MIT Computational Law Report

Data Intermediaries: Fourth Amendments, Third Parties, Second Chances, and First Principles

Jonathan Askin Brian Fischer Kristin Kuraishi Patrick Lin

Published on: Jun 13, 2023

URL: https://law.mit.edu/pub/dataintermediaries

Introduction

The Fourth Amendment protects "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[1] This constitutional right shields citizens against meritless governmental intrusion into their homes, letters, and other effects. However, the third-party doctrine holds that individuals who voluntarily provide information to a third party do not have a reasonable expectation of privacy in such information.[2] Therefore, Fourth Amendment protections do not apply to information that is unwittingly and automatically shared with third party private entities such as Facebook, Google, Amazon, and Apple, enabling the government to seize and search it without probable cause or a search warrant.[3] All the government really has to do is just ask for it.[4] This Article seeks to fill the gap in constitutional protection that currently exists over our personal data shared with third parties. Specifically, we posit that those entities voluntarily seeking to act as fiduciaries with their patrons' personal data, should be able to "stand in the shoes" of their patrons, and only provide any sensitive (and potentially incriminating) information to law enforcement through a transparent, structured, and standard-based process.

Part I of this Article provides background information about the relationship between trusts, fiduciaries, contracts, and data, the need to balance corporate and consumer interests, and the brief evolution of the third-party doctrine. Part II analyzes the U.S. Supreme Court's *Carpenter* decision, focusing on the applicability of Gorsuch's dissent when establishing a Fourth Amendment fiduciary, and finally how to operationalize this approach.

Background

The Common Law of Obligations: Trusts, Fiduciaries, and Bailors

A trust is a legal agreement that names someone ("trustee") to hold property for the benefit of others ("beneficiaries").[5] The individual who creates the trust is called the "settlor" (or "grantor") and that individual can also be a beneficiary of the trust.[6] Trusts divide the legal and actual possession over trust property, also referred to as a "corpus."[7] As a property-holding trustee makes decisions about the (potentially income-generating) corpus with only the interests of the beneficiary in mind, the trustee owes **fiduciary duties** to the beneficiary to ensure that proper and informed decisions are made.[8] Legal title generally stays with the settlor until their death, upon which legal title falls under the name of the trust, while actual enjoyment and possession remains with the beneficiary.[9]

Another type of entity that relies upon the common law doctrine of obligations is the actual fiduciary. In modern society, these fiduciaries often are members of a profession, such as doctors, lawyers, and certain financial advisors, bound by their obligations pursuant to an explicit code of conduct. Unlike the trust, these entities typically rely on contracts and other legal instruments to create and enforce formalized relationships with their clients or patrons.

A third type of obligation created at common law is bailment. Typically this applies to individuals or entities (the "bailee") who have temporary possession of property on behalf of someone else (the "bailor"). Classic cases of the bailor-bailee relationship are the dry cleaning business, and the parking valet at a restaurant. In each instance, the bailee warrants to the bailor that the property in question will be returned, at the agreed-to time and location, and in an agreed-to condition.

Fiduciary duties are legal duties one party owes to act on behalf of a second party in order to manage assets.[10] There are two main duties: duty of care and duty of loyalty. The duty of care requires a fiduciary to act reasonably in their decisions. An often related duty of care imported from the common law of torts is the "do no harm" standard, which obligates the party not to impose physical or other harms on the other party. Meanwhile, the duty of loyalty can be viewed as a higher standard of conduct and requires the fiduciary to act in the best interests of the other party; here, the beneficiary. These fiduciary duties are legally binding on the fiduciary and result in stronger protections and assurances for the beneficiaries involved. One of the most prominent fiduciary duties of loyalty is to avoid a conflict of interest so that the fiduciary does not use the beneficiary's information or assets to the beneficiary's detriment, the fiduciary's advantage, or both.

A trust is advantageous because it frees up your time to pursue other ventures and activities, with the confidence that the trustee will work in your best interest. The trustee also likely has experience, data, and other insights from managing additional property. Pooled trusts, combined with expertise from handling multiple assets from numerous clients, may be extremely lucrative and have the potential to earn significant returns.[11]

The primary downside to using trusts is the cost, which is most often a percent-of-assets management fee or a fixed fee.[12] The fees can decrease as your assets under management decrease, while some trust funds charge higher fees on complex assets such as private equity investments, standalone businesses, or multigenerational parcels of land.[13]

In addition to the question of "how much" to pay is a somewhat related question: To whom specifically do the duties attach? Whitt notes that fiduciary duties can be *assumed* due to an entity's consent, or automatically *imposed* due to "an entity's status, its specific role vis-à-vis its customers."[14] The latter category is easily seen in the relationships between lawyers and clients or doctors and patients.[15] On the other hand, voluntary assumption of fiduciary duties is often created by one party making external representations to another that the former will hold the sensitive information of the potential beneficiaries with care, loyalty, and other indica of trust.[16]

Many of these trust-generating representations made by large technology platforms can be found in privacy policies and promises relating to data security, data minimization, and access rights.[17] However, there are few companies, entities, or associations that focus *primarily* on the manner of care and loyalty in which they or

their constituents handle data – as a goal in and of itself – rather than using privacy as an incidental benefit to another primary service they offer.

