NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
VOLUME 22, ISSUE 4: MAY 2021

MEANINGFUL CHOICE: A HISTORY OF CONSENT AND ALTERNATIVES TO THE CONSENT MYTH

Charlotte A. Tschider*

Although the first legal conceptions of commercial privacy were identified in Samuel Warren and Louis Brandeis's foundational 1890 article, The Right to Privacy*, conceptually, privacy has existed since as early as 1127 as a natural concern when navigating between personal and commercial spheres of life. As an extension of contract and tort law, two common relational legal models, U.S. privacy law emerged to buoy engagement in commercial enterprise, borrowing known legal conventions like consent and assent. Historically, however, international legal privacy frameworks involving consent ultimately diverged, with the European Union taking a more expansive view of legal justification for processing as alternatives to consent.*

Unfortunately, consent as a procedural substitute for individual choice has created a number of issues in achieving legitimate and effective privacy protections for Americans. The problems with consent as a proxy for choice are well known. This Article explores the twin history of two diverging bodies of law as they apply to the privacy realm, then introduces the concept of legitimate interest balancing as an alternative to consent. Legitimate interest analysis requires an organization to formally assess whether data collection and use ultimately result in greater benefit to individuals than the organization with input from actual consumers. This model shifts responsibility from individual consumers having to protect their

* Assistant Professor of Law, Loyola University Chicago School of Law and the Beazley Institute for Health Law & Policy. Professor Tschider would like to extend her heartfelt thank you to Professor Anne Klinefelter and the rest of the participants of the N.C.J.L. & Tech symposium, "Privacy Norms Across Borders and Boundaries." Professor Tschider would also like to thank W. Nicholson Price, I. Glenn Cohen, Jason Crites, Danielle Keats Citron, Woodrow Hartzog, Neil Richards, Daniel Solove, Eric Goldman, and Ari Ezra Waldman for their helpful ideas and lively discussions around the concept of consent and trust.

own interests to organizations that must engage in fair data use practices to legally collect and use data. Finally, this Article positions the model in relation to common law, federal law, Federal Trade Commission activities, and judicial decision-making as a means for separating good-intentioned organizations from unethical ones.

TABLE OF CONTENTS

I. INTRODUCTION

Informational privacy law, both as a consumer concern and as a civil right, has a history that spans as long as organized society has existed. Indeed, the first notions of privacy are recorded as early as 1127.[1] Aristotle defined the *polis* (gr: πόλις), or the political and public realm, from the *oikos* (gr: οἶκος), the private realm, where a person's individual realm existed, the *idia* (gr: ἴδια).[2] Since this time, philosophers have identified a separation between public and private life and, indeed, the negotiation between these two realms, as a central human experience.[3]

In 17th Century Europe, economic participation moved from the personal to a more dynamic, public participation in the market, or commercial economics, *Kommerzienwirtschaft*.[4] By the 18th century, finance and agricultural technology were separating from traditional economics, and private spheres of civil society became connected to public authority.[5] The relationship between public commercial activity and private life began to influence understanding of these spheres, their connectivity, and their overlap. Within small communities, unauthorized disclosures of health information specifically became a concern when sensitive information was shared with others in the community.[6]

---

[1] JUDITH WAGNER DECEW, IN PURSUIT OF PRIVACY LAW, ETHICS, AND THE RISE OF TECHNOLOGY 9 (1997) [hereinafter DECEW]. *See also* JÜRGEN HABERMAS, THE STRUCTURAL TRANSFORMATION OF THE PUBLIC SPHERE: AN INQUIRY INTO A CATEGORY OF BOURGEOIS SOCIETY (STUDIES IN CONTEMPORARY GERMAN SOCIAL THOUGHT) 3 (Thomas Burger trans., 1991) [hereinafter HABERMAS].

[2] *See* DECEW, *supra* note 1, at 10.

[3] *Id*. at 10–13.

[4] HABERMAS, *supra* note 1, at 20.

[5] *Id*.

