps Toward Managing Discrimination, Privacy, Security, and Consent*, 93 TEX. L. REV. 85, 140-42 (2014) ("Internet of Things devices are often small, screenless, and lacking an input mechanism such as a keyboard or touch screen . . . . The basic mechanism of notice and choice—to display and seek agreement to a privacy policy—can therefore be awkward in this context because the devices in question do not facilitate consent. This inherently complicates notice and choice for the Internet of Things. For example, even an interested consumer seeking privacy information about iHealth products and sensor data is led in an unending circle of confusion. This is a horrendous example of how not to provide consumers with clear notice and choice about privacy information.").

Smart devices rely upon autonomous relaying of personal data and the ability to connect and interface with a network.[124] These devices communicate with the network by sending data across it and using that data in their operations.[125] Such devices include conveniences such as smart light bulbs that "can be programmed so that when my boss sen[ds] me a text message, they all turn red";[126] a smart mattress cover that starts one's Bluetooth- or WiFi-enabled coffee maker upon waking in the morning;[127] and smart refrigerators that enable an app to view their contents in case doubt strikes mid-grocery shopping.[128]

Two major categories are wearable and voice-activated technology. Wearable devices, "equipped with microchips, sensors, and wireless communication capabilities . . . can collect data, track activities, and customize experiences to users' needs and desires."[129] Highly sensitive information from smart devices can also include "browsing habits to purchasing patterns to real-time location to personal health information."[130]

Perhaps even more sensitive is the subset of wearable devices that monitors consumers' health information, with a popular example being the Fitbit.[131] Such devices can "measur[e] heart rate, stress level, brain activity, respiration, and body temperature, among other data."[132] Therefore, people now routinely share large quantities of this data with third-party companies.[133]

---

[124] TECHOPEDIA, *supra* note 5; *Data Privacy in the Age of IoT*, TRENDMICRO (Mar. 8, 2016), https://blog.trendmicro.com/data-privacy-age-iot.
[125] *See* Bailey, *supra* note 103, at 1024, 1028.
[126] Stacey Higginbotham, *The Future is Now: Welcome to my (Smart) House*, FORTUNE (Feb. 17, 2017), http://fortune.com/2017/02/17/smart-home-tech-internet-of-things-connected-home.
[127] Robinson, *supra* note 6.
[128] *See, e.g.*, Renée Lynn Midrack, *What is a Smart Refrigerator?*, LIFEWIRE (Apr. 16, 2018), https://www.lifewire.com/smart-refrigerator-4158327 (A smart fridge will allow you to "[u]se interior cameras while at the store to double-check if you're low on milk or eggs").
[129] Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns Without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, at *1 (2015).
[130] *Data Privacy in the Age of IoT*, *supra* note 124.
[131] Thierer, *supra* note 129, at *18.
[132] Grant Arnow, *Note: Apple Watch-ing You: Why Wearable Technology Should Be Federally Regulated*, 49 LOY. L.A. L. REV. 607, 608 (Fall 2016).
[133] Ormerod & Trautman, *supra* note 8, at 148.

In recognition of the cybersecurity risks for medical device users, the Food and Drug Administration (FDA) has issued proposed guidelines for comment and review by industry and FDA staff.[134] These guidelines are "intended to provide recommendations to industry regarding cybersecurity device design, labeling, and the documentation that FDA recommends be included in premarket submissions for devices with cybersecurity risk."[135] The FDA ominously describes its concerns:

> The need for effective cybersecurity to ensure medical device functionality and safety has become more important with the increasing use of wireless, Internet- and network-connected devices, portable media (e.g., USB or CD), and the frequent electronic exchange of medical device-related health information. In addition, cybersecurity threats to the healthcare sector have become more frequent, more severe, and more clinically impactful. Cybersecurity incidents have rendered medical devices and hospital networks inoperable, disrupting the delivery of patient care across healthcare facilities in the U.S. and globally. Such cyberattacks and exploits can delay diagnoses and/or treatment and may lead to patient harm.[136]

The 24-page document defines two "tiers" of devices according to their cybersecurity risk level.[137] The draft proposes general principles and risk assessment, presents protocols for designing a "trustworthy device," suggests labeling recommendations for devices with cybersecurity risks, and makes recommendations for documentation of design and risk management efforts based on whether the device is Tier 1 or Tier 2.[138] The proposed guidelines, however, have received a "wary welcome," because "there is concern the guidance

---

[134] *Content of Premarket Submissions for Management of Cybersecurity in Medical Devices: Draft Guidance for Industry and Food and Drug Administration Staff*, FOOD & DRUG ADMIN. (Oct. 18, 2018), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM623529.pdf.
[135] *Id.* at 4.
[136] *Id.*
[137] *Id.* at 10.
[138] *Id.* at 8, 11, 18, 21, 22.

could add more confusion than clarity for device makers."[139] One concern is that "the guidance could be viewed as suggesting rapid changes and patches aimed at cyber resilience, although a patient's experience includes not incurring many changes to their invasive medical devices."[140] With implanted medical devices in particular, "[it]s not as easy as updating your PC."[141] Another cause for uncertainty is the lag time between research and development and bringing devices to the consumer market. Devices are a few years old when they come on the market, so the standards used in their design may no longer align with contemporary mores.[142] In the meantime, the public comment period is scheduled to end in March 2019.[143]

The second major category of smart technology, voice-activated devices, includes Amazon's Alexa, Apple's Siri, Microsoft's Cortana, and the Google Assistant, which all use voice control to provide various kinds of digital assistance.[144] These "ambient sound capture and assistive technologies" create an "invasive cache of data retained by a third-party business . . . [that] can record an untold amount of information about the interior of a home—records that could be construed as third-party business records."[145]

While consumers may perceive these as fun, modern gadgets, the networking that is integral to these devices' functions means they are not simply traditional, static devices. IoT devices also provide a continuous service due to their personalized data collection and constant communication with cloud-based service providers: "[W]ithout Alexa Voice Service, an Amazon Echo is merely an expensive doorstop. As a result, instead of an association that ends with the

---

[139] Victoria Hudgins, *FDA's New Cybersecurity Guidance for Medical Devices Receives Wary Welcome*, LAW.COM: LEGALTECH NEWS (Nov. 9, 2018, 12:00 PM), https://www.law.com/legaltechnews/2018/11/09/fdas-new-cybersecurity-guidance-for-medical-devices-receives-wary-welcome.
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*
[144] *See, e.g.*, Eric Boughman et al., *"Alexa, Do You Have Rights?": Legal Issues Posed by Voice-Controlled Devices and the Data They Create*, 2017 BUS. L. TODAY 1, 1 (July 2017), https://businesslawtoday.org/2017/07/alexa-do-you-have-rights-legal-issues-posed-by-voice-controlled-devices-and-the-data-they-create.
[145] Ormerod & Trautman, *supra* note 8, at 147-48.

purchase of an item, consumers now enter into in [sic] an ongoing relationship with IoT companies."[146]

Case in point: Apple's letter. The latent awareness that a cache of users' personal data may be created by these devices and then stored by IoT companies triggered an informal congressional inquiry. In July 2018, the House Energy and Commerce Committee sent a letter to Apple CEO Tim Cook and Alphabet CEO Larry Page "to probe the companies' representation of third-party access to consumer data, and the collection and use of audio recording data as well as location information via iPhone and Android devices."[147] Both letters also questioned whether the devices can collect "non-triggered" audio data, noting that "it has . . . been suggested that third party applications have access to and use this 'non-triggered' data without disclosure to users."[148]

The first part of Apple's August 2018 response appeared reassuring. Timothy Powderly, Apple's director of federal government affairs, asserted, "We believe privacy is a fundamental human right and purposely design our products and services to minimize our collection of customer data. When we do collect data, we're transparent about it and work to disassociate it from the user."[149] The letter explains that the iPhone does not listen to consumers, except to respond to locally stored, short buffers "that only wake up Siri if there's a high probability that what it hears is the 'Hey, Siri' cue."[150] Once Siri wakes up, actual recording takes place, attached to an anonymous