Data Trusts and Digital Fiduciaries

Data trusts are "legal structures that give independent, third-party stewardship of data."[18] Data trusts share many of the same characteristics as traditional trusts. For example, like a traditional trust, a data trust allows a trustee to make decisions about the corpus on behalf of the beneficiaries. In a data trust, these beneficiaries can be made up of individuals, organizations, or essentially anyone or anything that holds data. Importantly, a data trustee has a fiduciary duty to do what is best for the beneficiary, much like a doctor has a fiduciary duty to do what is best for their patient. In other words, the trustee is not allowed to have a unilateral profit motive or, more broadly, a conflict of interest in the data or data rights under its custody. The key distinction is that data trusts are trusts in which the corpus of the trust is data, rather than real property, stocks, or bonds, and the decisions made concern that data.[19]

The key players in a data trust remain virtually unchanged from a traditional trust; however, the roles differ slightly. For instance, while settlors grant rights to trustees and trustees have fiduciary duties to beneficiaries, the beneficiary composition in a data trust is expanded to those who are provided access to the data *as well as* those who benefit from the result of the data, a potentially much larger pool than a typical trust. That is, a trustee can also be a beneficiary of a trust. Furthermore, data trusts can be particularly advantageous when there are conflicting interests between beneficiaries. A trustee can decide who may access and use the data under the trust's control. If that data user fails to comply with the terms and conditions, the trustee can revoke their access.

However, consider the competing interests of a corporation and consumers, or data subjects. If a data controller has a business interest in data provided by data subjects, this often results in a conflict between that interest and their duties towards data subjects.[20] Under these conditions, data controllers would be obligated to both maximize the value of the personal data they collect (for the benefit of shareholders) *and* honor fiduciary obligations towards data subjects.[21] The data subject in most instances would prefer that the data controller minimize the use, sharing, and monetization of its data. Therefore, a fiduciary obligation towards data subjects is incompatible with the data controllers' responsibility towards shareholders.[22] Sylvie Delacroix has compared the information fiduciary to a doctor who gains a commission on particular drug prescriptions or a lawyer who uses a company to provide medical reports for his clients while owning shares in that company.[23] In each case there exists a likelihood for a conflict of interest that brings into question whether the one under fiduciary duties is able to fulfill those duties to the extent the law requires.

While trusts as a legal structure have existed for centuries, data trusts are relatively novel. At present, there is no universal or standard model for data trusts, as each structure must be curated to address its unique circumstances and risks.[24]

The digital fiduciary is another novel concept at law. It should be clearly demarcated from a related but different framework articulated by Jack Balkin and Jonathan Zittrain known as the Information Fiduciary Model.[25] The latter model posits that special relationships of trust and confidence arise between doctors, lawyers, or accountants and their customers not only due to legal contractual language, but also due to the exchange of sensitive personal information between the parties:[26]

An information fiduciary is a person or business who, because of their relationship with another, has taken on special duties with respect to the information they obtain in the course of the relationship. People and organizations that have fiduciary duties arising from the use and exchange of information are information fiduciaries whether or not they also do other things on the client's behalf, like manage an estate or perform legal or medical services. Because most professional relationships are fiduciary relationships, most professionals are also information fiduciaries. And that means, in particular, that professionals have duties to use the information they obtain about their clients for the client's benefit and not to use the information to the client's disadvantage.[27]

Since online service platforms handle similarly sensitive data to lawyers and doctors, Balkin argues that such duties should extend to large online platforms.[28] Moreover, these fiduciary duties "run with the data" and do not require the formation of a specific contract between the individual and the data handler, easing the burden on individuals to use these platforms with reduced concern that their sensitive information is being mishandled.[29] Balkin posits that although these duties do not necessarily extend to advertisers that leverage data, they should certainly extend to online service providers, "especially if you trust and depend on them."[30] For reasons of information asymmetries, user dependence, representations of expertise and good faith made by these platforms, and – most significantly – the potential for abuse, Balkin argues that fiduciary duties should be *imposed* by the government onto these platforms.[31]

On the other hand, Richard Whitt argues that *voluntary* adoption of fiduciary duties by a willing entity is a more feasible and prudent approach.[32] After Balkin published the Information Fiduciary ("IF") model, but before Whitt published his work, Lina Khan and David Pozen issued their own paper critiquing the IF model.[33] Similar to the arguments noted above, Khan and Pozen focus on the fiduciary duties that the directors of Facebook and Google owe to shareholders, and that the government mandated nature of the duty of loyalty attending the IF model would impede such duties by lowering the ability of Facebook or Google to monetize their data.[34] The mandated IF model would also risk violating the First Amendment.[35]

Whitt instead posits that the rich history of fiduciary obligations, rooted in the common law, can evolve, just as common law doctrines do, to apply to new digital applications.[36] He discusses at length not only the IF model noted above but also the idea of what he terms a Digital Trustmediary ("DTM"). This DTM model "involves entities providing advanced digital service to their clients, while ***voluntarily*** operating under heightened fiduciary duties of loyalty, care, and confidentiality."[37] These DTM entities would arise from commercial contracts, codes of conduct, or other agreements between the user and the data handler.[38] Built upon *trust*,

rather than on the technology,[39] the fiduciary's client would have an "actual understanding" of the fiduciary relationship,[40] thus allowing both parties to maximize the benefit of the relationship. This memo addresses the latter instance of the "opt-in" digital fiduciary, operating under a duty of loyalty towards its patrons.