[6] *See* Daniel J. Solove, *A Brief History of Information Privacy Law*, PROSKAUER ON PRIVACY, PLI 17 (2006), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2076&context=faculty_publications [https://perma.cc/94JQ-9MDQ] (quoting Simonsen v. Swensen, 177 N.W. 831 (Neb. 1920), in which the court identified a "wrong" and recognized damages for loss of confidentiality). In *Simonsen*, the Nebraska Supreme Court noted that confidentiality within a physician and patient

By the time the first populations settled U.S. colonies, the legal concept of privacy was only beginning to develop, and privacy was a luxury usually experienced by wealthy individuals.[7] Large homes accommodated physical privacy and etiquette training discouraged reading others' private communications, while having less economic means usually involved sharing private spaces.[8] At the time, most people did not trust the privacy of mail communications and instead communicated by cipher or other code.[9] The United Kingdom's Post Office Act of 1710 created the first statutory recognition of privacy and levied a fine for postmasters opening private communications, which was recognized in the early colonies.[10] Despite this, during the American Revolution both sides regularly opened their adversary's communications.[11]

In 18th Century Colonial America, privacy was often considered a negative, rather than a positive.[12] Those who expected privacy could not be readily observed by neighbors, which was necessary for communities prior to centralized policing.[13] In small communities, observation by neighbors supported a kind of self-governance, an early form of the surveillance-privacy tradeoff.[14] Privacy was a "source of tension" both because of an increasing interest in personal privacy and a conflicting interest in community monitoring, or surveillance.[15] From the outset, privacy was a nuanced and complex concept.

---

relationship improves outcomes and treatment, a public good. *See, e.g.*, Humphers v. First Interstate Bank of Oregon, 696 P.2d 527 (Or. 1985) (discussing the variety of circumstances giving rise to physician's liability for disclosing confidential information, including by express or factual implication).

[7] Cathy Hellier, *Physical, Intellectual, Biographical: Our Idea of Privacy and Their Evolution*, COLONIAL WILLIAMSBURG (2013), https://research.colonialwilliamsburg.org/foundation/journal/winter13/privacy.cfm [https://perma.cc/Q8SH-9RV5].

[8] *Id.* Although not addressed in this paper, privacy protection still favors those who can afford it.

[9] *Id.*

[10] *Id.* The Post Office Revenues Act of 1710, 9 Ann. c.10 (Gr. Brit.).

[11] *See* Hellier, *supra* note 7.

[12] *Id.*

[13] *Id.*

[14] *Id.*

[15] *Id.*

The specific privacy roots and motivations of the United States and Europe in the 20th century had very different origins. In 1890, future Supreme Court Justice Louis Brandeis and attorney Samuel Warren penned *The Right to Privacy*, which focused on the commercialization of individuals in the news media including newspaper photojournalists seeking sensational and tawdry information, especially about famous individuals.[16] Notably, three of the four invasion of privacy torts identified in the famous piece are related to commercialization—appropriation, unreasonable publicity, and false light (what would become libel).[17] It is likely that the concept of "personal information" as a potential risk for individuals was simply not on the radar, before the development of computers and broad-scale personal information use.

Today's privacy world is dramatically different than the world of Warren and Brandeis. Data are collected, retained, transferred, duplicated, and analyzed, sometimes by humans, sometimes by artificially intelligent algorithms.[18] Quality and reliable data are tremendously valuable—and are used for nearly every service, whether simply to provide service, enhance service, measure performance, or to increase adoption of a service.[19]

---

[16] Benjamin E. Bratman, *The Right to Privacy and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623, 624 (2002).

[17] *Id.*

[18] Charlotte A. Tschider, *Deus ex Machina: Regulating Cybersecurity and Artificial Intelligence for Patients of the Future*, 5 SAVANNAH L. REV. 177, 183–84 (2018) [hereinafter Tschider, *Deus ex Machina*]; Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. L. REV. 87, 109 (2018) [hereinafter Tschider, *Regulating*]; Charlotte A. Tschider, *AI's Legitimate Interest: Towards a Public Benefit Privacy Model for Healthcare Data*, HOUST. J. HEALTH L. & POL'Y (forthcoming, 2021) [hereinafter Tschider, *AI's Legitimate*] (describing the value of data in sectors like healthcare for a variety of artificial intelligence applications).

[19] *See* Hugo Moreno, *The Importance of Data Quality – Good, Bad Or Ugly*, FORBES (June 5, 2017), https://www.forbes.com/sites/forbesinsights/2017/06/05/the-importance-of-data-quality-good-bad-or-ugly/?sh=507a90fb10c4 [https://perma.cc/S3DA-RGCV]; Anne W. Branscomb, *Global Governance of Global Networks: A Survey of Transborder Data Flow in Transition*, 36 VAND. L. REV. 985, 987 (1983).

