An Expectations Based Privacy Framework for Management of Personal Data as a Common Resource

By Matthew Anderson

Aristotle, in his treatise on ethics, identified three forms of justice: distributive, rectificatory, and reciprocal.[1] Distributive justice deals with equality and just outcomes in society before anyone is wronged (e.g. racial or income equality); rectificatory justice deals with damages and remedies (i.e. tort law). The less used and understood form of justice is reciprocal justice. Reciprocity forms a more democratic, socialist, and fluid foundation for justice.[2]

For example, the right to a jury of your peers is clearly reciprocal – anyone could be a juror one day and the accused the next. Indeed, juries were one of the first common rights granted and practiced in feudal England that helped elevate all other rights. Juries were also the first institution altogether separate from the crown.[3] Juries, however, have reputations for being more arbitrary than judges and can even nullify the law with little recourse.[4] Some would argue, on the other hand, that seemingly arbitrary outcomes simply mean that juries are just better at determining the right exceptions to an overly rigid law.

The darker side of reciprocity is the ancient form of justice of "an eye for an eye and a tooth for a tooth."[5] The reciprocity of this retaliatory rule is not just in the mutual damage inflicted but rather in the license provided to an injurer's victim and peers to find identical retribution inside the law but outside of the state.[6] That is, the victim and their family were responsible for the retribution, providing an efficient, effective, peer-based deterrent to crime.

---

[1] Theodore Scaltsas, "Reciprocity and Justice: What Aristotle tells us about it!", BUSINESS THINKER, http://www.businessthinker.com/reciprocity-and-justice-what-aristotle-tells-us-about-it

[2] Adam Smith, The Theory of Moral Sentiments, Oxford UP: (Glasgow Ed. 1976) at I.i.I.10.

[3] Geoffery Robertson, "Magna Carta and Jury Trial" British Library. March 13, 2015. https://www.bl.uk/magna-carta/articles/magna-carta-and-jury-trial.

[4] Karen Bates, The Jury is Still Out on Why OJ Simpson was Acquitted, NPR, available at https://www.npr.org/sections/codeswitch/2014/06/12/321392845/the-jury-is-still-out-on-why-o-j-simpson-was-acquitted.

[5] The Bible, Exodus 21:24 (KJV).

[6] James Davis, Jesus and the Law of Retaliation, Bible.org, https://bible.org/seriespage/17-jesus-and-law-retaliation-lex-talionis-matthew-538-42.

Juries and retaliatory license historically dealt with crime, which is essentially an act against society. After such an act or alleged act, the interests of society are almost entirely reciprocal. While society needs punishment for such acts, the accuracy of that punishment is equally important. Thus, a jury equally identifies with the accused who pleads innocence and the victim who demands justice.

The empathy that allows for fair judgement by a jury of peers is hard to replicate in rules and institutions outside the visceral area of crime. Though some areas of commercial law utilize juries extensively as well, in particular intellectual property, the jury's application of justice in those situations is widely challenged.[7] Furthermore, direct reciprocal justice accomplished via empathy is more difficult to use outside of the court, in administrative regulations for example. If, however, the direct reciprocal relationship can be seen as a first order interaction, then the second order interaction (or next level of abstraction) of society's will would be expectations. The expectations of society as a whole are a median of what a citizen would expect of other reasonable citizens. For instance, what one would expect a jury, having certain evidence, to decide, which is already used as a rule of law canonized as the "no reasonable jury" standard for judgement as a matter of law (Federal Rule 50(a)).[8] Indeed, the philosopher John Rawls condensed all lawmaking and consensus building in complex democracies into this middle ground shared by reasonable people.[9] Given the apparent fundamental nature of this measurement standard in lawmaking, the application of this standard to the interpretation of laws seems reasonable. Nowhere is the use of this yardstick more apparent than in Fourth Amendment jurisprudence, which has condensed the reasonableness of a warrantless search down to a person's reasonable expectation of privacy.[10]

Recently during an interview with the Federalist Society, Justice Thomas of the United States Supreme Court was asked about the right to privacy in the context of "newly found rights" and specifically whether the expectations test was adequate.[11] First, Justice Thomas noted he did

[7] Loren Steffy, Patently Unfair, TEXAS MONTHLY, available at https://www.texasmonthly.com/politics/patently-unfair/
[8] Federal Rules of Civil Procedure, Rule 50(a).
[9] Joh Rawls, Encyclopedia of Philosophy, available at https://plato.stanford.edu/entries/rawls/
[10] United States v. Jones, 565 U.S. 400 (2012).
[11] Clarence Thomas, Justice Clarence Thomas at the Federalist Society, CSPAN, https://www.c-span.org/video/?450905-1/justice-clarence-thomas-speaks-federalist-society&et=editorial&bu=National%20Law%20Journal&cn=20180919&src=EMC-Email&pt=Supreme%20Court%20Brief

not disagree with the expectations test, but then stated he did indeed disagree.[12] Justice Thomas is rarely so undecided on a rule of law. Indeed, he commonly writes his own standards and rules whole cloth in lone dissents without deference to the opinions of the majorities or other dissents.[13] Justice Thomas is not alone in his indecision, even the famous Justice Holmes noted in an early privacy case, *Olmstead v U.S.*, that "[w]hile I do not deny it, I am not prepared to say that the penumbra of the Fourth and Fifth Amendments covers the defendant."[14]

Furthermore, Justice Thomas's indecision is certainly a more honest opinion than that of Justice Posner who has openly rejected privacy as a right altogether while also demanding heightened privacy standards for himself as a judge.[15] The hypocrisy of Posner highlights the importance of societal reciprocity as a touchstone for democratic law. In contrast, the uncertainty that Justice Thomas expressed with regard to the "penumbra of rights" theory of the Constitution centers on the uncertainty of the source and boundaries of these rights lying in the shadows of constitutional law.[16] While not all of the "newly found rights" have been created equal, the right to privacy planted as it is in the expectations of society is, I will argue, on solid ground.

This paper attempts to answer these uncertainties with respect to expectations, the Fourth Amendment, and privacy law. In a first part, the paper provides the philosophical foundation for reciprocity as the foundation for law and society. This first part also addresses the inherent upper and lower bounds of reciprocity that help keep any legal rule based on reciprocity constrained, constant, and fair. In a second part, the paper looks at how courts have utilized and adapted the expectations test for what constitutes a reasonable search. This adaptability is perhaps the strongest aspect of the expectations basis for search and seizure rules since facts vary so much from one search to the next. In a third part, the paper introduces several areas of privacy law that have adopted the expectations test of the Fourth Amendment along with a few areas of privacy law which could benefit from the application of the expectations test for clarity and consistency.

---

[12] Tony Mauro and Marcia Coyle, 'Expectation of Privacy'? Thomas Asks: 'Where Does This Stuff Come From?', National Law Journal: Supreme Court Brief (Sept. 19, 2018).
[13] Ian Millhiser, Clarence Thomas is the most important legal thinker in America, THINK PROGRESS, https://thinkprogress.org/clarence-thomas-most-important-legal-thinker-in-america-c12af3d08c98/.
[14] Olmstead v. U.S., 277 U.S. 438, 469 (1928)
[15] Mike Masnick, Judge Posner Says NSA Should Be Able To Get Everything & That Privacy Is Overrated, TECHDIRT, https://www.techdirt.com/articles/20141208/14063329364/judge-posner-says-nsa-should-be-able-to-get-everything-that-privacy-is-overrated.shtml
[16] See generally Griswold v. Connecticut, 381 U.S. 479 (1965); see also supra note 11.

A. RECIPROCITY AS A SELF-BOUNDED BASIS FOR LAW

Besides Rawls who dealt with the building of consensus in politics via reciprocity or reasonableness, two other thinkers have highlighted reciprocity as being the framework of complex, equal societies. The first is Adam Smith, the author of The Wealth of Nations, who, in his book The Theory of Moral Sentiments, attempted to structuralize how societies develop the boundaries of morals. The second is Elinor Ostrom, the only female Nobel Prize winner in Economics, who pioneered theories on reciprocity in public common resources (like privacy). Together, these explanations of how society reaches consensus provide a template for reaching consensus on privacy law and a framework for applying the expectations test to the right to privacy.

I. Reciprocity and the Golden Rule

In the beginning of his book, The Theory of Moral Sentiments, Adam Smith asks how society is able to develop such a rigorous set of social behavior requirements without laws, rules, or even open explanations. The founders of economic theory, Adam Smith, David Hume, and John Stewart Mill, to name a few, were far ahead of modern economic theory which assumes all rational agents to be selfish.[17] David Hume, in fact, took this modern fancy of selfishness, dreamt up by Chicago-school economists, as the initial strawman on which to build his utilitarian reciprocity model of moral law.[18]

David Hume, who could be considered one of the first humanists, argued that individuals make decisions, and society reinforces decisions, that move the median welfare of society forward.[19] This judging mechanism for actors requires not only that the individual estimate the median welfare and society's desired direction of progress, but also requires that those judging or affirming the individual's action do the exact same calculation before affirming or objecting to the action.[20] Judging the outcome of an act on all of society along with the desired outcome of society in that situation is not second nature to humans who typically rely on one-to-one empathy to guide their reciprocal interactions.