Comparing Trusts and Contractual Fiduciary Duties

Fiduciary law in general offers the potential of providing protective measures to individuals who are too often left vulnerable online. This can be the case whether the individual is dealing with large tech companies or with smaller scale collaborative projects. Individuals may be forced to depend on services that accumulate and store personal data that can actually harm the data subject (e.g. behavioral and targeted advertising).[41]

Applying trust law principles and practices to data may begin to remedy these situations. Under one scenario, for example, a legislative body could apply a statutory duty of care (reasonable conduct, do no harm standards) and bailment requirements (safekeeping of property interests standard) to any entity that collects and stores and shares personal data. By contrast, entities seeking to become data trusts or digital fiduciaries could adopt a higher level duty of loyalty that runs with its beneficiaries.

Other proposals have recommended imposing fiduciary obligations on organizations that control data and rely on user trust.[42] Legislation introduced in the Senate has also put forth assigning fiduciary obligations on Internet Service Providers.[43] If enacted, such legislation could allow the Federal Trade Commission ("FTC") or state attorneys general to decide penalties for breaching these duties.[44]

Another approach for establishing fiduciary duties is through contractual obligations.[45] Traditionally, fiduciary duties were viewed as determining the course of action to suit the beneficiary through a general relationship-governance framework. This is in contrast to contracts, which spell out responsibilities of the parties before the relationship is formalized. Fiduciary duties offer some benefits for trusts; however, because some subscribe to the idea that a trust is a type of contract, the question remains as to whether trusts are distinct from ordinary contracts.

For example, contract parties are able to equitably breach certain obligations while trust parties cannot. While the contractual obligations of parties are bound by contract, even ironclad duties in trust law can be waived if a provision in a contract states as much. Furthermore, although trust fiduciaries are bound by the duties of loyalty and care, contract parties generally are bound only by good faith.

Some courts have recognized contractual fiduciary duties where (1) a duty of loyalty is not automatically invoked due to the nature of the fiduciary relationship and must be added contractually; or (2) non-fiduciary relationships where the parties wish to add a duty of loyalty. The former was introduced in *Gatz Properties, LLC v. Auriga Capital Corp.* (2012).[46]

The Third-Party Doctrine: Legal Origins

The boundaries of the third-party doctrine were outlined in *United States v. Miller* (1976) and *Smith v. Maryland* (1979): once an individual discloses information to a third party, that individual forfeits any reasonable expectation of privacy they may have had in that information.[47] In other words, the individual assumes the risk that this information may be revealed to law enforcement[48] and there are no fiduciary duties of care and loyalty, or duties under bailment, or any other legal duties that can protect the individual's interest in their data.

United States v. Miller (1976)

In *United States v. Miller*, the Court held that the third-party doctrine applies to bank records. In the course of an investigation of Miller, federal agents served subpoenas to two banks demanding production of all records and accounts in Miller's name.[49] Miller raised a Fourth Amendment challenge to the government's acquisition (i.e. the government's seizure) of these bank records.[50] The Court held that Miller had no protected Fourth Amendment interest in the bank records.[51] The Court stated, "the checks are not confidential communications but negotiable instruments to be used in commercial transactions. All the documents obtained… contain only information voluntarily conveyed to the banks and exposed to their employees in the ordinary course of business."[52] The third-party doctrine effectively means that when a person shares information with a third party, that person relinquishes control over that information so that it belongs to the third party instead of the person. In response to *Miller*, Congress passed the Right to Financial Privacy Act (1978), which provided consumers with an opportunity to object to government requests to financial records.[53]

Smith v. Maryland (1979)

Three years after *Miller*, in *Smith v. Maryland*, police asked a phone company to install a monitoring device to record the numbers dialed from Smith's home phone line.[54] The phone company installed a "pen register", a device that records numbers dialed from a particular phone line, at the phone company's headquarters.[55] The pen register revealed that Smith's phone was used to call the victim.[56] Smith argued that the government-induced installation of the pen register to record his numbers dialed was a Fourth Amendment search.[57] The Court held that this was not a search, and that Smith had "no actual expectation of privacy in the phone numbers he dialed, and that, even if he did, his expectation was not 'legitimate.'"[58] The Court reasoned that when Smith used his phone and dialed the phone number, he "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers dialed."[59] The dissent in this case disagreed with the idea that a caller assumes the risk that the phone company will disclose the numbers dialed to the police.[60] In response to *Smith*, Congress passed the Electronic Communications Privacy Act (1986), which provides some protections to prevent private communications from being intercepted by another private actor.[61]

Legal Analysis: *Carpenter*

Overview of the Case

Decades after *Smith*, in *Carpenter v. United States*, the FBI obtained 12,898 cell-site location information (CSLI) points cataloguing Carpenter's movements over 127 days, which showed he was near four robbery locations at the time those robberies occurred.[62] The Court held that when the government accessed CSLI from the wireless carriers, it "invaded Carpenter's reasonable expectation of privacy in the whole of his physical movements."[63] The Court relied on *Katz v. United States*, which held that a person has a "reasonable expectation of privacy" protected by the Fourth Amendment when making a phone call from a telephone booth.[64] The Court recognized that there was a qualitative difference between the "limited types of personal information address in *Smith* and *Miller*, and the exhaustive chronicle of location information casually collected by wireless carriers today."[65]