One key problem, however, is that in transactions, providing personal information is a condition of service, and an individual supplies this information after having an opportunity to read a privacy notice and consent to it. On its face, notice and consent appears to be a manifestation of individual knowledge and subsequent choice. In reality, the notice/consent model is fraught with a variety of issues, originally posed by Daniel Solove, that have been well established in recent writings.[20]

Although privacy scholars have admired the EU's General Data Protection Regulation ("GDPR"), few U.S. scholars have discussed the origins of consent in U.S. and EU law, in order to identify the function and purpose of this convention.[21] Fewer still have analyzed the impact of alternatives to consent, including legitimate interest, a justification for data collection and processing that involves balancing interests of an organization with interests of the individual about whom data are collected.[22] This model reflects inherent

---

[20] *See, e.g.*, Neil M. Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1479 (2019) (describing the challenges of consent in the United States); Charlotte A. Tschider, *The Consent Myth: Improving Choice for Patients of the Future*, 96 WASH. U.L. REV. 1505, 1519 (2019) [hereinafter Tschider, *The Consent Myth*] (describing the challenges of contemporary consent in healthcare in the United States). *See generally* Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1880 (2013) (describing the consent dilemma and calling for more discussion of consent's problems). This article aims to clearly articulate the history and function of consent from U.S. and European perspectives, while building on previously identified issues with notice and consent.

[21] Mike Hintze has discussed privacy statements and their purpose but has not explored the finer details of alternative lawful bases for processing under the General Data Protection Regulation ("GDPR"). Mike Hintze, *Privacy Statements under the GDPR*, 42 SEATTLE U.L. REV. 1129 (2019) (describing the many requirements to meet GDPR privacy statement [notice] requirements).

[22] Elettra Bietti has explored the dominating "free pass" of consent and introduces the alternative bases available under the GDPR. Elettra Bietti, *Consent as a Free Pass: Platform Power and the Limits of the Informational Turn*, 40 PACE L. REV. 314, 338. As Bietti remarks, in the case studies evaluated within Bietti's article, specifically the CNIL v. Google case, no alternative lawful bases for processing existed: only consent. *Id.* at 344. Legitimate interest is largely a convention of EU law, one that has not been discussed in relation to U.S. law, especially in a comparative manner. Rather, much of its discussion has occurred

notions of decision-making under the common law, including relativity and reasonableness while simultaneously promoting fairness in data processing behaviors.[23]

This Article proceeds in four parts. Part II describes the history of consent in the United States to illustrate why consent is the preferred model for privacy frameworks in the United States, while illustrating why relational models are inherent in these transactions and worth building upon. Part III describes the history of consent in the EU, including the evolution to multiple forms of lawful bases for personal information processing from consent-based models. Part

---

in the EU. *See generally* Federico Ferretti, *Data Protection and the Legitimate Interest of Data Controllers: Much ado About Nothing or the Winter of Rights?,* 51 COMMON MKT. L. REV. 843 (2014) (describing the role of legitimate interest as an expansive lawful basis); Paolo Balboni, Daniel Cooper, Rosario Imperiali, Milda Macenaite, *Legitimate Interest of the Data Controller New Data Protection Paradigm: Legitimacy Grounded on Appropriate Protection*, 3 INT'L DATA PRIV. L. 244 (2013) (describing legitimate interest as a new paradigm); Irene Kamara & Paul De Hert, *Understanding the Balancing Act Behind the Legitimate Interest of the Controller Ground: A Pragmatic Approach*, 4 BRUSSELS PRIV. HUB 1 (2018) (exploring how to create a usable legitimate interest model); Mark J. Taylor & Tess Whitton, *Public Interest, Health Research and Data Protection Law: Establishing a Legitimate Trade-off between Individual Control and Research Access to Health Data*, 9 L. 1 (2020) (describing the benefits of data access); Dolenc Dubravka, *Legitimate Interest as Legal Grounds for Processing Personal Data*, 49 BANKARSTVO 145 (2020) (discussing legitimate interest under the GDPR as a valid lawful basis); Michael Veale, Reuben Binns & Jef Ausloos, *When Data Protection by Design and Data Subject Rights Clash*, 8 INT'L DATA PRIV. L. 105 (2018) (explaining the differences between user rights and data use under privacy by design). These scholars all individually have described challenges and solutions related to the concept of legitimate interest in the European Union and individual member states. Fred Cate first discussed a "public interest" with respect to the EU Data Protection Directive in his piece, as early as 1995. Fred Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest*, 80 IOWA L. REV. 431, 441 (1995). In it, Cate describes the contours of the Data Protection Directive, which informed later global laws and the General Data Protection Regulation. *Id.* Cate briefly introduced the tension between the value of information and privacy protections that supports the "public interest," though this concept was not defined more fully into the concept of "legitimate interest." *Id.* at 441–42.