---

[146] Rebecca Crootof, *Introducing the Internet of Torts*, BALKINIZATION (July 24, 2018), https://balkin.blogspot.com/2018/07/introducing-internet-of-torts.html.
[147] *E&C Leaders Press Apple and Google on Third-Party Access, Audio and Location Data Collection*, HOUSE COMMITTEE ON ENERGY & COM. (July 9, 2018), https://energycommerce.house.gov/news/press-release/ec-leaders-press-apple-and-google-on-third-party-access-audio-and-location-data-collection.
[148] *Id.*
[149] Lisa Vaas, *Siri Is Listening to You but She's NOT Spying, Says Apple*, NAKED SECURITY (Aug. 13, 2018), https://nakedsecurity.sophos.com/2018/08/13/siri-is-listening-to-you-but-shes-not-spying-says-apple; *see also* Letter from Timothy Powderly, Dir. of Fed. Gov't Affairs, Apple, to Greg Walden, Chairman, House Comm. on Energy and Commerce (Aug. 7, 2018), https://www.scribd.com/document/385685064/Apple-Response-to-July-9-Letter [hereinafter Apple Letter].
[150] Vaas, *supra* note 149.

identification number that is not tied to an individual's Apple ID.[151] As for the privacy implications of those recordings, "Siri utterances are sent to Apple and handled in accordance with Apple's Privacy Policy. Users have control over the random device identifier associated with Siri utterances, which can be reset at any time . . . . When the identifier is reset, Apple deletes information it stores that is associated with the identifier."[152]

However, the latter part of Apple's letter confirms the necessity of a third-party service provider in order for Siri to work. When actual audio recording is taking place, an iOS device provides the user a visual indicator with the words, "What can I help you with?"[153] Apple's Developer Guidelines require that developers of third-party apps display this visual indicator when their app is collecting audio information from the microphone—i.e., when Siri is listening.[154]

Visual indicator aside, microphone data is then collected by the third-party app that the customer has chosen to download to his or her Apple device. At that point, "the customer and app developer enter into a direct contractual relationship with one another . . . . Apple is not a party to these relationships; rather, developers are fully responsible for the content and services they provide in their apps."[155] Apple itself states, "Apple does not and cannot monitor what developers do with the customer data they have collected, or prevent the onward transfer of that data, nor do we have the ability to ensure a developer's compliance with their own privacy policies or local law." Apple does offer that when it has "credible information that developer is not acting in accordance with the PLA or

---

[151] Apple Letter, *supra* note 149, at 8 ("Siri utterances, which include the audio trigger and the remainder of the Siri command, are tied to a random device identifier, not a user's Apple ID."); *see also* Vaas, *supra* note 149 (However, "[s]imilar services store voice recordings in ways that are associated with an individual user, Apple said. In other words, in ways that can be linked to an individual who can then be target-marketed").
[152] Apple Letter, *supra* note 149, at 8.
[153] *Id.* at 9, 13; *see also* Vaas, *supra* note 149.
[154] Apple Letter, *supra* note 149, at 10; *see also* Vaas, *supra* note 149.
[155] Apple letter, *supra* note 149, at 13.

App Store Review Guidelines or otherwise violates privacy laws, we will investigate to the extent possible."[156]

Apple's letter attempts to assure that "consistent with Apple's view that privacy is a fundamental human right, we impose significant privacy-related restrictions on apps."[157] Thus, despite "the developer's responsibilities and direct relationship with customers, Apple requires developers to adhere to privacy principles."[158] Notwithstanding this reassurance, it is apparent that "at a certain point, what happens to user data comes down to whatever a user has signed off on when agreeing to an app's terms."[159]

As an initial matter, Apple's letter seems to assume that the typical user understands that the "visual indicator" means that a third party is now collecting, and possibly storing, microphone data. More fundamentally, Apple's attempt at reassurance actually confirms the Energy and Commerce Committee's fear that third parties indeed must access this data for the technology to function. Disturbingly, it also confirms that even Apple itself does not control whether app developers will comply with privacy policies or agreements.

Other potential third parties. Not only do all smart devices require an initial third party who holds the user's personal data, but other third parties can seek this data, including law enforcement. Law enforcement has already successfully obtained such personal information in pursuing criminal investigations.[160] In *Carpenter*'s wake,

---

[156] Vaas, *supra* note 149 ("In other words, Apple does its damnedest to make sure iPhones aren't eavesdropping on us, including through privacy policies, short buffer windows, local storage, and app review.").
[157] Apple Letter, *supra* note 149, at 13.
[158] *Id*.
[159] Vaas, *supra* note 149.
[160] Law enforcement has conducted investigations based on contradictions between defendants' stories and information recorded by smart devices. For example, in 2015, Richard Dabate told police that a masked intruder assaulted him and killed his wife in their Connecticut home. *See* Rory Carroll, *Inspector Gadget: How Smart Devices Are Outsmarting Criminals*, GUARDIAN (June 23, 2017, 5:00 AM), https://www.theguardian.com/technology/2017/jun/23/smart-devices-solve-crime-murder-internet-of-things. Police obtained a warrant to investigate the couple's digital data. *See* Adam Janos, *If Google Can Have Your Data, Can Police Investigating Crimes Have It Too?*, A&E: REAL CRIME (Apr. 23, 2018), https://www.aetv.com/real-crime/smart-wearable-home-technology-apps-data-solving-crimes. The data found on the wife's Fitbit contradicted the defendant's timeline of events, and he has been charged with murder. *See* Carroll, *supra*. Also

law enforcement would be well-advised to obtain a warrant to investigate in-car smart apps "that contain sensitive information, such as navigation apps that contain travel history,"[161] in Terry stops—brief warrantless detentions that are exceptions to the requirements for standard physical searches.

In addition to law enforcement, other potential third parties are the "data brokers" to whom IoT companies may choose to sell data.[162] Google and Target, for example, create targeted advertising and goods based on user data.[163] Car manufacturers, meanwhile, have begun gathering the sensitive data generated by vehicles' onboard sensors and computers, storing it in cloud-based servers, and using it "to craft targeted in-car advertisements or sell [the data] to mapping firms looking to provide more accurate traffic information."[164]

---

that year, James Bates claimed an acquaintance who went to his Arkansas home to watch a football game had accidentally drowned in his hot tub. *Id*. Bates, however, "had several internet-connected devices, including a Nest thermostat and Amazon Echo, which responds to voice commands and streams audio to the cloud, including a fraction of a second of audio before its 'wake word'. . . . Amazon initially resisted a police request for Echo data, citing the First Amendment, but relented after Bates approved the handover." *Id.* Bates has been charged with murder. *Id.* Ross Compton told investigators in 2016 that he woke up to find his Ohio home on fire and climbed through a window to escape the flames, but investigators pulled data from his pacemaker which a cardiologist found undermined Compton's account. Compton was charged with arson and insurance fraud. *Id*.; *see also* Meagan Flynn, *Police Think Alexa May Have Witnessed a New Hampshire Double Homicide. Now They Want Amazon to Turn Her Over*, WASH. POST (Nov. 14, 2018), https://www.washingtonpost.com/nation/2018/11/14/police-think-alexa-may-have-witnessed-new-hampshire-double-slaying-now-they-want-amazon-turn-her-over ("[A]n Amazon spokesman indicated that Amazon wouldn't be turning over the data so easily, appearing to prioritize consumer privacy as it has done in the past.").

[161] *See* Daniel Castro & Alan McQuinn, *Congress Should Close the Loophole Allowing Warrantless Digital Car Searches*, TECH CRUNCH (Feb. 25, 2018), https://techcrunch.com/2018/02/25/congress-should-close-the-loophole-allowing-warrantless-digital-car-searches.