According to the Court, collecting and tracking CSLI is more akin to the facts of *United States v. Jones*, where the government's installation of a GPS device on the defendant's car, and its use of that device to monitor the vehicles' movements, constituted a search within the meaning of the Fourth Amendment.[66] CSLI, like GPS tracking, allows the government to "chronicle a person's past movements" through "detailed, encyclopedic, and effortlessly compiled" cell phone location information.[67] These tracking tools are more cost effective and easier to implement than other traditional investigative methods, and they reveal "not only particular movements, but… familial, political, professional, religious, and sexual associations."[68] The difference is that CSLI is even more invasive on an individual's privacy than GPS tracking because people carry cell phones on their person at all times, "beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[69]

The retrospective feature of CSLI also made the Court hesitant to allow police to freely access it, effectively "travel[ling] back in time to retrace a person's whereabouts… for up to five years."[70] The automatic and continuous recording of CSLI for every person, not just those under police investigation, would provide police with the power to track anyone, without even knowing in advance whether they want to follow them.[71] The Court saw this as affording police too much ability in circumventing Fourth Amendment protections.[72]

Gorsuch's Dissent

Gorsuch's dissenting opinion in *Carpenter* expressed skepticism with respect to the third party doctrine's ability to survive in the modern digital age.[73] He noted that most internet companies "maintain records about us and, increasingly, for us."[74] In the past, these records, including private information, would have been locked away or destroyed but now exist in potential perpetuity on third party servers.[75] The third-party doctrine assumes that no one reasonably expects any of this information to be kept private, but in reality, most people *do* expect that information they give to third parties will be kept in confidence.[76] He noted the Fourth Amendment provides protection of your "persons, houses, papers and effects, against unreasonable searches

and seizures" and in some circumstances the data you entrust to internet companies can be considered "modern-day papers and effects," entitled to the same level of protection.[77] CSLI is also "customer proprietary network information" which cannot be disclosed by carriers without the customer's consent.[78] Gorsuch contemplated that because customers have "substantial legal interest" in their CSLI, "including at least some right to include, exclude, and control its use," these interests may even be deemed a property right.[79] Gorsuch suggested that Carpenter could have prevailed on a trespass test used in *United States v. Jones* and *Florida v. Jardines*.[80]

There is a stark difference between consenting to allow a third party access to your property and consenting to allow the government to search that property.[81] Gorsuch described entrusting your property to internet companies as a bailment, which is "the delivery of personal property by one person (the bailor) to another (the bailee) who holds the property for a certain purpose."[82] As noted above, bailees owe a legal duty to protect property.[83] Gorsuch observed, "just because you *have* to entrust a third party with your data doesn't necessarily mean you should lose all Fourth Amendment protections."[84]

Ultimately, Gorsuch agreed with the majority's decision but disagreed with the majority's reasoning. He agreed that law enforcement agencies need a warrant to access cell phone data, but rather than applying the *Katz* reasonable expectation of privacy test, Gorsuch argued that CSLI records are the property of the cell phone owners, and, under the Fourth Amendment, law enforcement agencies cannot search a person's property without a warrant. In order for the government to secure a timely and reasonable warrant, it would need to articulate probable cause to search and restrict the search to a reasonable timeframe, instead of obtaining access to all available records. If law enforcement is capable of obtaining a warrant, companies must comply with the request.

Applying Gorsuch's Dissent to Data Fiduciaries

First, Data as Property

Gorsuch's dissenting opinion in *Carpenter* sets forth the idea that data can be interpreted through the lens of bailment and the general common law of obligations. In applying bailment principles to data, internet companies become the bailees that warrant the safe-keeping of the user-bailor's data. Bailments can be expressly agreed to by written terms of a contract (i.e. the Terms of Use), or they can be implied by conduct. Going a step further, though, fiduciaries and trustees at common law have duties beyond those typically imposed on bailees.

Employing a bailment, trust, or fiduciary obligation to personal data may necessitate the acceptance of data as property. However, this is not settled law. For example, as Whitt observes, because fiduciary law is considered relational between two people, the legal basis of the relationship "is limited only by what is deemed important to the entrustor."[85] This includes, importantly, "relational information" – knowledge gained by the entrustee as

a result of the fiduciary relationship.[86] As Whitt concludes, "entrusted power relationships encompass many forms of tangible and intangible 'stuff,' often of a deeply personal nature…."[87]

Property is "anything that is owned by a person or entity" and is generally understood as one of two categories: real property, such as land and real estate, and personal property, such as movable items.[88] Data is unique, however, because the very concept and nature of data is not clearly understood under the law.[89] Data is often discussed in abstract terms, and not specifically defined as a resource, good, activity, or other attribute.[90] Given the four traditional economic "factors of production" (buckets of land, labor, capital, and entrepreneurship), data could be any one of these, a combination of these, its own separate factor, or no factor at all.[91]

One school of thought, for example, perceives personal data as a form of labor.[92] Under the Lockean labor theory, property ownership follows from one's exertion of labor upon a certain raw item.[93] In the context of data, consumers could be the party exerting labor by creating data through the movement of their thumbs and creation of electronic signals that constitute our data. On the other hand, internet companies can also be considered as the laboring party because such companies both use the data signals stemming from our typing and build and maintain the content distribution servers upon which we rely.