[23] Luke Irwin, *The GDPR: Legitimate Interest- What is it and When Does it Apply?,* IT GOVERNANCE BLOG (Nov. 17, 2020), https://www.itgovernance.eu/blog/en/the-gdpr-legitimate-interest-what-is-it-and-when-does-it-apply [https://perma.cc/PB8Z-E9C6].

IV draws upon philosophy and previous scholarly works to illustrate how consent does not adequately meet existing privacy needs, proposing instead a relational model which imposes more responsibility on organizations in a superior position to understand risk to data subjects.

II. CONSENT IN THE UNITED STATES

The law in the United States developed, at least initially, through judicial decision-making in the common law. Over time, the intersection of public and private life, and a need to safely traverse these different spheres, resulted in the development of privacy torts and recognized commercial obligations in contract.[24] As data became more important for specific sectors, and the risks to individuals became higher, specific sectors developed privacy laws to minimize potential risk to individuals and instill trust in these systems.[25] These laws took the form of federal laws, largely managed by administrative agencies, then spurred state law developments where federal laws did not regulate.[26]

As a key point of difference between the United States and the European Union, the United States does not have a common, broadly applicable, omnibus privacy law that creates obligations for organizations and individuals.[27] Privacy law developed from early

---

[24] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193. *See generally* Omri Ben-Shahar & Lior Strahilevitz, *Contracting over Privacy: Introduction*, 45 U. CHI. L. REV. 51 (2016) (describing the law and economics of contracting related to privacy, including privacy notices); Alicia Solow-Niederman, *Beyond the Privacy Torts: Reinvigorating a Common Law Approach for Data Breaches*, 127 YALE L.J. 614 (2018) (advocating for a return from sectoral privacy laws to the common law).

[25] *See* Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 448 (2016). Indeed, "trust is a state of mind that enables its possessor to be willing to make herself vulnerable to another." *Id.*, at 448 n. 61. For sectors where trust is of utmost importance, and, correspondingly, fiduciary relationships also inure, Congress has recognized the need for privacy commitments. However, much requires such commitments outside narrow sectoral legislation.

[26] *See* CHARLOTTE A. TSCHIDER, INTERNATIONAL CYBERSECURITY & PRIVACY LAW IN PRACTICE 26 (2018).

[27] *Id.*

tort law and contract law, eventually growing though accretion of federal sectoral laws and state laws. Consent, therefore, has roots in all of these bodies of law in the United States. Unfortunately, for most of these bodies of law, consent is not actually effective in representing individual choice, as will be described in more detail in Part IV.

A. Consent in Tort Law

Most modern notions of privacy, outside embedded notions in the Constitution related to the Third, Fourth, and Fifth Amendments, originate from common law tort, originally identified in the oft-cited *The Right to Privacy* by Justice Warren and Justice Brandeis.[28] Warren and Brandeis's privacy torts stemmed, at least in part, from a lack of agreement to share or make public something private, "a psychological or spiritual interference caused by the unconsented to collection and publication of personal information," a negative freedom.[29] This negative freedom presumably included its reciprocal freedom, an "affirmative capacity" for decisions on disclosure of private information about an individual's life.[30]

Early privacy torts in the United States, therefore, sought to secure personal autonomy through affirmative decision-making, or choice. Warren and Brandeis expressly linked affirmative decision-making with the concept of consent, referencing consent no less than eighteen times, though privacy torts were concerned with different problems at the time.[31] Although grouped as "privacy torts," rights to publicity and invasion of privacy serve different purposes and flow from different legal concepts. Rights to publicity, for example, flow from contractual principles of unjust enrichment,

---

[28] *See* Solove, *supra* note 6, at 5. The tort as a "wrong," provides an interesting conceptual framework for evaluating privacy obligations and lack thereof in comparison to contractual relationships where breach of contract does not evidence a wrong. Privacy in the United States, as an evolution from both tort and contract law, falls somewhere in between. *See* Warren & Brandeis, *supra* note 24.

[29] Dorothy J. Glancy, *The Invention of the Right to Privacy*, 21 ARIZ. L. REV. 1, 16 (1979). Although Professor Glancy describes this as *control*, control here is used not as a legal term, but as language used to represent the ability to make decisions about information privacy or disclosure.

[30] *Id*. at 24.