---

[17] David Hume, A Treatise on Human Nature: Book III, 492-494 (Oxford UP: 1896); Adam Smith, The Theory of Moral Sentiments, Oxford UP: (Glasgow Ed. 1976) at I.i.I.10; contra Burton Malkiel, The Efficient Market Hypothesis and Its Critics, CEPS Working Paper No. 91, (April 2003).
[18] Hume, at 494-496.
[19] Hume, at 496-500.
[20] Hume, at 499.

A simpler, and therefore better,[21] moral rule is the Golden Rule which incorporates direct reciprocity. "Do unto others as you would have them do unto you," the maxim goes.[22] This rule has two parts: direct empathy and reverse empathy. That is, first, how do I think the other person will receive this action, and second, if I were that person how would I receive this action. This logic is far easier for the human mind and emotions to process instinctively than estimated societal outcomes. Almost identical to this pairing of direct and reverse empathy is the expectations test of Fourth Amendment jurisprudence which can be formulated as: "do I expect privacy from others here, and if I were the average third party would I be given privacy (or have a reasonable right to privacy given) by them here?" Hopefully this simple comparison does not give away the whole paper.

The similar structure of these moral rules from different millennia and different contexts is not coincidence. These two moral rules summarize two separate feedback loops that together govern much of the consensus building in society. Adam Smith proves reciprocal morality by illustrating these two feedback loops. Despite apparent uncertainty as to how sympathy or emotion towards things is caused, Smith argues that empathy arises from our emotional imagination using reciprocity. His treatise sets out the following foundational axioms. First, that we encourage and are excited by the correspondence of sympathy amongst our peers;

> The mirth of the company, no doubt, enlivens our own mirth, and their silence, no doubt disappoints us. [TMS, I.i.2.2]

Second, that people enjoy offering corresponding sympathies; and

> [a]s the person who is principally interested in any event is pleased with our sympathy, and hurt by the want of it, so we, too, seem to be pleased when we are able to sympathize with him and hurt when we are unable to do so. [TMS, I.i.2.6]

Third, that the propriety of a sentiment is judged by comparison with our own.

> [w]hen the original passions of the person principally concerned are in perfect concord with the sympathetic emotions of the spectator, they necessarily appear to this last just and proper…and, on the contrary, when, upon bringing the case home to himself, he finds that they do not coincide with what he feels, they necessarily appear unjust and improper [TMS, I.i.3.1]

[21] Occam's Razor
[22] The Bible, Matthew 7:12 (KJV).

From these axioms, one feedback loop becomes clear whereby we encourage sympathy of the same kind as our own. When positive, we encourage positive; when negative we encourage negative. Furthermore, we are happy to offer corresponding sympathy as well, and are sad when we cannot. Thus, this feedback loop, if allowed to continue, would build towards a polarized set of sentiments where all things are universally, utterly hated or loved. What reigns in society's tendency towards complete aversion and complete infatuation with those things deemed respectively despicable and lovable?

The first loop, thus far, is summarized by Smith as a tautology:

> To approve of another man's opinions is to adopt those opinions, and to adopt them is to approve of them. [TMS, I.i.3.2]

Smith answers the question of what limits this primary loop by pointing to the fact that at some point the primary feedback loop reverses. Indeed, there is a secondary feedback loop that requires agreement in degree as well. The man who laughs too hard at our joke is reviled alongside the man who did not laugh at all.[23] In a pair of two people, this feedback may not be useful (e.g. even though we feel that our friend has laughed too hard, we cannot be assured unless the company of people alongside him reacts in kind to our lower expected level of sentiment). This is one reason isolated minorities become more radical.

In the secondary loop, agreement or disagreement with another's level of reinforcement also warrants approval or disapproval, respectively (i.e. did they meet expectations). That is, over-reinforcement and under-reinforcement by individuals in a crowd reacting together generates instant embarrassment or awkwardness, respectively, amongst the outliers. Thus, the crowd is able to quickly build consensus.

Whatever the future interactions may hold, in the next instant both actors will only be positively reinforced (and enjoy the exchange of opinion) if they agree both on what should be approved and on the level of that approval. In large groups, or among diverse populations, this further requirement of positive feedback only upon agreement at equal levels quickly limits moral sentiment to small deviations from the median. Thus, individuals judge excess reinforcement not only as harmful but also as improper in view of the little occasion given for

[23] Smith, Theory of Moral Sentiments, at I.i.3.2.

it.[24] The result of the two feedback loops combined is essentially a self-checking, self-reinforcing, and self-limiting feedback system.

If society uses this feedback system to reliably constrain everything from sexual attraction to modest laughs, consensus on the expectations of society on the right to privacy in different situations is likely also built this way. Indeed, little is more fundamental to human interaction than privacy.[25] Similarly, the counterbalance to privacy between individuals is a constant curiosity and exchange of "secrets." If society's expectation of privacy and the individual's expectation of privacy are built in this way, then these expectations will hew tightly to a median rule useful for legal determinations. Furthermore, since humans use this reciprocal judgement mechanism every day in determining when to remain private, the legal outcomes will mirror the desired result of society. Finally, due to the use of the reciprocal mechanism every day in other social situations, police officers, perpetrators, and juries will also be able to apply consistent and quick evaluations of the right to privacy in a situation using the same familiar mechanism. Thus, Justice Thomas' concerns with the capriciousness of the expectations rule should be assuaged.

II. The Use of Reciprocity to Determine the Optimal Level of Use of a Common Resource

Privacy is increasingly becoming a common good, in the economic sense. Every day more data about our lives becomes collectable for little or no cost. The amount that we allow to be harvested and used is crucial. Overharvesting and exploiting data could destroy the fabric of society through cynicism, narcissism, and discrimination which thrive in low privacy environments.[26] Under-harvesting or destruction of data, on the other hand, would reduce the benefits of the digital revolution and destroy some social media business models altogether.[27]

---

[24] Id. at I.i.3.8.
[25] Plato, The Republic, Book III, 415e-416e.
[26] Rick Nauert, For Many, Narcissism Tied to Social Media Behaviors, Psych Central, https://psychcentral.com/news/2016/12/05/social-media-provides-forum-for-narcissistic-individuals-to-self-promote/113460.html; Hannah Devlin, Discrimination by algorithm: scientists devise test to detect AI bias, The Guardian, https://www.theguardian.com/technology/2016/dec/19/discrimination-by-algorithm-scientists-devise-test-to-detect-ai-bias.
[27] Barton Gellman, Facebook: You're Not the Customer, You're the Product, TIME MAGAZINE, http://techland.time.com/2010/10/15/facebook-youre-not-the-customer-youre-the-product/

Therefore, it is imperative that society quickly formalize their expectations of privacy to protect this common good and utilize it appropriately.[28]

Fortunately, Elinor Ostrom devoted her academic career to examining how societies dependent on limited but easily accessible resources have developed rules for managing those resources. Perhaps unsurprisingly at this point, her observation across societies was that many social systems used reciprocity to build consensus on use. In particular, where control and monitoring were expensive or private gain is high for those over-exploiting a resource, then reciprocal peer-based use systems are the most efficient.[29]

The new social media services of internet 2.0 generate volumes of data. Even if this data is not exploited by the service providers, others will still be able to scrape the data and exploit it. For instance, several counter-intelligence agencies and human resources companies utilized a script to scrape details of Linkedin profiles without Linkedin's permission and in violation of their Terms of Service.[30] So in any case, the nature of internet 2.0 is such that the data we share will be available to many people, whether on the open market or the grey market, and none of the sharing done between social groups can be done without releasing this information. While this vast pool of unaggregated data is integral to the use of social media, it is also valuable and potentially destructive if misused.

Furthermore, this vast pool of information is lying available to any technically sophisticated company. For instance, the Mercer family funded extensive data mining prior to the 2016 election using overnight server time in Europe and a few computer programmers with huge success.[31] The entry costs for those wishing to exploit this data are very low. Likewise, the large gains, whether monetary, electoral, or fraudulent, to any successful aggregator of the data are a powerful incentive. As a result, regulatory enforcement to prevent exploitation at any level would likely be costly or impossible (like preventing piracy of music). Therefore, governmental control may not be the answer in this case, but rather consumer-based monitoring and auditing.

---

[28] Elinor Ostrom, Governing the Commons, 52 Cambridge UP (2015) (mutual expectations are the fundamental rules of a collective action institution).
[29] Id. at 20, 64.
[30] Hacken Proof, New Report: Unknown Data Scraper Breach, available at https://blog.hackenproof.com/industry-news/new-report-unknown-data-scraper-breach/.
[31] Joshua Green, This Man Is the Most Dangerous Political Operative in America, BLOOMBERG, https://www.bloomberg.com/politics/graphics/2015-steve-bannon/

In her book "Governing the Commons" Elinor Ostrom describes numerous collective action systems that have been used to regulate use of a common resource. Collective action systems, relative to contract or government monitoring systems, are utilized most by communities when the exploitation costs are low, rewards for exploitation are high, and monitoring costs by a third party are too high.[32] This collection of incentives, which commonly requires collective monitoring, describes the incentives in the present battle between user privacy and social media. Therefore, analysis of some collective action solutions identified by Dr. Ostrom may be instructive to the approaches used to solve the data exploitation problem in the final section of this paper.