Currently, the Web's status quo is "free data for free services," where users do not pay to use digital services, but are also not compensated for the data they produce.[94] Data that users generate is often viewed from a lens of consumption rather than production – as "capital rather than as labor."[95] This attitude undermines the productive value of user data. When data is viewed as capital, it is treated as "natural exhaust from consumption to be collected by firms," while data as labor is treated as "user possessions that should primarily benefit their owners."[96] Data as capital perpetuates the myth that online activity is a social contract of "free services in exchange for prevalent surveillance."[97] Data as labor recognizes the substantial value of user data in a wide range of applications, for example, in fueling input for artificial intelligence machine learning. Adopting a data as labor approach in connection with the Lockean labor theory can provide an avenue to accepting data as property.

Appreciating data as real property or an asset gives individuals – not just tech companies – the opportunity to claim legal ownership of their data, and the ability to extract value from it.[98] Yet the concept of personal data ownership is complicated by the fact that some elements of personal data are held by multiple parties and are publicly available.[99]

Second, Lowest Cost Avoidance

Gorsuch's discussion of bailment implies that the data we provide to third parties is, in essence, just like property that the bailee has a duty to reasonably protect. For example, as noted in *Carpenter*, when you toss your keys to your car to a valet, you do not expect the valet to "lend your car to his buddy."[100] Likewise, you certainly do not expect the valet to allow someone to go look under the seats in the hopes of finding something

incriminating against you, the car owner. Like a parking valet, a data fiduciary and/or data bailee may have extremely good reasons to violate their duties. Per *Katz*, however, the reasonable expectation is that he or she will not do so. Otherwise, what is the point of going to the restaurant, the dry cleaners, or the inn, in the first instance?

A bailee is expected to keep property safe. A fiduciary is expected to go further than that, however, since the bailee does not often obtain a material benefit from holding the property. Moreover, the bailee typically does not owe a strong duty of loyalty to the bailor – return of the property unharmed is sufficient to satisfy the duty of care.

By allowing the data trust or fiduciary to hold and monetize this property-like intangible asset for countless users, the trust/fiduciary becomes the party that is best positioned to assess, analyze, and investigate how best to use that asset. Following Gorsuch's examples in *Carpenter*, consider the costs that the individual would have to incur if she were forced to check for all actual and potential conflicts of interest, instead of allowing the trustee/bailee to do so. For example, she would have to ensure that the valet taking your keys does not have extreme debts or rambunctious friends that could incentivize the valet to sell your car or allow the friend to drive it, rather than simply trusting the restaurant or valet himself to avoid harming your interests.

These investigatory costs are simply too great for the individual to be expected to handle. The law has evolved to protect our expectations that those in possession of our things shall act in a manner to keep our things safe (bailment) and to promote its value (trusts and fiduciary duties). This principled expectation should extend to data-based fiduciaries because the cost – for the individual – of ensuring that no conflicts of interest arise is excessive and unreasonable. In fact, it would be *impossible* for an individual to ensure that no conflicts arise when her location and personal data is constantly being transmitted to countless cellular networks, advertising companies, data brokers, and other information processors, all in the background of our applications. As a matter of pragmatism, therefore, the lowest-cost avoider is not the individual, but the data holder, who, by holding our property, should be expected to act in our best interest. However, unlike the restaurant, where if the valet takes your car for a joyride, you can simply eat elsewhere and sue for conversion, the analogies from Gorsuch's dissent in Carpenter start to lose relevance. This is because, quite simply, your cellphone is the only restaurant in town. Thus, the duty to act as a fiduciary when holding individuals' data should only be *enhanced*, since the individual at some point or another is going to have to grab a bite to eat.

Third, Burdens of Proof

When a bailee loses or converts property, or a fiduciary embezzles money, the proof required to successfully sue the law-violating individual is quite straightforward: one person/entity had possession of your property; some of your property is missing; thus that person/entity must have violated a legal duty.

However, in the context of electronic information shared with law enforcement, the burden of proof to claim a 4th Amendment violation becomes insurmountable for the average individual. Unless you get a police officer knocking on your door, it is nearly impossible for an individual to prove that Google, Amazon, Facebook, or any of the hundreds of applications on your phone shared your sensitive data and information with law enforcement without a warrant in violation of the 4th Amendment. Even then, it would be extremely difficult for the individual to prove that the private company was acting as an instrument of the state and violated the 4th Amendment, rather than the state itself.[101] Additionally, it is difficult to trust that Facebook will use adequate *procedural* mechanisms in making a "good faith" decision that the law requires the company to share its users' data with law enforcement.[102]

The law needs to evolve to eliminate such corporate-focused protections and instead shift the burden to the *company* to show that it did not violate the 4th Amendment, or at the very least the company should follow a set of principled standards in deciding whether to share this information with law enforcement. As noted above, such companies are already in a much better position than the individual to access this information.

Fourth, Incentives

The Court noted in *Coolidge* that "it is no part of the policy underlying the Fourth and Fourteenth Amendments to discourage citizens from aiding to the utmost of their ability in the apprehension of criminals."[103] Thus, companies like Google, Facebook, Amazon, and Apple are faced with little to no disincentive to provide sensitive information to the government and may in fact have an affirmative incentive to share this data in a privacy-invasive manner. Standing alone, this positioning does not seem to create any issues; after all, what do we have to hide from law enforcement?