[162] Bailey, *supra* note 103, at 1025 (defining "data brokers" as "entities that aggregate consumer profiles that 'may reveal where consumers live; how much they earn; and their race, health conditions, and interests'") (citations omitted).

[163] *Id.*

[164] Christina Rogers, *What Your Car Knows About You; Auto Makers Are Figuring Out How to Monetize Drivers' Data*, WALL ST. J. (Aug. 18, 2018), https://www.wsj.com/articles/what-your-car-knows-about-you-1534564861.

Finally, a prominent risk is that the technology can be hacked.[165] Hackers can use numerous methods to break into and share data from these devices. Moreover, "[t]he more information they can transfer, the more valuable it becomes, making this type of hijacking ever more tempting."[166] Hackers, for example, "have demonstrated a capability to compromise IoT devices and have broken into online video cameras and baby monitors."[167] Wearable technology may be of particular concern, because it "creates a personalized data profile, recording continuous logs of consumer activity levels through bio-medical feedback."[168] This data, which "provides priceless insight to marketers, advertisers, retailers, insurers, employers, financial service providers, and social contacts," is stored within vulnerable and unregulated network systems.[169] One survey points specifically to lack of awareness of the possible risks associated with collecting health data with wearable devices.[170]

Anecdotes abound of consumers shocked by the experience of devices being hacked. Parents have realized a man was talking to their child through their smart baby monitor. [171] Home security systems have been breached.[172] In a more light-hearted but nonetheless telling example, "plenty of viewers complained that [a] TV broadcast

---

[165] *See Data Privacy in the Age of IoT*, *supra* note 124 ("Because a host of convenient smart devices now continuously gather, process, and send data to make our lives more convenient, they have also magnified the threats to data privacy. You just have to look at all the connected devices around us to see a simple dilemma: our ability to collect and process data has overwhelmed our ability to protect that information.").
[166] *Data Privacy in the Age of IoT*, *supra* note 124.
[167] Bailey, *supra* note 103, at 1025.
[168] Arnow, *supra* note 132, at 614-15.
[169] *Id.*
[170] Tegan Ayers, *Self-Regulation Within the Wearable Device Industry and the Alignment to Device Users' Perceptions of Health Data Privacy* (May 2018) (unpublished master's thesis, Rochester Institute of Technology), https://scholarworks.rit.edu/cgi/viewcontent.cgi?article=10913&context=theses; *see also* Arnow, *supra* note 132, at 615 ("Consumers are generally clueless about the range of information that wearable devices record.").
[171] Healthline, *Parental Warning: Your Baby Monitor Can Be Hacked*, HUFFPOST (Aug. 24, 2017), https://www.huffpost.com/entry/parental-warning-your-bab_b_11668882.
[172] Kenneth Amaro, *Wireless Camera Hacking Leaves St. Augustine Family Feeling Unsecure*, FIRST COAST NEWS (Jan. 10, 2017), https://www.firstcoastnews.com/article/news/wireless-camera-hacking-leaves-st-augustine-family-feeling-unsecure/384901995.

caused their voice-controlled personal assistants to try to place orders for dollhouses on Amazon" after a San Diego reporter concluded a television broadcast about a six year-old in Dallas who had asked the family's Echo to get her a dollhouse, with the remark, "I love the little girl, saying Alexa order me a dollhouse."[173]

The shock consumers express when their privacy has been breached in these ways demonstrates the phenomena of dissociative appeal and social mandate. Consumers are eager to adopt smart technologies, but typically lack awareness that the devices are actually networked computer systems,[174] let alone the specific understanding that a third party may exercise control over their personal data.

2. IoT devices lack meaningful ability to opt out

Moreover, even if consumers are aware that by utilizing a digital device they have shared information with a third party, and even if they understand that a device manufacturer such as Apple disavows any control over whether the third party respects consumer privacy, these consumers have no meaningful alternatives or opportunity to disengage.

Although Apple's letter assumes that consumers will pay attention to privacy agreements that third-party apps offer, it is "generally accepted that people do not read TOS or privacy policies, which is understandable considering that most of these documents span several pages and are often written in unwieldy 'legalese.'"[175]

---

[173] Shaun Nichols, *TV Anchor Says Live On-Air 'Alexa Order Me A Doll House—Guess What Happens Next*, REGISTER (Jan. 7, 2017, 12:58 AM), https://www.theregister.co.uk/2017/01/07/tv_anchor_says_alexa_buy_me_a_dollhouse_and_she_does; *see also* Andrew Liptak, *Amazon's Alexa Started Ordering People Dollhouses After Hearing Its Name on TV*, VERGE (Jan. 17, 2017), https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse.

[174] *See also* Bailey, *supra* note 103, at 1023-24 ("The reaction to Superfish stands in stark contrast to consumers' everyday privacy-sacrificing behaviors."). Superfish was a software preloaded onto Lenovo's computers that tracked consumers' online movements without their full knowledge of consent. *Id.* This Article suggests that the apparent contrast between consumers' reaction upon realizing their privacy has been breached and the everyday privacy-sacrificing behaviors is actually behaviorally consistent, because consumers generally do not recognize, as an initial matter, that a third party can access their data at all.

[175] Kesan, *supra* note 69, at 288.

In a survey of 287 wearable device users, 213 said they had never read a privacy policy, and of those, 87 percent "cited reasons that indicate a failure on the part of the privacy policy maker." Specifically, people feel that the policies are "too long or too difficult to understand", or somewhat concerningly, that they are "unable to change *any* of their privacy settings so, reading the policy is pointless."[176]

Thus, consumers feel a sense of helplessness when faced with agreements they must accept before using services and products: "One of the self-reported reasons that participants gave for not reading privacy policies was that it would not make a difference whether they read the policy or not."[177]

Finally, scholars have noted that nothing under the current U.S. law provides individuals with a "way to review the personal information that the dominant digital assistant collected about them," nor does current U.S. law give them a "way to revoke their consent and refuse the further use or collection of personal information, or to delete already-retained personal information."[178]

In sum, consumers are eager to embrace convenient, helpful technologies, yet generally lack a technological understanding of how IoT devices work and the ways in which their privacy can be breached by utilizing the devices. Even consumers with awareness of potential privacy breaches may agree to privacy policies simply

---

[176] Ayers, *supra* note 170, at 26, 46.

[177] Kesan, *supra* note 69, at 271 ("[C]onsumers often do not seem to be making a meaningful choice when agreeing to a website's terms and submitting information online."). In part, consumers may "believe that the benefits of using the service outweigh the downsides of using the service. Or they may believe that the benefits from using the service are greater than the benefits from not using the service." *Id.* at 343. Not only do consumers feel they have no choice about accepting service terms, but they often feel compelled to provide personal information in order to utilize an online service. The results of the same survey show that "[o]ver 80% of our survey participants . . . indicated that on some occasion they have submitted information online when they wished that they did not have to do so." *Id.* at 267.

[178] Maurice E. Stucke & Ariel Ezrachi, *How Digital Assistants Can Harm Our Economy, Privacy, and Democracy*, 32 BERKELEY TECH. L.J. 1239, 1284 (2017).

because they do not feel a meaningful choice actually exists. A similar pattern can be seen with private DNA and genetic testing companies, the subject of the next Section.

D. Private DNA and Genetic Testing Companies

1. Private DNA testing services necessitate a third party, but not necessarily consumer awareness

Seeking the intrigue of discovering one's genealogy or uncovering genetic health risks by merely spitting into a tube and paying an affordable fee,[179] many consumers may not recognize the privacy compromises they are making by providing their uniquely personal DNA data to testing companies. This Section takes a closer look at the services of 23andMe, the second largest private genealogy company,[180] to contextualize the discussion of third-party access.