One solution to common resource management is based on peer assignment and rotation. In Alanya, Turkey, fishing sites in a small bay are allocated to eligible fisherman at the beginning of the season and rotated based on movement of fish. Importantly, the assignments mean that each fisherman is given a location where they know they can be free of competition, even if the site is not the best. The assignment switches incentives so that the assigned location is better than mass rivalry over the few best spots. Furthermore, monitoring is effective because all spots are covered by fisherman, so any defection to other spots is obvious to the fisherman at that spot.[33] Thus, as long as the assignments are fair, then commitment and enforcement costs are reduced substantially.

Similar complex assignments schemes for meadows and forests have endured for centuries to this day using low cost peer-monitoring.[34] In addition, more complex scenarios, where some parties are responsible for extensive infrastructure (irrigation canals) while others merely use the system, can still be managed by a reciprocal framework. These split reciprocal systems are particularly informative for the current platform internet ecosystem. Furthermore, in some systems assignment and enforcement is delegated to a third party, while monitoring and reporting is largely a peer duty.[35] The monitoring of the resource by peers allows for flexibility and for development of norms or expectations for proper behavior without explicit regulation.[36]

[32] See supra note 29 at 34-35, 59.
[33] Id. at 18-19.
[34] Id. at 61-68.
[35] Id. at 74.
[36] Id. at 88.

Finally, Dr. Ostrom provides seven design criteria for successful resource management institutions: (1) clearly defined boundaries for the resource and rights, (2) rules adapted to the nature of the resource and the time/place/manner of its appropriate use, (3) inclusion of most of those affected by the resource in decision making for rules, (4) low cost monitoring and auditing procedures, (5) graduated sanctions for violators, (6) conflict resolution bodies, (7) recognition or authorization by government to manage the resource, possibly within an overarching regulation framework.[37]

Unfortunately for the management of data privacy, almost none of these structures exist. They can, however, be built from existing principles and institutions. For instance, peer involvement and monitoring/auditing procedures are within the ambit of current Federal Trade Commission (FTC) authority. Furthermore, because the Fourth Amendment expectations test is so flexible, several of these structures can be inferred from the results of that test. Therefore, after a detailed analysis of privacy expectations under the Fourth Amendment and reasonableness under the FTC framework, we can derive a more cohesive system for understanding and applying the variety of privacy laws required across the United States.

B. THE DEVELOPMENT AND APPLICATION OF THE EXPECTATIONS TEST UNDER THE FOURTH AMENDMENT

The early decisions of the Supreme Court on privacy used two different terms to address the possibility of such a right: personal security[38] and personal affairs.[39] In addition, the Federal Courts treated the Fourth Amendment right against unreasonable search and seizure as an extension of the Fifth Amendment right against self-incrimination.[40] That is, where the Fifth Amendment prevented the government from directly torturing out confessions, the Fourth Amendment prevented violence (in the form of unreasonable search and seizure) against a citizen's personal effects to achieve the same result.[41] Likewise, the general warrants and arbitrary arrests by the British were also used to harass those who were protesting the Crown.[42]

---

[37] Id. at 90.
[38] See Olmstead v U.S., 277 U.S. 438, 474 (1928)(citing Boyd v. U.S. 116 U.S. 616, 627); Gouled v. U.S., 255 U.S. 298, 304 (1921).
[39] Interstate Commerce Comm. v. Brimson, 154 U.S. 447, 479 (1894) (citing In re Pacific Railway Commission, 32 Fed. 241, 250 (N.D. Cal. 1887)).
[40] Boyd v U.S., 116 U.S. 616, 621, 630 (1886)(finding coercive subpoena procedure to produce documents or admit guilt was violation of Fifth and Fourth Amendments).
[41] Olmstead v. U.S., 277 U.S. 438, 473 (1928).
[42] Wilkes v. Wood, 98 Eng. 489 (C.P. 1763).

Thus, together these amendments to the constitution were read as preventing unreasonable intrusions regarding persons, houses, papers, and effects to coerce or create self-incrimination.[43] The recent court battles over compelled password disclosure to execute searches on encrypted devices seem to have revived this understanding.[44] Based on this original understanding of the application of the Fourth Amendment, the whole of a person's affairs were included under the combined umbrella of the Fourth and Fifth Amendments.

I. Early Formulations of Privacy Rights

Before *Olmstead v. U.S.* in 1928, the Supreme Court liberally applied the Fourth and Fifth Amendments, holding papers "seized" where no physical seizure had occurred,[45] holding entry by invitation and taking by stealth was still a seizure,[46] and mail left in the third party care of the United States Postal Service could not be searched.[47] Furthermore, with *Weeks v U.S.*, the Court added teeth to the two amendments by creating the exclusionary rule for evidence obtained in violation of these amendments.[48] Throughout these cases, the right to privacy was the underlying subtext, with the expectation of privacy often the focus of arguments.

In *Gouled v U.S.* in 1921, the majority argues that the Fourth Amendment is not limited to forcible means but covers any unreasonable intrusion:

> if for a government officer to obtain entrance to a man's house or office by force or by an illegal threat or show of force, amounting to coercion, and then to search for and seize his private papers would be an unreasonable, and therefore a prohibited search and seizure, as it certainly would be, it is impossible to successfully contend that a like search and seizure would be a reasonable one if only admission were obtained by stealth, instead of by force or coercion. The security and privacy of the home or office and of the papers of the owner would be as much invaded and the search and seizure would be as much against his will in the one case as in the other[49]

[43] See supra note 38 at 633 ("For the 'unreasonable searches and seizures' condemned in the Fourth Amendment are almost always made for the purpose of compelling a man to give evidence against himself, which, in criminal cases, is condemned in the Fifth Amendment").
[44] Orin Kerr, The Fifth Amendment and Compelled Decryption, LAWFARE, available at https://www.lawfareblog.com/fifth-amendment-and-compelled-decryption
[45] See supra note 40.
[46] See Gouled v. U.S., 255 U.S. 298, 304 (1921).
[47] Ex parte Jackson, 96 U.S. 727, 733 (1878).
[48] See Weeks v. United States, 232 U.S. 383 (1914) (exclusionary rule).
[49] Gouled v. U.S., 255 U.S. 298, 305 (1921).

Similarly, in *Boyd v. U.S.* the Court quotes extensively from a British case, *Entick v. Carrington*, which dealt with unreasonable searches prior to the creation of the Fourth and Fifth Amendments. Regarding this British decision, the Court states:

> The principles laid down in this opinion affect the very essence of constitutional liberty and security. They reach farther than the concrete form of the case then before the court, with its adventitious circumstances; they apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offence, but it is the invasion of his indefeasible right of personal security, personal liberty, and private property[50]

Therefore, courts interpreted the prohibition of unreasonable searches and seizures as a broader right to personal security and privacy. Though broader terms such as "privacies," "security," "private affairs," and "invasions" are used by the Court throughout these opinions, the concepts of expected personal privacy and security remained limited by competing notions of property and contract.

Nowhere is this conflict more apparent than in *Olmstead*, which was decided in 1928. There, the Court's majority used expectations to find against a right to privacy in a transmitted phone call,[51] while distinguishing *Ex parte Jackson* as based on contractual grounds[52] and *Gouled v. U.S.* as based on property grounds.[53] Meanwhile the Brandeis dissent in *Olmstead* interprets expectations differently and points to the illegality of the intrusion by the government as evidence that the defendant intended to be secure in his communication.[54] Likewise, the *Olmstead* majority supports its decision with an expectations argument by stating:

> The reasonable view is that one who installs in his house a telephone instrument with connecting wires intends to project his voice to those quite outside, and that the wires beyond his house and messages while passing over them are not within the protection of the Fourth Amendment.[55]

While the Justice Brandeis dissenting in the same case states:

> Protection against such invasion of "the sanctities of a man's home and the privacies of life" was provided in the Fourth and Fifth Amendments by specific language. [citing Boyd] But "time works changes, brings into existence new conditions and purposes." Subtler and more far-reaching means of invading privacy have become available to the

[50] See Boyd v. U.S., 116 U.S. 616, 630 (1886).
[51] See Olmstead v. U.S., 277 U.S. 438, 466 (1928).
[52] Id. at 464.
[53] Id. at 465.
[54] Id. at 475-76.
[55] Id. at 466.

> Government. Discovery and invention have made it possible for the Government, by means far more effective than stretching upon the rack, to obtain disclosure in court of what is whispered in the closet.[56]

Indeed, the reasoning of the majority in *Olmstead* compares phone wires to highways and infers by analogy that privacy has been similarly given up.[57] This harkens of later formulations of the Third Party Doctrine that have a more direct grounding in expectations. Likewise, Brandeis seems equally prescient in his description of future government inventions that capture whispers in a closet without invasion as a technological exception which the Fourth Amendment should cover.[58] After the recent decision by the Supreme Court in *Carpenter v. U.S.* that attempts to balance all these issues under the umbrella of privacy expectations, clearly there is nothing new under the sun.

II. The Creation of the Expectations Test in Katz v. U.S. and Subsequent Cases

The original understanding of the Fourth and Fifth Amendments as covering personal affairs was rolled back by *Olmstead v. U.S.* which summarized precedent as "[n]either the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant unless there has been an official search and seizure of his person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house."[59] This reduced the penumbra of rights around the individual with requirements of property interests, tangibility, and personal contact.