But when viewed in the context of a voluntary data fiduciary, where we provide that entity with our immensely valuable digital assets (our property) due to the trust-based nature of the relationship and the sensitivity of the information, the subsequent disclosure of that information without notice to law enforcement becomes less appropriate. In essence, the fiduciary "stands in the shoes" of its client, customer, or patron when the government seeks her data. Like the attorney-client relationship and the corresponding privilege rights, we expect that person or entity to vehemently protect our information, *even if we have nothing to hide*. To somehow find under the 4th Amendment (rather, the third party doctrine's exception to the 4th Amendment) that a data-focused company provides almost no protection other than an ostentatious claim to act in "good faith"[104] with law enforcement access requests, and likely protect our information with significantly lower care than we would ourselves, is a result contrary to both logic and law. As Gorsuch explained, there is no assumption of risk to a 4th Amendment search or seizure by simply using your phone.[105] A new approach is needed, premised on the human trust-based nature of any individual's ongoing relationship with a fiduciary. We need to recognize the lawful place of the Fourth Amendment Fiduciary.

Application and Conclusion

The law has already evolved substantially to give effect to certain principles regarding the collection and use of data. For example, Europe's General Data Protection Regulation and the California Consumer Privacy Act (and soon the California Privacy Rights Act) all enforce permutations of certain concepts such as notice, choice, transparency, and consent. These laws give control back to users over their data. And yet the Third Party Doctrine eviscerates any fair interpretation of these fundamental concepts because it involves purely *ex parte* negotiations and communications between private technology companies and the state. Thus, all these laws do from a law-enforcement access standing point is allow companies to place hard-to-find representations of "good faith" efforts in their privacy policies to avoid potential liability.[106]

There are a few examples outside the context of privacy policies where companies affirmatively display and represent to consumers an intent to provide certain rights. Many of these representations are the product of privacy legislation. For example, under the CCPA, websites must have a page called Do Not Sell My Personal Information that allows consumers to opt-out of the sale of personal information. Meanwhile, other efforts are actually made in response to *avoid* legal requirements. For example, warrant canaries are voluntary notices on a company's website which state that a company has *not* complied with a government data access request under, for example, the Foreign Intelligence Surveillance Act, in a certain number of days.[107] Usually, when the government orders the production of information from a technology company through a subpoena, there is a corresponding gag order.[108] Warrant canaries are industry efforts to toe the line of the law and explain to their consumers that the company has, in fact, disclosed its customers' information.

Alternatively, a new approach can combine common-law property rights with the *Katz* reasonable expectation of privacy test. In property law, individuals tend to have a greater expectation of privacy in both real and personal property that belongs to them. When applied to data collected and held by an organization, the question becomes: What kind of legal interest is sufficient to make something *yours*?

Complete ownership or exclusive control may not be necessary to assert one's Fourth Amendment right. As noted above, because the nature of data is not well-determined under law, it is also conceivable that ordinary property law is not sufficient to cover the potential harms from breaching fiduciary duties. For instance, even paying for an Uber, hotel room, or telephone booth has been shown to produce a sort of license to temporarily use or control a space.

There are a number of options available for internet companies seeking to become data fiduciaries, and fully protect the interests of their patrons. As noted above, while the prescriptive imposition of legislation is not necessary, given the voluntary nature of the entrustor-entrustee relationship, legislative bodies could pass laws, such as the ACCESS Act, that create powerful incentives for entities to become data fiduciaries.[109] Entities on their own also could adopt and implement best practices, codes of conduct, or self-certification regimes.[110]

Another path is creating an entirely new profession for digital agents. Much like a physician or an attorney, the digital fiduciary agent would hold itself out as the member of a professional guild of experts. As Whitt notes, treating a digital trustmediary as its own profession, complete with enforceable codes of conduct and disciplinary processes, also "can qualify for special treatment under the U.S. Constitution."[111] Godwin and others have argued that such entities should have legal standing to defend their clients' Fourth Amendment rights against government searches and seizures[112]. To the extent that analysis, buttressed here, proves correct, "a professional DTM becomes all the more attractive to would-be clients."[113]

Exactly how this road to the Fourth Amendment Fiduciary" plays out in the near term is unclear. Perhaps entities should form a consortium, similar to lawyers and doctors, that abides by the common law of obligations and acts under a code of conduct that *voluntarily* imposes fiduciary duties to the handling and disclosure of users' data. Professional fiduciaries of this kind typically use contracts to formalize the fiduciary relationship with their clients. Alternatively, an internet company could use its terms of service and privacy policy to act as a contract that spells out the nature of the fiduciary relationship. Too often, though, the average consumer will not read the privacy policy or Terms of Use. Another option could be for the company to post a seal or similar watermark on its website, app, or marketing materials that signals to consumers the approach to which the company will take when handling data access requests from law enforcement.

Regardless of how the fiduciary relationship is formed and instantiated, the larger conclusion remains. The digital trustmediary should be able to act on behalf of its clients and patrons, as the "constitutional floor below which Fourth Amendment rights may not descend".[114]

Footnotes

0. U.S. Const. amend. IV. ↩
0. *Smith v. Maryland* , 442 U.S. 735, 743-44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."). ↩
0. Richard M. Thompson II, Congressional Research Service, *The Fourth Amendment Third-Party Doctrine* (June 5, 2014) [https://sgp.fas.org/crs/misc/R43586.pdf]. State laws can provide more rights than federal laws. The third-party doctrine is a constitutional floor, meaning states can limit its application via statute and provide more rights to its residents. ↩
0. *Id.* ↩
0. *Trust*, law.com Legal Dictionary, https://dictionary.law.com/Default.aspx?selected=2169 (last visited Jan. 14, 2022). *See* Betsy Simmons Hannibal, *Common Questions: Trusts*, Lawyers.com (Mar. 22, 2019) https://lawyers.com/legal-info/trusts-estates/common-questions-trusts.html#1. ↩
0.