23andMe describes itself as being founded in 2006 "to help people access, understand and benefit from the human genome." It claims it has "more than five million genotyped customers around the world," and that in 2015, it was "granted authorization by the US Food and Drug Administration (FDA) to market the first direct-to-consumer genetic test."[181]

These tests, and the consumer data thereby curated, currently occur "largely outside pertinent federal regulations ordinarily governing the handling of private health information."[182] This, in turn, "means consumers may not fully understand the implications of the transaction during the process of submitting their genomic and health information."[183] Although the FTC has issued an advisory warning consumers to consider the privacy implications of private DNA test

---

[179] *See, e.g.*, 23ANDME, https://www.23andme.com ($49 for 23andMe's "Ancestry Service (when you buy 2+ kits)"; $199 for "Health + Ancestry Service").
[180] Antonio Regalado, *2017 Was the Year Consumer DNA Testing Blew Up*, MIT TECH. REV. (Feb. 12, 2018), https://www.technologyreview.com/s/610233/2017-was-the-year-consumer-dna-testing-blew-up.
[181] 23ANDME, *supra* note 179 ("What is the history of the company?").
[182] *See generally* Katherine Drabiak, Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Informational Privacy Risks, 27 HEALTH MATRIX 143, 143 (2017).
[183] *See generally id.*

kits,[184] the industry is for the most part unregulated "because most federal and state laws that do regulate genetic information only apply to insurers, employers, health care organizations."[185] Some states have begun to pass laws in this area, but the laws "vary widely in scope, applicability, and the amount of protection provided."[186]

23andMe has various assurances on its website: "You choose how your genetic information is used and shared with others. We tell you how those choices are implemented and how we collect, use and disclose your information."[187] Still, there are multiple situations in which customer information may be shared with third parties. As 23andMe advises on its website, "We work with third-party companies to provide users with services on behalf of 23andMe, and in some cases these companies may have access to a limited amount of non-genetic user information. Specifically, our contracted lab has access to users' DNA samples and limited user information for processing purposes."[188] In other words, 23andMe contracts with third-party service providers to process and analyze saliva samples. Thus, "Personal Information" may be shared with 23andMe's "service providers, including [its] genotyping laboratory, as necessary for them to provide their services."[189] This statement, which includes but apparently is not limited to the genotyping laboratory, broadly covers other, unidentified service providers, while providing very little in the way of specifics as to what those services may be or why they are necessary.

Scientists. In addition to the necessary service providers, 23andMe shares data with scientists. A subtle peer pressure exudes from 23andMe's declaration that over eighty percent of its customers

---

[184] Leslie Fair, *DNA Test Kits: Consider the Privacy Implications*, BUREAU OF CONSUMER PROTECTION (Dec. 12, 2017), https://www.consumer.ftc.gov/blog/2017/12/dna-test-kits-consider-privacy-implications.
[185] Rhys Dipshan, *Giving Away Your Genes: US Laws' Blind Spot with DNA Data*, NAT'L L.J. (Aug. 2, 2018), https://www.law.com/legaltechnews/2018/08/02/giving-away-your-genes-u-s-laws-blind-spot-with-dna-data.
[186] *Privacy Best Practices for Consumer Genetic Testing Services*, FUTURE OF PRIVACY F. 16 (July 31, 2018), https://fpf.org/wp-content/uploads/2018/07/Privacy-Best-Practices-for-Consumer-Genetic-Testing-Services-FINAL.pdf.
[187] 23ANDME, *supra* note 179 ("How is my privacy protected?").
[188] *23andMe Guide for Law Enforcement*, 23ANDME, https://www.23andme.com/law-enforcement-guide.
[189] *Privacy Highlights*, 23ANDME, https://www.23andme.com/about/privacy.

have opted in to participate in scientific research. By saying that each individual "on average . . . contributes to 200 different research studies,"[190] the company seems to suggest that any individuals who do not opt in are missing out on an enthusiastic wave of collaborative scientific discovery. It touts the fact that "[t]o date, 23andMe has published more than 100 peer-reviewed studies in scientific journals."[191] The consumer is assured that personal information will be shared "[w]ith research collaborators, only if you have given your explicit consent."[192] They further add, "If you choose to consent to participate in 23andMe Research, 23andMe researchers *can* include your de-identified Genetic Information and Self-Reported Information in a large pool of customer data for analyses aimed at making scientific discoveries."[193] The word "can" suggests that the consumer is being presented with an opportunity, and few individuals would necessarily dispute the value of "scientific discoveries," despite the vagueness of the phrase.

A quick look at one of the articles listed finds its authors gratefully acknowledging 23andMe contributors for sharing their data: "We thank all contributors to the CREAM Consortium, 23andMe and UKEV for their generosity in sharing data and help in the production of this publication."[194] It is unclear exactly who the "contributors" are or what type of data the scientists were given.

Commercial profit. Consumers may not be aware of the commercial value of their personal DNA information sitting in companies' databanks, and the efforts to monetize that information. While 23andMe's website features the potential for advancing academic knowledge, including links to impressive medical research and scholarly publications, the potential for commercializing that information may be less apparent to the consumer of genomic testing. However, a Wired article published in the summer of 2018 claims that "23andMe has been sharing insights gleaned from consented

---

[190] *About Us*, 23ANDME, https://mediacenter.23andme.com/company/about-us.
[191] *Id.*
[192] *Privacy Highlights*, *supra* note 189.
[193] *Id.* (emphasis added).
[194] *See, e.g.*, Milly S. Tedja et al., *Genome-Wide Association Meta-Analysis Highlights Light-Induced Signaling as a Driver for Refractive Error*, 50 NATURE GENETICS 834-48 (May 28, 2018). *See generally Publications*, 23ANDME, https://research.23andme/publications.

customer data with GSK and at least six other pharmaceutical and biotechnology firms for the last three and a half years."[195]

Case in point: GlaxoSmithKline (GSK). Just this past July, GSK—a global company that describes itself as researching, developing, and manufacturing pharmaceutical medicines, vaccines, and consumer healthcare products[196]—prominently unveiled on its homepage an "exclusive four-year collaboration [with 23andMe] that will focus on research and development of innovative new medicines and potential cures, using human genetics as the basis for discovery."[197] GSK's July 2018 press release declared, "The collaboration will combine 23andMe's large-scale genetic resources and advanced data science skills, with the scientific and medical knowledge and commercialization expertise of GSK,"[198] and that the company and its investors would "leverage" 23andMe's genetic insights to develop its pharmaceuticals.[199] A corresponding announcement was not immediately found on the 23andMe homepage, although a more recent search unearthed one after clicking through an elaborate series of links on the website.[200]

Another potential third party: law enforcement. In its "Guide for Law Enforcement," 23andMe specifically promises it will not provide information to law enforcement, but with a caveat: "[U]nless required to comply with a valid court order, subpoena or a search

---

[195] Megan Molteni, *23andMe's Pharma Deals Have Been the Plan All Along*, WIRED, https://www.wired.com/story/23andme-glaxosmithkline-pharma-deal (Aug. 3, 2018).
[196] *About Us*, GSK, https://www.gsk.com/en-gb/about-us.
[197] *GSK and 23andMe Sign Agreement to Leverage Genetic Insights for the Development of Novel Medicines*, GSK (July 25, 2018), https://www.gsk.com/en-gb/media/press-releases/gsk-and-23andme-sign-agreement-to-leverage-genetic-insights-for-the-development-of-novel-medicines.
[198] *Id*.
[199] *Id.*
[200] *GSK and 23andMe Sign Agreement to Leverage Genetic Insights for the Development of Novel Medicines*, 23ANDME (July 25, 2018), https://mediacenter.23andme.com/press-releases/gsk-and-23andme-sign-agreement-to-leverage-genetic-insights-for-the-development-of-novel-medicines. This link is found by searching the bottom of the page, under "About," then selecting "Newsroom," then "Newsroom" again, this time at the top of the screen, then selecting "Press Releases" from the drop-down menu, then clicking on "2018," and then, finally, finding it in the brief list.

warrant for genetic or Personal Information."[201] 23andMe has already managed to obtain five million records since its founding in 2006.[202] By comparison, law enforcement's own national DNA database, the Combined Index DNA System, founded as a pilot software project almost twenty years earlier in 1990,[203] holds 13 million records.[204]