This narrower interpretation of the Fourth Amendment prevailed for about forty years between the decision in *Olmstead v. U.S.* and the decision in *Katz v. U.S.* in 1967.[60] During that time, while wiretapping became acceptable without a warrant, other listening methods with little tangible difference were rejected on property-based rationales.[61] The use of this property basis along with the formalized Third Party Doctrine based in privacy expectations complicated the Supreme Court's jurisprudence. The court in *Katz v. U.S.* realized this tension and redirected Fourth Amendment analysis from property to people as originally interpreted.

---

[56] Id. at 473.
[57] Id. at 465.
[58] Id. at 473; Kyllo v. U.S., 533 U.S. 27, 33-35 (2001).
[59] Olmstead v US, 277 U.S. 466 (1928)
[60] GPO, Fourth Amendment Search and Seizure, 1205-1206 (1992).
[61] Silverman v. United States, 365 U.S. 505 (1961) (spike mike pushed through a party wall is too much of an invasion).

The defendant in *Katz* had been discussing illegal sports wagers on a telephone in a telephone booth at regular times each day. The government used a listening device on the outside of the booth to record the conversations and ultimately convict Katz. The Supreme Court reversed the conviction, however, stating "[w]e conclude that the underpinnings of *Olmstead* and *Goldman* have been so eroded by our subsequent decisions that the "trespass" doctrine there enunciated can no longer be regarded as controlling." The most cited cases that "eroded" the usefulness of the trespass doctrine were *Silverman v. U.S.*, which found a microphone pushed through half a wall but not on the defendant's property was too close to trespass[62], and *Goldman v. U.S.*, which found a microphone placed against the wall was not intrusion under the *Olmstead* trespass standard.[63] Fundamentally, *Silverman* and *Goldman* were indistinguishable except in their outcomes, a result which forced the Court to abandon the *Olmstead* test.

Accordingly, to correct the bad precedent of Olmstead, the Supreme Court shifted to a different stance, holding that the Fourth Amendment "protects people not places." After all the original understanding was that the Fifth and Fourth Amendments were intended to protect people against compelled disclosure, unreasonable searches, and harassment by the government.[64] Thus, the majority opinion in *Katz v. U.S.* merely returned the Court to the original meaning — citing many of the cases distinguished in *Olmstead* instead as support, including *Ex Parte Jackson*.[65]

In the same year, the Supreme Court also decided *Warden v. Hayden*, holding that the Fourth Amendment's principle objective was the protection of privacy.[66] Indeed, Hayden more directly invoked privacy as the fundamental right of the Fourth Amendment, but did not provide a standard to replace the *Olmstead* test. For that matter, the majority in *Katz v. U.S.* also could not elucidate a general means for determining when a person's privacy had been violated. Justice Harlan in his concurrence in *Katz v. U.S.* put the problem thus:

> As the Court's opinion states, "the Fourth Amendment protects people, not places." The question, however, is what protection it affords to those people. Generally, as here, the answer to that question requires reference to a "place."

[62] Silverman v. United States, 365 U.S. 505, 512 (1961).
[63] Goldman v. United States, 316 U. S. 129, 134 (1942).
[64] Richard Thompson, The Fourth Amendment Third-Party Doctrine, 3-4 Congressional Research Service (June 2014).
[65] Katz v. U.S., 389 U.S. 347, 352-53 (1967).
[66] Warden v. Hayden, 387 U.S. 294 (1967).

Therefore, Justice Harlan proposed a two part test with a subjective part and an objective part. Though this test was merely proposed in a lone concurrence, it has become the standard of Fourth Amendment jurisprudence.

The two-part test as explained by Justice Harlan is:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable." Thus, a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the "plain view" of outsiders are not "protected," because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[67]

While the test is framed by Harlan as a subjective/objective test, the logic required by the test is better framed as an objective societal expectations test with exceptions for subjective circumstance of the individual or place.

The most well-known "subjective" exception to the Fourth Amendment and privacy in general is the public square. No one conducting themselves in a public space has ever had privacy from those they interacted with or those observing the space.[68] That is, even if society wished to be completely invisible in the public square, simple observation and experience would tell them that they are not. This knowledge cannot be ignored by the law or by the ordinary person desiring privacy. Indeed, in tort law and contract law, the standard of care from a reasonable person is an objective standard that is heightened based on knowledge or skill.[69] Similarly a person's subjective privacy expectations must be limited by their knowledge of the capabilities and observations of their peers.

While Harlan was certainly correct that any privacy expectations test will ultimately have to revert to an analysis of the place of intrusion, the provision of a right to privacy generally means that places or property would only act as mitigating or aggravating factors in a Fourth Amendment analysis. In other words, property interests, such as the home, can heighten the reasonable expectations, or conversely, the place of the intrusion can lower the reasonable

[67] See supra note 65 at 361.
[68] See Terry v. Ohio, 392 U.S. 1, 20 (1968) (noting that historically warrant procedure did not apply to officers responding to observations in public spaces).
[69] Heath v. Swift Wings, Inc., 252 S.E.2d 526, 529 (1979).

expectations. In all cases though, the expectations are an objective standard that is merely adjusted for circumstances. This arrangement has all the hallmarks of the useful and longstanding tests from contract and tort law.[70]

Another doctrinal aspect of privacy expectations is the Third Party Doctrine, which pre-dates *Katz v. U.S.* but fits very well within the expectations test analysis. The Olmstead line of property-based Fourth Amendment cases failed in their usefulness because, at least in part, they failed to satisfactorily incorporate the Third Party Doctrine into their logic. In contrast, within the privacy expectations paradigm, the Third Party Doctrine for tangible and intangible property merely applies an expectations test to seizure whereas typical privacy intrusion cases like Katz v. U.S. dealt with searches.

For instance, the Third Party Doctrine allowed the Supreme Court to find that a police search of trash left by a suspect was not subject to seizure protections;[71] likewise, following suspects on public streets was not a violation of the Fourth Amendment;[72] nor is the NSA meta-data collection program.[73] As a whole, the Third Party Doctrine provides a mode of determining if a search or seizure has even taken place, a threshold test for expectations. Thus, the expectations test seems to work equally well for search and seizure.

The Third Party Doctrine, however, is not without its detractors. Most notably Justice Sotomayor believes the doctrine needs to be rethought.[74] Principle amongst the objections is that the modern world of email and cloud computing extends much more of our private lives into the hands of third parties while users continue to expect the same protections as were previously provided to physical mail and filing cabinets. Fundamentally, these objections should not be directed at the Third Party Doctrine writ large, but rather directed at the courts' failure to look behind the provision of the data to the third party and their failure to consider the relationship between the user and the carrier/host in the expectations analysis.

---

[70] Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, McGeorge L. Rev., Vol. 40, pg 11.
[71] California v. Greenwood, 486 U.S. 35, 43-44 (1988)
[72] United States v. Knotts, 460 U.S. 276, 285 (1983).
[73] ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013).
[74] Richard Thompson, The Fourth Amendment Third-Party Doctrine, 2-3 Congressional Research Service (June 2014).

The Third Party Doctrine already balances the warrantless release of information to law enforcement that has resulted from tradeable two-party transactions (e.g. financial instruments),[75] identifying information necessary for a communication (e.g. IP addresses and phone numbers),[76] or public actions (e.g. public internet chats),[77] while also protecting private emails on third party servers,[78] location data from cellular service providers,[79] and detailed personal banking history.[80] Therefore, the problem lies not in the Third Party Doctrine but in courts' reluctance to dig further into the expectations of privacy present in the information exchange.

In some contexts, especially digital information, the Third Party Doctrine may seem to swallow the expectations test. The Supreme Court, however, has repeatedly noted that even though the Third Party Doctrine and the expectations test were developed independently, the Third Party Doctrine is still subject to expectations analysis as is the public square exception.[81] With this understanding of the breadth of the application of the expectations test established, we can move on to two prohibitions created by the use of the expectations test that will be essential to our derivation of a privacy law framework.

III. Carpenter v U.S.: Technology and Big Data

Inherent in the reasonable privacy expectations of a person is knowledge of the capabilities of their peers to observe them, the probabilities that technologies will uncover their activities, and the linkability of their offered data. Knowledge is not only essential to an analysis of privacy expectations, but it is also the foundation to collective monitoring of data privacy. The Supreme Court in *Kyllo v. U.S.* formalized a new prohibition on using little known, cutting edge technology – in this case an infrared imager – to pierce the protection of the home.[82] While Justice Scalia, who wrote the majority opinion, tried to resurrect property-based rationales for Fourth Amendment jurisprudence, he largely only succeeded in establishing a rule that

[75] U.S. v Miller, 425 U.S. 435, 442 (1976) (finding no expectation of privacy in checks and financial instruments since they are not confidential but rather made to travel).
[76] Smith v Maryland, 442 US 735, 750 (1979); United States v. Caira, 833 F.3d 803, 809 (7th Cir. 2016), cert. denied, 138 S. Ct. 2700 (2018).
[77] See S. Rep. No. 99-541, at 36 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3590 (discussing bulletin boards).
[78] Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001) (stating that sender of email "would lose a legitimate expectation of privacy in an e-mail that had already reached its recipient but not while on server).
[79] See Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).
[80] State v. Miles, 156 P.3d 864, 868 (2007) (finding an expectation of privacy in bank records).
[81] Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)(A person does not surrender all Fourth Amendment protection by venturing into the public sphere); U.S. v Jones, 565 U.S. 400, 430 (2012).
[82] Kyllo v. U.S., 533 U.S. 27, 35 (2001).

technology not known to the general public can violate privacy expectations if used to pierce otherwise private black boxes.[83] Thus, the knowledge of the existence and use of technology by law enforcement is an important piece of the objective expectation of privacy; so important, indeed, that a general lack of knowledge of a specific technology can be fatal to a warrantless search using that technology.