Mary Randolph, *The 'Executor' of a Trust - The Trustee*, AllLaw.com, https://www.alllaw.com/articles/nolo/wills-trusts/successor-trustee.html (last visited Jan. 14, 2022).

↩

0. Adam Hayes, Investopedia, *Trust Property*, https://www.investopedia.com/terms/t/trust-property.asp (last updated mar. 27, 2021). ↩
0. Julia Kagan, Investopedia, *Trust*, https://www.investopedia.com/terms/t/trust.asp (last updated Oct. 19, 2020). ↩
0. *Id*. ↩
0. Adam Barone, Investopedia, *What Are Some Examples of Fiduciary Duty?*, https://www.investopedia.com/ask/answers/042915/what-are-some-examples-fiduciary-duty.asp (last updated Nov. 20, 2021). ↩
0. NYSARC Trust Services, *What is a Pooled Trust?*, https://www.nysarctrustservices.org/nysarc-trusts/pooled-trusts (last visited Jan. 14, 2022); Commonwealth Community Trust, *CCT's Multiple Portfolio Investment Model*, https://commonwealthcommunitytrust.org/medicare-set-aside/investment-information (last visited Jan. 14, 2022). ↩
0. Amy Feldman, Barron's, *Trust Costs Go Up; Get Ready to Negotiate*, https://www.barrons.com/articles/SB513675781168750046937045804863919457838 42 (last visited Jan. 14, 2022). ↩
0. *Id*. ↩
0. Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 Santa Clara High Tech. L. J. 75, 90 (2020). ↩
0. *Id*. ↩
0. *Id*. ↩
0. *See*, e.g., privacy policies from Facebook https://www.facebook.com/policy.php and Apple https://www.apple.com/legal/privacy/en-ww/. ↩
0. Peter Wells, Open Data Institute, *UK's first data trusts to tackle illegal wildlife trade and food waste* (Jan. 31, 2019), https://theodi.org/article/uks-first-data-trusts-to-tackle-illegal-wildlife-trade-and-food-waste/. ↩

0. Jack Hardinges, Open Data Institute, *What is a data trust?* (Jul. 10, 2018) https://theodi.org/article/what-is-a-data-trust/. ↩
0. Sylvie Delacroix and Neil Lawrence, *Bottom-Up Data Trusts: Disturbing the 'One Size Fits All' Approach to Data Governance*, International Data Privacy Law (2019), doi.org/10.1093/idpl/ipz014. ↩
0. *Id*. ↩
0. *Id*. ↩
0. *Id*. ↩
0. A browser such as Mozilla's Firefox could serve as a technical extension of the trust/fiduciary, including having embedded duties of care/loyalty embedded in the code. But that would not obviate the need for a huma being somewhere "in the loop." ↩
0. Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. Davis L. Rev. 1183 (2016). ↩
0. *Id*. at 1207. ↩
0. *Id*. at 1209. ↩
0. *Id*. at 1221. ↩
0. *Id*. at 1220. ↩
0. *Id*. ↩
0. *Id*. at 1222. ↩
0. Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations of Loyalty and Care in the Digital Platforms Era*, 36 Santa Clara High Tech. L. J. 75 (2020). ↩
0. *Id*. at 79. ↩
0. *Id*. at 84. ↩
0. *Id*. at 85. ↩
0. *Id*. at 101. ↩
0. *Id*. at 75 (emphasis added). ↩
0. *Id*. at 107 (emphasis added). ↩

0. *Id*. at 108. ↩
0. *Id*. at 108. ↩
0. Kashmir Hill, *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did*, Forbes (Feb. 16, 2012), https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/. ↩
0. Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 Harv. L. Rev. 497, 499-500 (2019). *See also* Whitt, *Old School Goes Online*, at 122-124 (describing the Data Care Act of 2018 and ACCESS Act of 2019). ↩
0. Khan and Pozen, at 501. ↩
0. *Id*. at 525. ↩
0. Adam S. Hofri-Winogradow, *Contract, Trust, and Corporation: From Contrast to Convergence*, 102 Iowa L. Rev. 1691 (2017). ↩
0. *Gatz Properties, LLC v. Auriga Capital Corp.*, 59 A.3d 1206 (Del. 2012). ↩
0. *Smith v. Maryland* , 442 U.S. 735, 743-44 (1979). ↩
0. *Id*. at 744. ↩
0. *United States v. Miller*, 425 U.S. 435, 437 (1976). ↩
0. *Id*. at 439. ↩
0. *Id*. at 440. ↩
0. *Id*. at 442. ↩
0. Matthew N. Kleiman, *The Right to Financial Privacy Versus Computerized Law Enforcement: A New Fight in an Old Battle*, 86 NW. U. L. Rev. 1169, 1187 (1992). ↩
0. *Smith v. Maryland* , 442 U.S. 735, 737 (1979). ↩
0. *Id*. ↩
0. *Id*. ↩
0. *Id*. at 738. ↩
0. *Id*. at 745. ↩