It has been well documented that investigators used private genomic testing data to solve the Golden State Killer investigation.[205] In that case, investigators had said they did not require a court order before using GEDmatch, which is a crowdsourced database containing roughly a million DNA sets shared by individuals.[206] Since then, law enforcement has already used genetic genealogy again, this time to solve a recent crime, which was not a cold case or serial murder like the Golden State Killer.[207] In July 2018, 31-year-old Spencer Glen Monnett was arrested by police in Utah for a rape that occurred in

---

[201] *Privacy Highlights*, *supra* note 189.
[202] *About Us*, *supra* note 190.
[203] *Combined Data Index System (CODIS)*, FED. BUREAU INVESTIGATION, https://www.fbi.gov/services/laboratory/biometric-analysis/codis.
[204] *Id.*
[205] *See, e.g.*, Yasemin Saplakoglu, *How the Golden State Killer's DNA Nabbed Him*, LIVESCIENCE (Apr. 26, 2018, 9:51 PM ET), https://www.livescience.com/62421-golden-state-killer-dna-genealogy.html.
[206] *See* Tony Romm & Drew Harwell, *Ancestry, 23andMe and Others Say They Will Follow These Rules When Giving DNA Data to Businesses or Police*, WASH. POST (July 31, 2018), https://www.washingtonpost.com/technology/2018/07/31/ancestry-andme-others-say-they-will-follow-these-rules-when-giving-dna-data-businesses-or-police. GEDmatch is a free, volunteer-run service in which "raw data from 23andMe, AncestryDNA, and other DNA-testing services can be uploaded," allowing its genealogists "to compare segments of DNA. These tests are more sophisticated than the DNA tests police typically run, and they generate more data than is stored in the FBI's CODIS database." Sarah Zhang, *The Coming Wave of Murders Solved by Genealogy*, ATLANTIC (May 19, 2018), https://www.theatlantic.com/science/archive/2018/05/the-coming-wave-of-murders-solved-by-genealogy/560750. On its website, GEDmatch itself states, "If you are a member of Law Enforcement and you are looking for help with your cold cases, please click HERE. It is a FREE (yes, FREE!) service provided by very intelligent and motivated genetic genealogists. Anyone with genetic genealogy test results from 23andMe, FTDNA.com (the Family Finder test), and Ancestry.com. [sic]" (emphasis in original). YOUR DNA GUIDE, Error! Hyperlink reference not valid.https://www.yourdnaguide.com/upload-to-gedmatch.
[207] Antonio Regalado, *Genetic Genealogy Is Now Solving Recent Crimes, Not Just Cold Cases*, MIT TECH. REV. (July 30, 2018, 2:34 PM), https://www.technologyreview.com/the-download/611748/genetic-genealogy-is-now-solving-recent-crimes-not-just-cold-cases.

April 2017.[208] He was located through DNA he left at the crime scene that first was used to find his relatives, and then him.[209] The St. George Police Department's press release thanked officers, the state crime lab and Parabon NanoLabs for helping with the investigation.[210] Parabon Nanolabs' website says its "Phenotyping Service . . . produces a descriptive profile of the source of any human DNA sample, including pigmentation, face morphology, and other forensically relevant traits."[211]

While solving violent crimes may appear to be an uncontroversial objective, law enforcement's ability to access genomic data for prosecutorial purposes raises questions for private citizens who are not in a law enforcement database but whose DNA sequencing now resides in a private databank. Law enforcement may very conceivably investigate future crimes that are not as patently heinous as the Golden State Killer murders by seeking access to information in a private databank. This information might exist only because a consumer or a relative—possibly a distant relative—engaged genomic testing services for personal reasons such as satisfying curiosity or obtaining medical insights, without imagining that law enforcement might one day seek that data.

2. Testing services lack meaningful ability to opt out

The public's fascination with DNA testing has been fueled by such intriguing possibilities as discovering one is related to royalty, combined with the ease of the process for the consumer.[212] These services have become "increasingly popular with people who are eager

---

[208] *Id.*
[209] *Id.*
[210] David DeMille, *Arrest Made in Home Invasion Rape of Elderly St. George Woman*, ST. GEORGE SPECTRUM & DAILY NEWS (July 28, 2018, 3:03 PM MT), https://www.thespectrum.com/story/news/2018/07/28/79-year-old-woman-raped-assaulted-her-st-george-home/855583002; *see also St. George, Utah, Police Department,* FACEBOOK (July 28, 2018, 9:09 AM), https://www.facebook.com/sgcitypubsafety.
[211] PARABON NANOLABS, https://www.parabon-nanolabs.com.
[212] Mark Williams, *The Lucrative Rise of DNA Testing: 'We Created the Market for What We Do*,' GUARDIAN (May 25, 2017), https://www.theguardian.com/small-business-network/2017/may/25/dna-testing-we-created-the-market-for-what-we-do-living-dna-dnafit-geneu.

to learn more about themselves, their families, and their health."[213] More people took genetic tests through private genealogy testing in 2017 than in all past years combined.[214] In February 2018, Ancestry.com reported that over seven million people had sent in their DNA for testing to date, including two million during the last four months of 2017, and that this represents more customers than all of Ancestry's competitors combined; while 23andMe, the next largest, has over three million customers, followed by MyHeritage and FamilyTreeDNA.[215]

The websites of these genealogical services offer so much information that it is unlikely most people read it all. Consumers are likely to be attracted to the intriguing possibility that one may be able to discover, in six to eight weeks, information about their family genealogy across 350 regions.[216] On the other hand, perhaps less intriguing is the statement that 23andMe makes, for example, that "we push the boundaries of what's possible to enable groundbreaking research and innovative products. And we empower those outside the company to leverage the platform we've built. "[217] 23andMe's "Guide for Law Enforcement"[218] makes plain as well the possibility that law enforcement may seek the data. One bioethics researcher summed it up by saying, "If you read the documents

---

[213] Katherine Kwong, *Third-Party Services as Potential Sources for Law Enforcement Procurement of Genomic Data*, 15 CAN. J.L. & TECH. 99 (2017) (citing Wylie Burke et al., The Deceptive Appeal of Direct-to-Consumer Genetics, 164 ANNALS INTERNAL MEDICINE 563, 564 (2016); Cathelijne H. Van Der Wouden et al., *Consumer Perceptions of Interactions with Primary Care Providers after Direct-to-Consumer Personal Genomic Testing*, 164 ANNALS INTERNAL MEDICINE 513, 514 (2016)).

[214] Regalado, *supra* note 180.

[215] *Id.* Note that this number has actually risen from three to five million in the short time span from February to November 2018. *See* 23ANDME, *supra* note 181.

[216] ANCESTRY.COM, https://www.ancestry.com/dna.

[217] *Our Mission*, 23ANDME, https://mediacenter.23andme.com. Notably, the tenor of this language, which emphasizes sensitivity to the individuals whose data is used, has changed from prior language that could not be located: "23andMe customers who participate in research are helping us advance scientific knowledge in revolutionary new ways. Each discovery helps pave the way for advances in medicine." The prior language itself was a change from even earlier language that also could not be located, in which the emphasis was on the company's mission, versus the consumer's opportunity to participate: "[s]haring our research with the scientific community is key to our mission. Read our scientific publications, white papers, and conference presentations below." *Publications*, *supra* note 194.