The danger of these unknown intrusions was first voiced by Justice Brandeis in *Olmstead* when he made reference to government technologies that could ferret out the whispers in the closet. Likewise, in *Katz* the Court noted that electronic surveillance was different in many ways, since it could pierce private places like telephone booths, hotel rooms, and homes without consent or knowledge of the suspect.[84] Then, in *Jones* and *Carpenter*, the Court noted that the low cost of tracking in real time and the ability to summon past locations via electronic GPS or cell-site data made these technologies different. In each of these cases, while reasonable persons may expect their hotel room or their route to work to be private based on their knowledge and observations, technology has made it so that that privacy can be pierced.

Indeed, viewed in this context the conflict between *Silverman* and *Goldman*, which doomed the Olmstead standard, can be settled on expectations grounds. One would not expect a microphone to be pushed through a wall by neighbors as in *Silverman*, but merely listening through a wall with electronic surveillance like in *Goldman* evokes the Third Party Doctrine. Likewise, wired informants do not change the expectations calculus from prior informants who would listen and then testify to conspiracy (the recording merely enhances the veracity of the evidence).[85] Thus, if technology is merely replacing old methods of collecting information without additional intrusion or capabilities, then the technology does not invoke a heightened scrutiny. If, however, the technology enhances police capability to track and record or reduces surveillance costs significantly, then a careful analysis of suspect's expectations in absence of the technology is required.

In parallel to the Court's heightened scrutiny of specialized technology, the recent decisions in *Jones v. U.S.*, *Riley v. California*, and *Carpenter v. U.S.* have solidified another area

[83] Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018) (citing Kyllo as applying to government use of sophisticated technology); supra note 78 at 36 (citing U.S. v Karo, which protected closed containers, as analogous to a house).
[84] Katz v. U.S., 389 U.S. 347, 358-59 (1967).
[85]Richard Thompson, The Fourth Amendment Third-Party Doctrine, 7-8 Congressional Research Service (June 2014).

of heightened scrutiny for invasion of privacy under the Fourth Amendment. This area is big data. In *Jones*, the Court noted that GPS tracking of a person's vehicle for nearly a month presented a new problem. Namely, the GPS tracking seemed to merely replace the tracking of the suspect possible with normal police tails, but the volume of the data along with the low cost of the surveillance seemed to invite easy warrantless invasions of a citizen's every move. The big data cases differ from the prior technology cases not because they are generally known or they enhance the capabilities of police so much as to pierce traditional Fourth Amendment boundaries and private affairs, but rather because the scope of big data can be so vast as to swallow all of Fourth Amendment law.

Between the smart phones on our persons at all times and the smart devices in our homes that are always collecting data for third parties, warrantless access to such information would open every aspect of citizens' lives to the government. Greg Nojeim and other data privacy advocates argue that because of the unprecedented scope of the information available without a warrant, that bulk collection and release to law enforcement, whether by Google or the NSA, should be treated differently.[86] That is, a strict Third Party rule should give way to the broader expectations test. This approach has certainly not been foreclosed by precedent and seems to be the direction taken by the Court in *Carpenter*.[87]

Stewart Baker, in contrast, argues that eliminating or reducing the Third Party Doctrine because of a "creepiness" factor inherent in big data is succumbing to the short-term uneasiness with this new technology without consideration of the fact that other new technologies of the past were deemed creepy but have since become common place and less feared. Indeed, Baker notes, Justice Brandeis was averse to the prevalence of the Kodak camera.[88] As Justice Sotomayor notes in *Carpenter*, however, non-sensitive data in the particular can become sensitive in bulk.[89]

---

[86] Greg Nojeim, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, ABA JOURNAL, (2012) http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited.

[87] Margot Kaminski, *Carpenter v. United States: Big Data is Different*, GEORGE WASH. U. L. REV., Oct. 2017, On the Docket Response.

[88] Stewart Baker, *Smith v. Maryland as a good first-order estimate of reasonable privacy expectations*, WASH. POST, 2014.

[89] See supra note 85.

Meanwhile Orin Kerr provides a middle ground arguing that the Third Party Doctrine should stand but adapt as it has in the past. Specifically, Orin Kerr, in response to Greg Nojeim, argues:

> In a world with no third parties, the Fourth Amendment strikes a balance of police power: It gives the government the power to investigate crimes in some ways, but also limits the government's investigations in important ways. I think that's a sensible balance, as it tries to balance our shared interests in deterring crime and punishing wrongdoing with our commitments to privacy and avoiding government abuses of power. …We should try to apply the Fourth Amendment so that it offers the same basic protections and strikes the same balance in a world of third parties as it did in a hypothetical world without them. The third-party doctrine achieves that, in my view. The doctrine ensures that the Fourth Amendment applies to conduct that harnesses third parties in the same way it applies to events that occur without third-party help. It does so by matching the Fourth Amendment protection in the use of the third party with the Fourth Amendment protection that existed before.[90](emphasis added)

To Orin Kerr, the Third Party Doctrine as applied to data should mean that warrantless access to third party held data turns on whether the suspect is using the third party to secure their information or share their information broadly. Indeed, Orin Kerr and Bruce Schneier asked the Supreme Court in *Carpenter*, via Amicus Brief, to allow the warrantless use of cell site data under the Third Party Doctrine.

The Court, without disagreeing with this wise modification of the Third Party Doctrine, held more widely that the use of particularized, identifying, bulk data from third parties triggered the warrant requirement. Likewise, in *Riley*, the Court noted that people's entire lives can be exposed by the contents of their smart phone, and that such vast amounts of information cannot be accessible to the government merely through the warrant exception of search incident to arrest. Therefore, together *Riley* and *Carpenter* stand for the proposition that big data is different; volume can change the nature of information.

In this section we have identified three facets of the expectations test as applied to the digital world that can have broader applicability. They are: (1) the Third Party Doctrine modified by expected use, (2) the scrutiny of specialized technology not in general use as dangerous to privacy protections, and (3) the rejection of warrantless use of bulk data as a clear privacy invasion. The expectations of privacy in the digital world are changing, but given the collapse of

[90] Orin Kerr, *The Data Question: Should the Third-Party Records Doctrine Be Revisited?*, ABA JOURNAL, (2012) http://www.abajournal.com/magazine/article/the_data_question_should_the_third-party_records_doctrine_be_revisited.

Facebook in recent months following several scandals involving bulk third party data sold to unscrupulous people, it is unlikely that the Supreme Court was far off from the long-term trend of privacy demands in the digital arena. A person's desire for secrets, shared secrets, and public information as distinct from each other has not changed in several millennia and is unlikely to change merely because of the advent of Internet 2.0. Therefore, if policy is to mirror the expectations of society, the ability of a person to have secrets shared in a home, bedroom, or closet must be enshrined in consumer protection law.

C. CONSTRUCTION OF AN EXPECTATIONS BASED COMPREHENSIVE PRIVACY LAW FOR THE UNITED STATES

The right to privacy generally, not just in relation to the government, is a right treated differently from culture to culture and from legal norm to legal norm. The European Union's citizens are aware, due to experience with the Stasi and Nazis, that mere associational information can be destructive, since member lists and travel history were used extensively by both to isolate individuals. Cultures based more on families and close communities, like Morocco or small town USA, view many aspects of privacy as unnecessary (while keeping a few secrets very closely held). The United States as a whole seems to value privacy less, perhaps because our experience with totalitarian governments is so remote. More generally, the common experiences of a culture form the expectations that the society has for their private affairs.

The privacy of a society at a social level is clear in the amount of communication in confined public spaces (e.g. trains and busses), in the amount neighbors and family know about eachother's daily lives, and in the willingness of strangers to carry on conversations with each other (e.g. in bars or elevators). The privacy of a society online is clear in the number of posts related to daily life shared, whether their profiles are public or private, the number of strangers allowed to view their updates as friends, and whether they have social media at all. These interactions, or lack thereof, build an expectation for openness in any interaction with another person of the same society. Fundamentally, though, the expectations are built from individual choices to share, whether online or in-person, and the reciprocal response from their peers.

Furthermore, on a more local level, societies can build in even more complexity with certain areas signaling openness more than others. For instance, in New York City few people know their neighbors, meaning that living in proximity does not signal openness to communicate, but talking to strangers in NYC bars is far more easy and personal than elsewhere

in the United States. Because of the diversity of the United States both geographically and demographically, our culture has always opted to give citizens choice. The United States was the first country to declare freedom of religion, giving all citizens the right to choose and exercise their religion. Likewise, privacy law in America has used choice as the basis for allowing anyone to maintain privacy online.