0. *Id*. at 744. ↩
0. *Id*. at 747. ("Implicit in the concept of assumption of risk is some notion of choice.") *Id.* at 749. ↩
0. Electronic Privacy Information Center, *Electronic Communications Privacy Act (ECPA)* https://epic.org/ecpa/ (last visited Jan. 14, 2022). ↩
0. *Carpenter v. United States*, 138 S. Ct. 2206, 2212-13 (2018). ↩
0. *Id*. at 2219. ↩
0. *Katz v. United States*, 389 U.S. 347, 360 (1967). ↩
0. *Carpenter*, 138 S. Ct. at 2219. CSLI is much more personally revealing in nature than call logs and bank statements. *See id.* at 2223 ("In light of the deeply revealing nature of CSLI, its depth, breaths, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that it is collected by a third party does not make it any less deserving of Fourth Amendment protection."). ↩
0. *Id*. at 2216. ↩
0. *Id*. "A phone goes wherever its owner goes, conveying to the wireless carrier not just dialed digits, but a detailed and comprehensive record of the person's movements." *Id.* at 2217. ↩
0. *Id*. at 2217-18. ↩
0. *Id*. at 2218. ↩
0. *Id*. ↩
0. *Id*. ↩
0. *Id*. ↩
0. *Id*. at 2262. ↩
0. *Id*. ↩
0. *Id*. at 2261-62. ↩
0. *Id*. at 2263 ("People often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private."). ↩
0. *Id*. at 2269. ↩
0. *Id*. at 2272. ↩

0. *Id*. ↩
0. *Id*. at 2265 ↩
0. *Id*. at 2263. ("The fact that a third party has access or possession of your papers and effects does not necessarily eliminate your interest in them.") *Id*. at 2268. ↩
0. *Id*. at 2268. ("Entrusting your stuff to others is a *bailment*.") *Id*. ↩
0. *Id*. at 2268-69 ("A bailee normally owes a legal duty to keep the item safe, according to the terms of the parties' contract if they have one, and according to the 'implications from their conduct' if they don't."). ↩
0. *Id*. at 2270 (emphasis in original). ↩
0. Whitt, *Old School Goes Online*, at 89. ↩
0. *Id*. ↩
0. *Id*. ↩
0. *Property*, law.com Legal Dictionary, https://dictionary.law.com/default.aspx?selected=1645 (last visited Jan. 14, 2022). ↩
0. For an overview of data as potentially fitting a variety of economic and legal categories, see Richard Whitt, *Hacking the SEAMs*, 19 Colorado Tech. L. J., 19:1, 137, at 166-182. ↩
0. Paulius Jurcys, et al. *Ownership of User-Held Data: Why Property Law is the Right Approach*, https://jolt.law.harvard.edu/assets/digestImages/Paulius-Jurcys-Feb-19-article-PJ.pdf. ↩
0. Whitt, *Hacking the SEAMs*, at 175. ↩
0. Whitt, *Hacking the SEAMs*, at 175. ↩
0. *Lockean Labor Theory Law and Legal Definition*, USLegal.com, https://definitions.uslegal.com/l/lockean-labor-theory/ (last visited Jan. 14, 2022) (The Lockean labor theory, introduced by John Locke, is the "justification of private property that is based on the natural right of one's ownership of one's own labor, and the right to nature's common property to the extent that one's labor can utilize it."). ↩
0. Imanol Arrieta Ibarra et al, *Should We Treat Data as Labor? Moving Beyond "Free"*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3093683. ↩
0. *Id*. ↩
0. *Id*. ↩

0. *Id.* ↩

0. Paulius Jurcys, et al. *Ownership of User-Held Data: Why Property Law is the Right Approach*, https://jolt.law.harvard.edu/assets/digestImages/Paulius-Jurcys-Feb-19-article-PJ.pdf. ↩

0. *Id.* (Personal data ownership has been difficult to define because "there are elements of personal data that are publicly available basically for anyone" and "personal data sets can be held by various parties."). ↩

0. Gorsuch dissenting in *Carpenter*. ↩

0. *Coolidge v. New Hampshire*, 403 U.S. 443, 487. ↩

0. Facebook's Privacy Policy can be found at https://www.facebook.com/policy.php ("We access, preserve and share your information with regulators, law enforcement or others … [i]n response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so."). ↩

0. *Coolidge v. New Hampshire*, 403 U.S. 443, 487. ↩

0. *See* Facebook's privacy policy at https://www.facebook.com/policy.php. ↩

0. *See Carpenter*, Gorsuch dissenting ("... knowing about a risk doesn't mean you assume responsibility for it."). ↩

0. *See* Facebook's privacy policy at https://www.facebook.com/policy.php. ↩

0. *Warrant canary*, Wikipedia, https://en.wikipedia.org/wiki/Warrant_canary (last visited Jan. 14, 2022). ↩

0. *Id.* ↩

0. Bennett Cyphers and Cory Doctorow, *The New ACCESS Act Is a Good Start. Here's How to Make Sure it Delivers.*, Electronic Frontier Foundation, https://www.eff.org/deeplinks/2021/06/new-access-act-good-start-heres-how-make-sure-it-delivers (June 21, 2021). ↩

0. Whitt, *Old School Goes Online*, at 124. ↩

0. Whitt, *Old School Goes Online*, at 125. ↩

0. *Id.* ↩

0. *Id.* ↩

0. *Id.* ↩