[218] 23andMe Guide for Law Enforcement, *supra* note 188.

carefully, all the information is there . . . but [t]he challenge is that people don't read it."[219]

23andMe reassures consumers that "23andMe will not sell, lease, or rent your individual-level information to any third party or to a third party for research purposes without your explicit consent."[220] Although "23andMe may share some data with external research partners and in scientific publications," it promises that "[t]hese data will be summarized across enough customers to minimize the chance that your personal information will be exposed."[221] Moreover, it "will not share your *individual-level Genetic Information* or Self-Reported Information with *any* third party without your explicit consent."[222] 23andMe acknowledges, nonetheless, that "[t]here is a very small chance that someone with access to the research data or results could expose personal information about you. 23andMe has policies and practices in place to minimize the chance of such an event."[223]

Consumers are also told they have the option to "withdraw from 23andMe Research at any time."[224] However, yet another caveat is presented: "Any of your data that have already been entered into a study cannot be withdrawn, but your data will not be included in studies that start more than 30 days after you withdraw (it may take up to 30 days to withdraw your information after you withdraw your consent)."[225] Thus, one scholar has already noted that the terms of

---

[219] Molteni, *supra* note 195 ("It's a lot of fine print that looks like a lot of other fine print people on the internet click through every day—to browse, buy, watch, and listen online. 'They're so used to sharing data that they may not realize it's just going in the front end and out the backend,' according to Kayte Spector-Bagdady, a lawyer and bioethics researcher at the University of Michigan who has reviewed 23andMe's customer policies. 'They really do disclose it all.'").

[220] *Privacy Highlights*, *supra* note 189. Notably, when this passage was originally written in July 2018, the language quoted from the website under the link "Consent" was "Participating in 23andMe's research is always voluntary and requires customers to affirmatively consent to participate." However, on a more recent visit, this language had been replaced with the above.

[221] *Research Consent Document*, 23ANDME, https://www.23andme.com/about/consent.

[222] *Privacy Highlights*, *supra* note 189 (emphasis added).

[223] *Research Consent Document*, *supra* note 221.

[224] *Id.*

[225] *Id.*

23andMe are such that "withdrawing from research still permits ongoing research use of the consumer's information within 23andMe and by external entities and only prevents the initiation of new, discrete research projects using that consumer's information." [226] The company's database will retain that information, so "even if a consumer attempts to close her account, 23andMe reserves the right to retain an indelible record of her full genomic sequence, highly personal self-reported information, and fact of participation."[227]

Underlying commercial opportunities for 23andMe, moreover, are not plainly spelled out on the website, although "offering access to customer information in the service of science has been 23andMe's business plan all along."[228] Perhaps this is part of the reason why, after learning of the GSK deal, some consumers were still "surprised and angry, unaware of what they had already signed (and spat) away."[229] While academic research is unobjectionable, consumers may not have realized and may find distasteful that their DNA can become a commodity for commercial profit.[230] The word "leverage"[231] in the GSK press release might have struck some as mercenary. This sense of betrayal may stem from the "tension between the way 23andMe portrays itself as a health company, and simultaneously wants to be treated like every other tech company that makes its money from big data."[232] Said one commentator, "You can't have it both ways. That's why we have HIPAA, it's why we have all these regulations that say health information is privileged information that can't be commodified."[233]

---

[226] Katherine Drabiak, *Caveat Emptor: How the Intersection of Big Data and Consumer Genomics Exponentially Increases Informational Privacy Risks*, 27 HEALTH MATRIX 143, 158 (2017).
[227] *Id.* at 159.
[228] Molteni, *supra* note 195.
[229] *Id.* ("GSK will receive the same kind of data pharma partners have generally received—summary level statistics that 23andMe scientists gather from analyses on de-identified, aggregate customer information—though it will have four years of exclusive rights to run analyses to discover new drug targets. Supporting this kind of translational work is why some customers signed up in the first place. But it's clear the days of blind trust in the optimistic altruism of technology companies are coming to a close.").
[230] Regalado, *supra* note 180.
[231] *See supra* text accompanying note 199.
[232] Molteni, *supra* note 195.
[233] *Id*.

As to its arrangement with GSK, 23andMe assures, "For those who do consent, their information will be de-identified, so no individual will be identifiable to GSK."[234] GSK echoes the reassurance that privacy breaches are not a concern, saying, "Both companies have stringent security protections in place when it comes to collecting, storing and transferring information about research participants. 23andMe employs software, hardware and physical security measures to protect the computers where data is stored and information will only be transferred using encryption to offer maximum security."[235] Nonetheless, and without disputing the benefits of technological innovation and advancing medical science, these measures demonstrate the underlying potential for individual privacy breaches and the inability to eradicate that potential.

Moreover, in what appears to be a contradiction to these earlier statements, 23andMe CEO and co-founder Anne Wojcicki, when asked a series of questions about the GSK agreement at TechCrunch's Disrupt show in San Francisco in September 2018, explained that 23andMe customers are not being asked to opt in to the data-sharing agreement, but rather, are being told via email that they can opt out.[236] Thus, the burden appears to be placed on the consumer to affirmatively decline to participate, with the default being that consent is assumed.[237]

Additionally, as a commercial enterprise, 23andMe, according to one legal commentator, "is not bound by the same obligations as medical professionals," and can, "at least in theory, unilaterally change those terms and conditions and privacy policies at any time."[238]

---

[234] GSK and 23andMe Sign Agreement to Leverage Genetic Insights for the Development of Novel Medicines, *supra* note 200.
[235] *Id.*
[236] Connie Loizos, *23andMe Underscores that Privacy-Loving Customers Need to Opt-Out of its Data Deal with GlaxoSmithKline*, TECHCRUNCH (Sept. 5, 2018), https://techcrunch.com/2018/09/05/23andme-underscores-that-privacy-loving-customers-need-to-opt-out-of-its-data-deal-with-glaxosmithkline.
[237] *See supra* note 220 and accompanying text, requiring "explicit consent" (formerly, "affirmative").
[238] Molteni, *supra* note 195 (quoting Katherine Drabiak, a legal expert in health law and research ethics at the University of South Florida: "As a commercial enterprise, it's not bound by the same obligations as medical professionals. 23andMe

Finally, the science behind the DNA testing process itself is also a black box to most. While Ancestry.com's website prominently features intriguing genealogical possibilities in its offer to start a free trial, details of the DNA testing process itself were not as obviously visible. The FAQ section does provide, mysteriously, "The AncestryDNA test uses microarray-based autosomal DNA testing, which surveys a person's entire genome at over 700,000 locations."[239] 23andMe's website likewise asserts, somewhat more simplistically, that "[o]ur CLIA-certified lab extracts DNA from cells in your saliva sample. Then the lab processes the DNA on a genotyping chip that reads hundreds of thousands of variants in your genome."[240]

Again, dissociative appeal and social mandate conflate to create a confusing picture about the consumer's expectation of privacy when it comes to private genomic testing. Consumer enthusiasm about an intriguing service, information overload, and fine print fatigue, along with general desensitization to sharing data and clicking "I do give consent" in order to engage services,[241] remove consumers' meaningful ability to recognize and opt out of potential privacy compromises. Moreover, opting out may not prevent personal data

---

doesn't have to take an oath to act in the interest of consumers or to promote their well being").

[239] *Frequently Asked Questions*, ANCESTRY.COM, https://www.ancestry.com/dna/en/legal/us/faq.

[240] *Our Science*, 23ANDME (Dec. 7, 2017, 9:30 PM ET), https://www.23andme.com/genetic-science; *see also* Rafi Letzter, *How Do DNA Ancestry Tests Really Work?*, LIVESCIENCE (June 4, 2018, 7:15 AM ET), https://www.livescience.com/62690-how-dna-ancestry-23andme-tests-work.html (As explained in an interview with Robin Smith, the head of 23andMe's ancestry program, "This string of letters would be incomprehensible to you and, on their own, just as incomprehensible to the biologists and engineers who study them. There's no string of letters that means 'Swiss' or 'Nigerian,' for example. But the algorithms can pull meaning out of the strings of letters."); Rachael Rettner, *DNA: Definition, Structure & Discovery*, LIVESCIENCE (DEC. 7, 2017, 9:30 PM ET), https://www.livescience.com/37247-dna.html.