In the 1960s, Chicago-school economists have seized on this preference for choice in America and suggested that markets should be preferred since they most efficiently conform the options made available to those choosing with their money. Even democratic socialist governance norms, however, allow choice through voting and regulatory consensus --though that consensus quickly converges choices down to one or two alternatives. As a regulatory regime, the expectations test is somewhere in between a market solution and a democratic solution. While the expectations of citizens would be codified and respected, the modes of implementation for technical developers would be broader than with a consumer rights regulatory framework under democratic socialist norms.

The EU has enacted a General Data Protection Regulation (GDPR) which codifies certain consumer rights for digital service users in the EU to utilize. In order to comply, internet companies must implement the ability for their EU users to exercise these rights. If the GDPR "right to be forgotten" is used extensively, for example, then data aggregators and collectors will be constantly culling data from their data sets leaving them incomplete and useless for large-scale data analysis studies that can benefit society. Since options for implementation are limited, innovation in user interfaces and services could be limited by the regulation, while creative solutions for providing users the same benefits without privacy risks are certainly hampered by the law.

The current American solution of choice via posted privacy notice, and in some cases opt out options, has, however, also caused problems.[91] First, posted privacy notices do not arise from negotiation and are take-it-or-leave-it; this arrangement presents a collective action problem which precludes any actual choice or input from the consumer. Second, privacy notices are not notices of actual data practices or equivalent to a data audit, instead they merely assert the foreseeable uses of the data collected from the user. If uses change, an update of a privacy policy

[91] Cameron Kerry, Why protecting privacy is a losing game today—and how to change the game, (July 2018), available at https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/.

cannot be consent for new uses of old data collected under the previous policy.[92] Third, the more detailed opt out options available for some mobile applications are based on the data collected or transmitted not based on sharing norms or social networks.[93] In other words, opting into a data telemetry feed to the application developer just to share your jogging route and speed with a close significant-other is privacy engineering gone wrong. The third party developer is a needless intermediary and the data feed results in oversharing to the third party beyond that needed to execute the peer-to-peer share of data. Thus, the present private law solutions to ensure consumer privacy are not working for consumers. Nor are internet companies benefiting from the constant demands for testimony before congress after each disclosure of data misuse.

To date, the American legislative solutions to secure consumer privacy have been far more successful. The Gramm-Leach-Bliley Act (GLB) requires notices to financial services users and an ability to opt out from sharing. More substantially (aside from the standard notice and opt-out), GLB limits any entity that receives non-public information from a financial institution to uses that conform with the financial institution's privacy policy.[94] This prevents data laundering.[95] In addition, the financial industry has self-policed its disclosures to third parties often sharing only with affiliates, because privacy in banking pays.[96] The Fair Credit Reporting Act (FCRA) and the Fair and Accurate Credit Transactions Act (FACTA) tackle consumer concerns with discrimination, inaccuracy, and auditability head on with explicit limitations on data use, rights to correct, and rights to inform (e.g. free credit reports). Considering the widespread use of credit and credit reports by Americans, the auditing function of FACTA may be the most utilized privacy right in America.

Finally, the Health Insurance Portability and Accountability Act (HIPAA) is probably the most comprehensive and well-thought out of the privacy regimes. From the beginning, HIPAA

[92] See Hooters of America, Inc. v. Phillips, 39 F. Supp. 2d 582, 606-07 (D.S.C. 1998).
[93] Rosie Spinks, Using a fitness app taught me the scary truth about why privacy settings are a feminist issue, (Aug. 2017) https://qz.com/1042852/using-a-fitness-app-taught-me-the-scary-truth-about-why-privacy-settings-are-a-feminist-issue/.
[94] FTC, How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act, available at https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm.
[95] GLB also bans fraudulent collection of information, preventing situations like Cambridge Analytica, where the actual use is not disclosed to the financial institution. See 15 U.S.C § 6821.
[96] See generally Wells Fargo Privacy Policy, https://www.wellsfargo.com/privacy-security/privacy/individuals; BB&T Privacy Policy, https://www.bbt.com/privacy-security/policies/consumer-privacy-notice.page.

was drafted to balance portability (use) with accountability (protection). To do so, it instituted an expectations-based limitation on disclosure of personal health information (PHI). A health provider or an associate can only disclose PHI for a limited set of the following purposes or situations without the written consent of the patient: (1) To the Individual; (2) Treatment, Payment, and Health Care Operations (TPO); (3) Opportunity to Agree or Object; (4) Incident to an otherwise permitted use and disclosure; (5) Public Interest and Benefit Activities; and (6) Limited Data Set for the purposes of research, public health or health care operations.[97] Largely two carve outs to explicit and informed consent are permitted: for TPO and for research.

Treatment, Payment, and Operations (TPO) functions are exactly the functions that a patient expects their information to be used for. Furthermore, any information collected as a part of treatment must be accessible or transferrable to other doctors at the request of the patient ensuring the ease of getting second opinions and switching care providers (at least theoretically). Finally, the research exception allows safe use of patient data to create better outcomes and improve health care for society.

Fundamentally, the TPO exception is based in the patient's subjective expectations while the research exception is based on the objective societal expectation or willingness to give the patient privacy. This parallels the expectations test of the Fourth Amendment which protects subjective expectations so long as society will grant those expectations. Here society's large benefit from the use of the data preempts any individual privacy demands. Therefore, the HIPAA regulations, which are the strictest and most enforced privacy standards in the United States, directly apply patient expectations to the data.

These siloed regulatory frameworks are largely aligned with industries. This method of regulation, even if by chance, allowed legislators to take into account the level of privacy for the information along with industry norms and needs. For instance, while GLB allows more sharing of data, banks were profitable via other means and the sale of data was an unnecessary and dangerous risk. In contrast, health data is valuable especially for hospitals and research, but patient information contains some of society's closest guarded secrets. The separate regulations reflect this in their approaches.

The downside of this separation of regulatory regimes is that the regulation needed to be clear what and who was regulated. Nevertheless, each regime has permitted uses that allow data

[97] See 45 C.F.R. § 164.502(a)(1).

to leak out to data collectors who are not directly regulated. Furthermore, non-regulated sources of data are increasingly being put to the same tasks as those within regulated industries.[98] This presents one of the reasons for a nationwide privacy law. Secondly, people's personal data which was intended to be private (and even set to private on social platforms) is increasingly being sold to the highest bidder.[99] Finally, if the 2016 and 2018 elections were any indicators, Americans are increasingly demanding the ability to look behind the algorithm, especially search algorithms, to root out the source of bias. All of these recent developments demand solutions which state laws and industrial sector laws cannot address alone.

I. Privacy as a Common Resource and Management Basics

As noted in the introduction, privacy is a common resource that is often voluntarily given up but increasingly it is given up under subterfuge or without choice. Personal data is also better thought of as a common resource rather than the private property of either the person or the collector, because both the person and the counterparty have equal rights to the data.[100] In other words, to a certain extent, information given up to a third party voluntarily is free for them and others to use. This parallels the Third Party Doctrine. The extent of third party use under Fourth Amendment law, however, has its limits. In particular, big data has been noted as converting innocuous data into intrusive data. The facts are no different in the private sphere where data aggregators increasingly hold personal data previously only available to well-funded spy agencies for a fraction of the population.

Clearly the data provided by users of search engines, social platforms, and cell phone connections is valuable and useful not only to their immediate collectors but to city planners, sharing networks, and rescue operations. To eliminate the data would be to remove the networks, instant connection to Wikipedia, and global communication. The exchange of data is inherent in the proposition of a modern world. Thus, as long as we have these technologies we as a society will have this valuable data resource which others will seek to exploit. As a method of managing

[98] Matt Scully, Big Data Tells Mortgage Traders an Amazing Amount About You, Bloomberg, (June 2017) https://www.bloomberg.com/news/articles/2017-06-29/big-data-can-tell-mortgage-traders-an-amazing-amount-about-you.

[99] Jennifer Valentino-Devries, et al., Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret, NY TIMES, https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

[100] Amitai Etzioni, Can We Save Privacy by Treating Info Like Private Property?, NATIONAL INTEREST, https://nationalinterest.org/feature/can-we-save-privacy-by-treating-info-private-property-25606

this resource, I propose adapting the common resource management principles identified by Elinor Ostrom to a privacy protection framework for big data.

(1) First, the boundaries for what parts of the resource should be regulated must be clearly defined along with any unilateral rights of stakeholders. Since nearly all digital data is currently considered valuable by data aggregators, a privacy framework should also cover all digital data, regardless of its source.[101] Already cheap facial recognition technology is being combined with public cameras to track shoppers and pedestrians, while regular use of license plate scanners enables tracking of vehicles.[102] As Justice Sotomayor has noted these innocuous public collection techniques can collect enough information to map people's lives. Thus, public collection cannot be a general exception to a useful privacy framework.

Based on consent, personal information given to a retailer for home delivery can be used to deliver the package, mail coupons, and email offers (all standard practices since before the internet or variations thereof). Likewise, consent to the exchange of financial details can result in the parties keeping each other's financial information for future transactions. Similarly, employee data is presumed to have been given by consent in the United States and should be able to be used by that employer. These carve outs accomplish two goals: first, government regulation would not be inserting itself into consensual business relationships; second, it directs regulation towards more serious abuses of data than those within an existing business relationship. Fundamentally, information generated in the course of business transactions should be usable by both parties in the future without limitation (but not necessarily transferrable).

(2) Second, the regulations should be adapted to the nature of the resource and the time/place/manner of its appropriate use. This principle follows the prior legislative solutions to privacy in the United States: HIPAA, GLB, FCRA/FACTA. Within each industry the differences in the treatment of data matter greatly, because they inform us about the expectations under which the information was provided. A home office investor that creates derivatives contracts with the family's name as the originator cannot expect privacy in that tradeable instrument. On the other hand, derivatives contracts once on the open market provide very little information,

[101] FTC Privacy Hearings, November 6, 2018, (the App Society) American University.
[102] Annie Lin, Facial recognition is tracking customers as they shop in stores, tech company says, CNBC, https://www.cnbc.com/2017/11/23/facial-recognition-is-tracking-customers-as-they-shop-in-stores-tech-company-says.html.

since positions and ownership can change by the day. Thus, the expected use of the information must be considered along with the ephemerality of its value.

Additionally, the manner in which the data was collected or used can also provide differentiation. For instance, information provided in a survey for an ipad prize is quite clearly provided with consent and consideration. Thus, paying people for their data in an open way should broaden the resale and transferability of the data. Furthermore, facial recognition for use by small brick and mortar stores to help in greeting repeat customers is merely technology facilitating old practices (like police using GPS trackers rather than follow cars for brief periods). Facial recognition for optimizing ads in Times Square, however, should be prohibited.

Most importantly, data collected by mobile applications and social media are not expected to be sold to the highest bidder. There's no clearer metric of this expectation, than Facebook's repeated denials that it sold user data.[103] Lying to Congress and the British Parliament about the selling of data, means Facebook likely benefited from the gap between data expectations and actual practices. At the furthest end of this type of exploitation is the flashlight mobile application that mysteriously needs access to your contacts, texts, and browser history. At the other end of the spectrum are the public profiles provided on Linkedin or Tinder which are meant to be viewed and shared widely. This should not kill ad-based applications, but may make those ads less efficiently targeted (like billboards).

Finally, people generally expect social networks, search engines, and even grocery store rewards programs to utilize their data to provide better services, predict demand, and operate more efficiently. Use within a system that houses the data or receives the data is expected, whereas ads that follow from Youtube to the smart TV across applications seems creepy and unexpected. While things may change in this space, sale of data out of a platform should be limited somewhat. As with all these context-based limitations, widespread input is necessary for an acceptable and useful determination of appropriate uses.

(3) The third, and perhaps the most difficult, principle to enact with an expectations-based framework is the inclusion of most of those affected by the resource in decision-making for rules. An expectations analysis defers to ordinary people for the standards and rulemaking since it is reciprocal in nature. This can leave big business feeling ignored during the decision

[103] Colin Lecher, Internal Facebook documents show how the company makes deals for data, THE VERGE, https://www.theverge.com/2018/12/5/18127230/facebook-data-documents-parliament-deals-zuckerberg

making process. Social media platforms and ad-supported apps do have one case to make in this process and that is that their products or business models would not be viable without use of their user data. While some platforms have argued this, they have not shown any evidence that less or no targeting of users in their ad provision would destroy demand for access to new media.

The selection of the forum for this decision making will be addressed in the next section. Nevertheless, one element of the digital world that should change the calculus for this process is the need to keep everyone engaged and make changes to the rules easy so as to accommodate future technologies. Thus, flexibility will be needed to keep America one of the most innovative digital economies.

(4) Fourth, for any reciprocal, peer-based monitoring to be possible, regular citizens must be able to audit where and how their data is being used. This goes beyond simply having a privacy notice of possible uses on each website they access. Instead, at least yearly, citizens should be able to obtain a privacy report by selecting which retailers and platforms they use. This report would be similar to the HaveIBeenPWND.com website that tracks major data breaches. By selecting the sites used (least detail) or the username (or hash of it) used on the site (highest detail), a report of which aggregators had acquired your data (if allowed) as well as end uses by non-aggregating purchasers. This would allow comparisons by users of the privacy standards of different companies based on their actual practices. This proposed report draws from both the data breach report and the free credit reports mandated by US consumer law.[104] Both have been very useful in bridging the gap between data use in the digital world and privacy expectations/information in the public sphere.

(5) Fifth, some enforcement body, whether private or government must be empowered to impose graduated sanctions for violators of the rules established under step 2. Preferably, this enforcement body would also have the power to interpret and issue warnings to companies who are close to the line, or who are innovating in new technology areas. Because most data is national or supra-national, enforcement and rule making would be far more efficient and effective if done on a national level. States could then have a role in developing rules to address new technologies before Federal action is taken (like the Illinois biometric data law).

[104] FTC, Get My Free Credit Report, https://www.ftc.gov/faq/consumer-protection/get-my-free-credit-report

(6) Sixth, in any reciprocal framework, conflict resolution bodies are essential. In an expectations based, national framework, conflict resolution would be necessary not only between users and alleged privacy violators, but also between rule making and enforcement bodies and those that they monitor and regulate.

(7) Seventh, in addition to any statutory framework which may need to be implemented by legislation, privacy advocacy groups, consumer rights groups, and the public must recognize and tacitly authorize the government to manage the resource while retaining certain rights to act on their own. Because of the auditing by the public possible via the privacy report, far fewer regulatory demands will be placed on government. This balance keeps the prior assignment of duties between industry, the public, and the FTC that has enabled the FTC to remain so small and effective. The benefit of a peer-based enforcement regime is that the cost of developing the infrastructure to enable easy audits is placed on industry who is best equipped to create it, and government is merely the rare enforcer that steps in to punish particularly bad actors. The implementation of this peer-based enforcement regime for management of data privacy will be tackled in the next section.

II. Implementation of a Privacy Regulatory Regime

Primarily this section will quickly describe the possible methods of implementing a privacy regime with legislative input and without it. Without a Federal data privacy law, the FTC can also step in to apply the GLB and FCRA to a wider breadth of data than currently regulated. Furthermore, a requirement by the FTC or other regulatory bodies (e.g. FCC,[105] OCC, and CFPB) to track sales of data and imbed tags as to the source of data would greatly help data auditors and journalists in tracking data around the globe. As laws stand currently worldwide (including GDPR) no tracking or tagging is mandated so the regulations really are meaningless without more relevant application to what is being tracked (much like anti-piracy laws).

(1) To redraw the boundaries of data privacy to include all data would likely require a Federal law since the current regimes only enable limited regulatory enforcement of privacy under section 5 of the FTC unfair or deceptive trade practices prevention statute. Nevertheless, the most insidious data privacy abuse can be regulated currently by the FTC and the OCC under FCRA and GLB.

[105] 47 CFR 64.2010, available at https://www.law.cornell.edu/cfr/text/47/64.2010; see also Sam Pfeifle, FCC Fines AT&T for Data Privacy Lapse, at https://iapp.org/news/a/fcc-fines-at-who-will-be-next/.

The FTC should expand the coverage of the FCRA's furnisher rules for data related to actions affecting employment, credit, or background checks.[106] While this proposed extension expands the data uses covered under these acts, it also broadens the data covered by the FCRA to include most of the serious forms of data indicators (e.g. age indicators, racial indicators, gender indicators, disability, and marital/parental status).[107] In fact, finding a single data element relevant for advertising that is not correlated with one of these protected statuses is almost impossible.[108] To justify the FTC expansion, however, it is only necessary to look at algorithmic bias in the provision of job ads to African-Americans or women on typical jobs boards.[109] While the FTC already provides accuracy and anti-bias regulations on background checks incidental to employment, many minorities face difficulties in the digital world before reaching that stage of the process. Indeed by expanding the furnisher rules of the FCRA, the FTC would increase those directly covered to more than just credit agencies (e.g. LinkedIn/Indeed) and increase the data covered to include Linkedin cookies (indicative of being a professional). Therefore, the regulation of the data used to provide jobs ads, investment ads, credit ads, election ads, and housing ads is only a small step beyond the traditional credit agency metrics to a broader world necessitated by the increased use of other metrics to replace the traditional credit metrics in equally important circumstances in the digital world (i.e. job ads on Facebook).

(2) In furtherance of the regulation of expectations based rules, limitations should follow data provided for very private purposes (e.g. medical examinations (WebMD), credit offers, porn preferences, and destination addresses to maps or ride-sharing apps). While the regulations of data at its source to ensure that that data was only used in the manner expected by the user would be ideal, it would require legislation. Such legislation would preferably require that each data collector/source add tags as to the reason and nature of the provision of the data. Was the data provided for shipping or for a private college major selection survey given to minors? Thus, the regulation of all uses may be limited by needed enacting legislation.

---

[106] 12 CFR Part 1022.
[107] Claire Miller, When Algorithms Discriminate, NY TIMES, available at https://www.nytimes.com/2015/07/10/upshot/when-algorithms-discriminate.html.
[108] Ellora Israni, When an Algorithm Helps Send You to Prison, NY TIMES, available at https://www.nytimes.com/2017/10/26/opinion/algorithm-compas-sentencing-bias.html.
[109] Anja Lambrecht et al., Algorithmic Bias? A study of data-based discrimination in the serving of ads in Social Media, (Sept. 2016), available at https://www.ftc.gov/system/files/documents/public_events/966823/lambrechttucker_algorithmicbias_final.pdf.