[241] Molteni, *supra* note 195 ("To register a DNA kit on 23andMe, customers are required to accept the company's privacy policy and terms and conditions, which together disclose what data 23andMe collects, how it's protected, and how it can be used and shared. Then customers are given the option to participate in 23andMe research. A lengthy document explains what that entails, and if they click a green box at the bottom saying 'I DO GIVE CONSENT,' then the majority of their data—their genetic profile plus any information they enter into surveys or authorize 23andMe to import—can be used for research in de-identified and aggregated form.").

from being incorporated in research already in place; and options for opting out of a commercial deal, such as that between 23andMe and GSK, appear murky.

"Privacy Best Practices." In the wake of privacy concerns raised by law enforcement's use of forensic genealogy to track down the Golden State Killer—and just a few days after the GSK announcement—Ancestry.com, 23andMe, and other popular companies that offer genetic testing publicly pledged to follow a new set of mutually agreed-upon privacy guidelines.[242] The "Privacy Best Practices for Consumer Genetic Testing Services" (PBP) were drafted with the assistance of the Future of Privacy Forum (FPF), a Washington, D.C.-based nonprofit.[243] According to FPF's July 2018 press release, "The Best Practices establish standards for genetic data generated in the consumer context by making recommendations for companies' privacy practices."[244]

As an initial matter, however, the PBP only applies to information that is not "deidentified . . . provided that the deidentification measures taken establish strong assurance that the data is not identifiable."[245] In other words, anonymized data is not subject to the PBP. This raises two questions: what deidentification measures are taken, and how do they establish strong assurances that the data is not identifiable? The PBP does offer, in a footnote, "Commercial technical protections and capabilities are currently being developed," and lists various protections available for genetic data to

---

[242] Tony Romm & Drew Harwell, *Ancestry, 23andMe and Others Say They Will Follow These Rules When Giving DNA Data to Businesses or Police*, WASH. POST (July 31, 2018), https://www.washingtonpost.com/technology/2018/07/31/ancestry-andme-others-say-they-will-follow-these-rules-when-giving-dna-data-businesses-or-police.

[243] *Privacy Best Practices for Consumer Genetic Testing Services*, *supra* note 186. The PBP is divided into eight sections: Transparency; Consent; Use and Onward Transfer; Access, Integrity, Retention, and Deletion; Accountability; Security; Privacy by Design; Consumer Education. It offers three "annexes": Definitions; Legal and Regulatory Guidance; Genetic Data Sharing Policies; and concludes with information "About the Future of Privacy Forum." *Id.*

[244] Melanie E. Bates, *Future of Privacy Forum and Leading Genetic Testing Companies Announce Best Practices to Protect Privacy of Consumer Genetic Data*, FUTURE OF PRIVACY F. (July 31, 2018), https://fpf.org/2018/07/31/future-of-privacy-forum-and-leading-genetic-testing-companies-announce-best-practices-to-protect-privacy-of-consumer-genetic-data.

[245] *Privacy Best Practices*, *supra* note 186, at 3.

date" concluding, "Without a corollary dataset for matching, the risks remain minimal."[246] Also listed as a safety measure is "aggregation of individual reports," which "*may* provide strong assurance that personal data is not identifiable, if appropriate safeguards are in place."[247] However, this language, with its abundant qualifications, only highlights that the risks exist. As a senior director of one trade association has observed, "Without more insight into how consumer data is being anonymized . . . it's difficult to tell how secure it really is."[248]

As for "individual-level information (i.e., Genetic Data and/or personal information about a single individual)," consumers are assured that "[s]eparate express consent will be required for [o]nward transfer of [the information] to third-parties for any reason, excluding vendors and service providers."[249] Specifically, "[i]nformed consent will be required when Genetic Data is transferred to third parties for research purposes; and Research is done under the control of the Company (i.e., internal research) for the purpose of publication or generalizable knowledge."[250]

This first category of data that is protected by the PBP from onward transfer does not seem to represent a meaningful change. Pre-PBP, 23andMe had already stated, "If you choose to consent to participate in 23andMe Research, 23andMe researchers can include your de-identified Genetic Information and Self-Reported Information in a large pool of customer data for analyses aimed at making scientific discoveries."[251]

The description of the second category of information, "incompatible secondary uses of Genetic Data,"[252] which the PBP asserts now requires separate express consent, also raises questions. "Incompatible secondary uses" are defined as "includ[ing] those uses outside

---

[246] *Id.* at 3 n.6.
[247] *Id.* at 3 (emphasis added).
[248] Kristen V. Brown, *Concerns Mount over Data Privacy Guidelines Set by Genetic-Testing Companies*, INSURANCE J. (Aug. 3, 2018), https://www.insurancejournal.com/news/national/2018/08/03/497037.htm.
[249] *Privacy Best Practices*, *supra* note 186, at 4.
[250] *Id.* at 5.
[251] 23andMe, *supra* note 193.
[252] *Privacy Best Practices*, *supra* note 186, at 5.

of the primary purpose of the purchased service and the inherent contextual uses. Incompatible secondary uses do not include activities intended to develop or improve new or current products."[253] However, what do "inherent contextual uses" mean? Also, by excluding "activities intended to develop or improve new or current products," the PBP appears to exempt itself from selling the data for commercial benefit, as 23andMe did with GSK. Thus, the PBP fails to address the concern some commentators raise of what happens to "consumers' data that is shared for research with pharmaceutical giants, academics and other, often for a profit."[254] 23andMe is not alone in this regard. Like social networks, many genetic-testing companies have made a business out of collecting data from customers; these companies form partnerships with GSK or Pfizer, giving them access to their vast "troves" of DNA data.[255] Notable as well is that "[t]he industry leaders involved in producing this document, while certainly occupying a large market share, represent only a fraction of the many companies offering these services."[256]

Another category of concern is data access by law enforcement.[257] The PBP addresses this not under "Section II. Consent," but rather under "Section IV. Access, Integrity, Retention, and Deletion,"[258] placed almost as an afterthought. In accordance with Section IV's title, its first four subsections are "Access," "Integrity," "Retention," "Deletion," respectively, but the fifth makes an awkward appearance as "Law Enforcement Access."[259] There, the PBP provides that "Genetic Data may be disclosed to law enforcement entities without Consumer consent when required by valid legal process."[260] In a footnote citing the Health Insurance Portability and Accountability Act (HIPAA),[261] which is the federal statute safeguarding medical

---

[253] *Id.* at 5 n.12.
[254] Brown, *supra* note 248.
[255] *See id*.
[256] *Id.*
[257] *Privacy Best Practices*, *supra* note 186, at 5 (identifying as a third category "Consumers or organizations that submit biological samples or Genetic Data on behalf of other individuals (others, elderly relatives, etc.)," which is not within the purview of this Article).
[258] *Id.* at 8.
[259] *Id.*
[260] *Id.*
[261] *Id.* at 8 n.27 (referencing HIPAA); *see also id.* at 13 (describing HIPAA).

information privacy, the PBP excludes the situation in which a warrant is served for a criminal investigation. The footnote notes that HIPAA prohibits disclosure of DNA information to identify or locate a suspect, "absent some other legal requirements such as a warrant."[262] Given that the Golden State Killer's DNA data was obtained without a warrant, this provision of the PBP may provide notice to law enforcement that they should obtain one henceforth.

Ultimately, adherence to the policy framework, which is industry-created and lacks the force of law, is voluntary even among those who pledge to abide by it.[263] While the PBP may offer some protection from warrantless access by law enforcement, a close look at the "new guidelines"[264] does not seem to reveal much in the way of a change in the policies for sharing data for science research, whether for profit or not. In the meantime, as the CEO of the FPF himself observed, "I don't think the average consumer has wrapped their head around the range of issues they should think about when they make a decision to share [DNA] data."[265]

The industry of private genomic testing provides a unique yet representative example of technologies and services in which a third party possesses some control over a consumer's personal information. A black-and-white application of the third-party doctrine in which the consumer either voluntarily shared the data or is reduced to a dependent pawn of technology does not serve the Fourth Amendment well. Thus, this Article urges an extension of the doctrine, in which determining whether the consumer maintains or has forfeited a reasonable expectation of privacy over that information includes two inquiries: first, whether the consumer understood that the technology's design necessitates a third party, and second, whether the consumer could opt out of sharing data with that third party.