Certain uses, however, as noted above can invoke coverage without a legislative update. The data used for critical purposes such as jobs, housing, and credit are subject to regulation at least under the Civil Rights Act and under the anti-discrimination rules of the FCRA.[110] In addition, the furnisher rules of the FCRA demand accuracy and provide correction rights to consumers. Given the many sources of data today, legal and illegal,[111] it is essential to look not only at accuracy as judged from consumer complaints but also from the source. In order for regulators to sufficiently judge the veracity and legality of a source of data to a credit rating agency or a rater of credit on the resale market, it is essential that the source of the data input into the algorithm be identified with a tag.

Similarly, in order for the FTC to determine if companies are complying with their privacy notices under section 5 of the FTC Act, the source and date of sale of all data must be identified so that data in use can be audited and determined to be legally gathered (essentially establishing a requirement for data provenance). Certainly, data scraping robots that scour social media sites in violation of their terms of service in order to sell their data without restriction fall within the ambit of "unfair trade practices."[112] Just like in black market art sales, the limiting factor should be provenance, so that illegal data cannot be laundered into usable data simply by acquisition. Furthermore, these data tags have been shown to actually increase the usefulness of data and are relatively easy to add.[113] In addition, more forward looking privacy compliance firms are suggesting tagging of data in similar ways just to be able to track it through out a firm and beyond to vendors. [114] Thus, tagging and provenances seem to just be a good business practice for tracking incoming data as well as recording outgoing sales.[115]

(3) If anything exemplifies how not to engage in rule making and regulation to effect broad societal outcomes it is the LabMD case. There, a data scraper attempted to extort a medical

[110] EEOC, Background Checks What Employers Need to Know, available at https://www.eeoc.gov/eeoc/publications/upload/eeoc_ftc_background_checks_employers.pdf.
[111] Hacken Proof, New Report: Unknown Data Scraper Breach, available at https://blog.hackenproof.com/industry-news/new-report-unknown-data-scraper-breach/.
[112] Id.
[113] eMarketer, Tag Management Becomes a Key Component of Big Data Strategy, available at https://www.emarketer.com/Article/Tag-Management-Becomes-Key-Component-of-Big-Data-Strategy/1010052 (allegedly improving analytics accuracy as well).
[114] Balaji Ganesan, Managing risks in big data #5—Tagging data and understanding risks, available at https://blog.privacera.com/managing-risks-in-big-data-4-tagging-data-and-understanding-risks-69bed5abd6b.
[115] DataTags Research Overview, Harvard, https://privacytools.seas.harvard.edu/datatags

research company, then turned to "FTC whistleblower" to effect its threat, then based on these bad facts and an even worse administrative guidance history, the FTC proceeded to create an adjudicative process while demanding that LabMD go through that process.[116] The FTC should be more deliberate, utilizing notice and comment rule making under the APA to enact the expansions to the FCRA and GLB as suggested above. In addition, if an administrative adjudication body is created, then procedures should be established well in advance of any actual case. Preferably public input would be accepted via comments and also via congressional input directly to FTC commissioners.

(4) With the data tags related to source and date of the collection of the data, then the FTC could simply mandate disclosure of the sale of data to an unaffiliated third party along with the tags associated with that data under its privacy notice enforcement authority. Such disclosure is not only essential to the ongoing mission of the FTC to ensure compliance with posted privacy notices, but also invaluable to data auditors who could take that disclosed data and generate yearly reports for users of various websites. Ideally, with additional legislative authority, every ad provided on the internet could be audited for the sources of information used and the tags simply by clicking part of it. Thus, with the provision of tags, the peer-based monitoring for the common data resource would be spearheaded by journalists not the FTC.

(5) In the case of particularly bad actors, such as Facebook at the moment, the pile on effects of state Attorney Generals, the FTC, the SEC, and foreign regulators each demanding their pound of flesh for misleading statements, poor security, and improper monitoring will quickly put bounds on the data trade.[117] Lower level sanctions could be available via private rights of action and low statutory damages enacted at the state level. In particular, private rights of action could be aided simply by the FTC expansion of the data types related to meaningful determinations under the FCRA.

(6) While the FTC could certainly provide a forum for resolving disputes between the government and companies, they could not provide private rights of action that would be needed to act on the privacy audit reports of step 3. These private rights of action or even whole forums

[116] Michael Daugherty, The FTC and its Section 5 Authority, House Oversight Committee, https://oversight.house.gov/hearing/federal-trade-commission-section-5-authority-prosecutor-judge-jury-2/.
[117] Rafia Shaikh, Things Get Serious: FBI, FTC and SEC Join the Justice Department to Investigate Facebook's Cambridge Analytica Disclosures, https://wccftech.com/fbi-ftc-sec-facebook-privacy/

for litigation could be provided under state law. This would allow for not only a single standard and report at the Federal level, but also a state level suit to enforce violations under the regulations (regulations governing use, tagging, sale disclosure, etc.). Only a few states would have to enact a private right of action under the Federal standard for the regulation to essentially become enforceable without FTC intervention.

(7) Possibly, the largest obstacle to a consumer-enforced expectations framework is the lack of private rights of action currently provided by government. Establishing actual damages when privacy is breached has been difficult to prove even when the personal information was stolen by a bad actor. In part, though these failures stem from the individual victims are suing a company who was also a victim and likely tried to protect the individual's information. The facts are worse when a company profits off user data by exploiting that data beyond what was disclosed. While these suits at present are hard to bring, since actual data disclosure is a closely guarded secret, if the reporting requirements listed above are demanded by the FTC, then these suits will be easy to bring. Indeed in order for the government or the consumer to enforce privacy notices, reporting is required.

D. CONCLUSION

The peer-based, expectations that are used by the Fourth Amendment jurisprudence have been successful in tailoring government intrusion to that which is acceptable to Americans. Furthermore, because of the nature of how societies build expectations and maintain them, the consistency of expectations over time can ensure that legal standards tethered to expectations do not go adrift. To build out the privacy framework from the expectations analysis, we introduced the long-standing principles of governing common spaces and resources. The two main requirements of such a peer-based monitoring system is auditability and consensus-based enforcement of clear expectations.

The digital privacy expectations of Americans have fortunately already been articulated by nearly thirty years of Fourth Amendment case law applied to digital technologies. Primarily, Americans expect to give up some privacy by dealing with a third party, but aggregation and specialized technologies that exceed the expected exploitation of the third party data are not expected. In addition, exceptions must be given for when society needs access to the data for its own benefit. Of the present privacy regimes in place in America, HIPAA enacts this expectations framework best, balancing doctor's needs, patient's use expectations, research needs, and

vendors. Furthermore, the credit reports of the FCRA provide an excellent example of how to build consumer monitoring into a privacy framework.

For the overarching solution proposed by this paper, the Fourth Amendment rules are incorporated into an expanded FTC regulatory scheme that counts any data related to a protected class under the Civil Rights Act as being regulated under its furnisher rules (ostensibly racial/age/disability information is used to discriminate online). Alternatively, or in addition, the FTC could broaden the background check regulations to include uses of data for jobs/credit/housing ads. In either case, the serious uses for data targeting are regulated, but the less serious uses of data (like tennis equipment ads) will remain unregulated. The FCRA already establishes accuracy requirements and source tracking for data used in credit reporting and background checks. These requirements along with public disclosure of data sources can ensure that targeted ads and the data behind them are traceable and auditable. Furthermore, under the FTC's section 5 powers, the FTC should require that data sales be disclosed so that both the FTC and consumers can determine if posted privacy policies are actually being followed. Without these changes by the FTC in response to big data, the benefits that resulted from the FCRA will be undercut as more decision making is being done with big data than by traditional background check metrics.[118]

While these would be the rationales for expansion by the FTC and implementation of the broadened regulatory regime, consumers would benefit by receiving two new oversight abilities. The first would be data aggregation disclosures by data providers which would enable consumers to generate data privacy reports to see the extent of the data usage and privacy loss. By matching these reports with the stated privacy policies of the companies, consumers (and class-action lawyers) could quickly ascertain if these companies' privacy pacts with their users had been broken. The second would be heightened standards for targeting of users for critical services, which, when breached, would have statutory damages under the FCRA. Together, this regime will not only increase consumer awareness of data use by digital companies, but also empower them to take action if these companies overstep.

These implementation steps and the principles behind them derive from Elinor Ostrom's seven principles for common resource management. In addition, they draw from the best

[118] Matt Scully, Big Data Tells Mortgage Traders an Amazing Amount About You, Bloomberg, (June 2017) https://www.bloomberg.com/news/articles/2017-06-29/big-data-can-tell-mortgage-traders-an-amazing-amount-about-you.

practices of the HIPAA and FCRA privacy laws. All in, they present a viable option to move forward on privacy regulation without significant action by Congress. Even if Congress does act, they should also consider taking the best from the HIPAA TPO process and FCRA credit reports to allow for public-based, consumer-monitored, privacy regulation.