---

[262] *Id*.
[263] Romm & Harwell, *supra* note 242.
[264] *Id.*
[265] *Id.*

V. CONCLUSION [266]

It may be that as the process of assimilating to the digital era continues to unfold, society will find its attitude toward digital technology emerging from a honeymoon phase. The Cambridge Analytica scandal[267] has awakened many to the reality that social media platforms such as Facebook collect personal data and redistribute it for commercial, political, and other purposes wholly unrelated to their stated social networking mission.[268] Mark Zuckerberg's testimony in front of Congress in spring 2018 amply demonstrated that, despite the enormous popularity of Facebook, many senators did not understand its business model. Journalists have already written about the seemingly "clueless" questions senators asked during the hearings.[269] More importantly however, the Boycott Facebook campaign, "Faceblock,"[270] demonstrated that many ordinary citizens as well, including those who used Facebook actively, did not understand the extent of Facebook's consumer-information-based targeted advertising and felt betrayed by it. In the campaign, Facebook users stopped using Facebook for one day to protest the company's involvement in the Cambridge Analytica scandal, the company's attitude toward data privacy, and the way the company was being regulated.[271] This reaction highlights the evolving dynamic between the expectation of privacy and digital technology, and how consumers' understanding of how the technology works—or lack thereof—

---

[266] *See generally* Park, *supra* note 26, at 35-36.

[267] Andrea Valdez, *Everything You Need to Know About Facebook and Cambridge Analytica*, WIRED (Mar. 23, 2018), https://www.wired.com/story/wired-facebook-cambridge-analytica-coverage.

[268] Len Sherman, *Why Facebook Will Never Change Its Business Model*, FORBES (Apr. 16, 2018, 1:01 PM), https://www.forbes.com/sites/lensherman/2018/04/16/why-facebook-will-never-change-its-business-model (noting that after the hearings, "it's widely understood that Facebook's voracious appetite for user data is driven by their business model which charges advertisers for access to precisely targeted segments of their massive consumer database. No one knows more about more consumers than Facebook").

[269] *See, e.g.*, Amelia Tait, *Five Clueless Questions United States Senators Asked Mark Zuckerberg*, NEW STATESMAN (Apr. 11, 2018), https://www.newstatesman.com/science-tech/security/2018/04/five-clueless-questions-united-states-senators-asked-mark-zuckerberg.

[270] Nicola Slawson, *Faceblock Campaign Urges Users to Boycott Facebook for a Day*, GUARDIAN (Apr. 7, 2018), https://www.theguardian.com/technology/2018/apr/07/faceblock-campaign-urges-users-boycott-facebook-for-one-day-protest-cambridge-analytica-scandal.

[271] *See id*.

needs to be recognized as such when making determinations about whether or not they have a reasonable expectation of privacy.

Americans, according to one commentator, have begun "changing their relationship with Facebook" in the wake of the Cambridge-Analytica scandal.[272] According to the Pew Research Center, 54% of Facebook users ages eighteen and older say they have adjusted their privacy settings in the past year; 42% say they have taken a break from checking the platform for a period of several weeks or more; and 26% have deleted the Facebook app from their cellphone.[273] Combined, 74% of Facebook users took one or more of these measures within the past year.[274]

Nonetheless, online social networking has become part of the social fabric. As initial feelings of shock and betrayal subside, consumers are likely not only to return to their customary social networking habits, but also to continue embracing new cutting-edge technologies and services with potentially unknown privacy implications, of which smart devices and DNA testing are but a small part.

In July 2017, a Wisconsin technology firm began offering employees microchip implants that could be used to scan into the firm's building and to purchase food at work.[275] The chip uses radio-frequency identification (RFID)—the same technology used in smart devices[276]—and the CEO, Todd Westby, foresees "the use of RFID technology to drive everything from making purchases in our office break room market, opening doors, use of copy machines, logging into our office computer, unlocking phones, sharing business cards, storing medical/health information, and used as payment at other RFID terminals." [277] He believes "this technology will become

---

[272] Andrew Perrin, *Americans Are Changing Their Relationship with Facebook*, PEW RES. (Sept. 5, 2018), http://www.pewresearch.org/fact-tank/2018/09/05/americans-are-changing-their-relationship-with-facebook.
[273] *Id.*
[274] *Id.*
[275] *Three Square Market Microchips Employees Company-Wide*, PRLOG (July 20, 2017), https://www.usatoday.com/story/tech/nation-now/2017/07/24/wisconsin-company-install-rice-sized-microchips-employees/503867001.
[276] Chrissie Cluney, *RF Fundamentals for the Internet of Things*, IOT EVOLUTION WORLD (June 6, 2017), https://www.iotevolutionworld.com/iiot/articles/432606-rf-fundamentals-the-internet-things.htm.
[277] *Id.*

standardized allowing you to use this as your passport, public transit, all purchasing opportunities, etc." [278] Currently, he says, there is no GPS tracking.[279]

Employees who enjoy hovering their hand in front of a digital reader at checkout to buy their afternoon snack, or in front of a lock instead of fumbling for a key card, have essentially made themselves into their own customized smart devices. Countless more unregulated opportunities for third-party access to personal data proliferate. Recent reports have found that that "[m]any Google services on Android devices and iPhones store your location data even if you've used a privacy setting that says it will prevent Google from doing so."[280] The *Wall Street Journal* reported that third-party app developers can read and analyze the contents of a user's Gmail message.[281] Another study found that "[s]ome popular apps on your phone may be secretly taking screenshots of your activity and sending them to third parties."[282]

The touchstone of the Fourth Amendment is reasonableness,[283] but what is reasonable has traditionally hinged on examining physical objects that either can be shared or not. Such an examination makes less sense with electronic data. Both smart devices and private DNA testing services illustrate the urgent need for extending the third-party doctrine now. These two consumer products are distinct from each other and from cell phones as well, but both are increasingly

---

[278] Mary Bowerman, *Wisconsin Company to Install Rice-Sized Microchips in Employees*, USA TODAY (July 25, 2017), https://www.usatoday.com/story/tech/nation-now/2017/07/24/wisconsin-company-install-rice-sized-microchips-employees/503867001.

[279] *Id.*

[280] Ryan Nakashima, *AP Exclusive: Google Tracks Your Movements, Like It or Not*, ASSOCIATED PRESS (Aug. 13, 2018), https://www.apnews.com/828aefab64d4411bac257a07c1af0ecb.

[281] Douglas MacMillan, *Tech's 'Dirty Secret': The App Developers Sifting Through Your Gmail*, WALL ST. J. (July 2, 2018), https://www.wsj.com/articles/techs-dirty-secret-the-app-developers-sifting-through-your-gmail-1530544442; Nick Statt, *Google Tries to Calm Controversy over App Developers Having Access to Your Gmail*, VERGE (July 3, 2018), https://www.theverge.com/2018/7/3/17533108/google-gmail-privacy-read-email-messages-response.

[282] Bill Ibelle, *Is Your Smartphone Spying on You?*, NORTHEASTERN: NEWS (July 6, 2018), https://news.northeastern.edu/2018/07/06/is-your-smartphone-spying-on-you.

[283] *See* Florida v. Jimeno, 500 U.S. 248, 250 (1991) (citing Katz v. United States, 389 U.S. 347, 360 (1967)).

ubiquitous technologies that require a third party to operate. Like CSLI, the data produced by smart devices and DNA testing involves no voluntary act or affirmative sharing. *Carpenter* is a step in the right direction, but clarity is needed for the vast array of unregulated technologies growing in popularity, and for those yet to emerge. If courts do not adopt a new third-party doctrine test for digital technologies whose design necessitates a third party, society may find that the distinction between man and machine, as well as the notion of a personal expectation of privacy, have become obsolete.