[31] Warren & Brandeis, *supra* note 24, 193–20.

whereas the second is more core to Warren and Brandeis's original argument.[32]

The first common law privacy tort statutes were enacted in response to *Roberson v. Rochester Folding Box Co*.[33] New York passed the first invasion of privacy tort in 1903, and Georgia followed with recognition of an invasion of privacy tort in *Pavesich v. New England Life Ins. Co.*[34] Even in the Warren and Brandeis era, certain sectors, like health care, remained a local, non-commercial service, which did not enjoy much protection under the Warren and Brandeis tort definitions.[35] Perhaps overt recognition of privacy in financial relationships and health care relationships resulted from the highly personal and community-based aspect of these services at the time. Consent emerged as this proxy through the historically dominant arms of the common law, tort law, and contract law, which in many ways created a procedural proxy.[36]

---

[32] *Id.*, at 199–200 (analogizing to written works as protected and valuable).

[33] Robertson v. Rochester Folding Box Co., 171 N.Y. 538 (N.Y. Ct. App. 1902).

[34] *See* Glancy, *supra* note 29, at 13; Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905).

[35] Although grouped as "privacy torts," rights to publicity and invasion of privacy serve different purposes and flow from different legal concepts. Rights to publicity, for example, flow from contractual principles of unjust enrichments, whereas the second is more core to Warren and Brandeis's original argument. Harry Kavlan, Jr., *Privacy in Tort Law – Were Warren and Brandeis Wrong?*, 31 L. & CONTEMP. PROBS. 326, 331 (1966).

[36] *See* infra, Part II and accompanying notes. In this way, consent preceded privacy legally and conceptually; consent therefore is foundational to many different legal disciplines including privacy law. Herein, this Author hopes to more fully illustrate the reasons why consent alone cannot serve as a proxy for individual choice. Indeed, society expects consent to do far too much by way of securing individual autonomy and representing broader consumer choice. Daniel J. Solove has previously noted the expectations and limitations of consent and the natural tension between free enterprise "choice" for consumers and paternalistic (statutory) privacy obligations. *See* Solove, *supra* note 20, at 1880. *See also* Daniel J. Solove, *A Brief History of Information Privacy Law*, PROSKAUER ON PRIVACY, PLI, 2006, at 5 (2006), https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=2076&context=faculty_publications [https://perma.cc/5E8J-CJMP]; Kavlan Jr., *supra* note 35, at 331. *See also* Glancy, *supra* note 29, at 16. Although Professor Glancy describes this as control, control here is used not as a legal term, but as language used to represent the

Yet, a full recognition of positive privacy rights did not develop, except in limited cases, where the common law recognized these freedoms and provided a means of recovery. States that have recognized privacy torts such as intrusion upon seclusion, appropriation of name or likeness (right of publicity), invasion of privacy, public disclosure of private facts, and false light temper these torts with a recognized affirmative defense of consent or agreement.[37] This analytically follows: if individuals consent to their name or likeness being used, share private facts publicly, agree to be portrayed inaccurately, or invite the public into their private affairs, they cannot later argue that another party has intentionally engaged in tortious conduct and receive damages.[38]

Warren and Brandeis connected the right to be left alone to the concept of consent as a defense to encroachment on privacy, mentioning consent eighteen times, crucially in articulating principles: "the right of privacy ceases upon the publication of the facts by the individual, or with his consent."[39] In this way, Warren

---

ability to make decisions about information privacy or disclosure. The first common law privacy torts were enacted in response to Roberson v. Rochester Folding Box Co., 171 N.Y. 538 (N.Y. Ct. App. 1902), when New York passed the first invasion of privacy tort in 1903. Georgia followed with recognition of an invasion of privacy tort in Pavesich v. New England Life Ins. Co., 50 S.E. 68 (Ga. 1905). *See* Glancy, *supra* note 29, at 13.

[37] *See* Glancy, *supra* note 29, at 14. William Prosser identified four distinct torts in 1960, and most states today recognize some variation of these torts. William L. Prosser, *Privacy*, 48 CAL. L. REV. 383 (1960). Although consent is an available affirmative defense for intentional torts, consent has been criticized for many of the same reasons it is criticized in privacy law. Actual and apparent consent loosely map to explicit and implicit consent, respectively. Although actual and apparent consent are specific legal standards in battery, explicit and implicit consent in privacy regulations illustrate both the regulatory standard and the procedural mechanism for facilitating consent.

[38] Public interests could weigh in favor of disclosure, even without consent. First, publication of private information could serve a public or general interest, support efficient adjudication within judicial or legislative proceedings, and may be allowed when free speech rights are implicated. *See* Glancy, *supra* note 29, at 38.

[39] *See* Warren & Brandeis, *supra* note 28, at 218. Warren and Brandeis quote Woosley v. Judd (1855): "[w]e must be satisfied, that the publication of private letters, without the consent of the writer, is an invasion of an exclusive right of

and Brandeis seem to present consent as a limiting factor, a variant of commercial transaction with greater attendant meaning.

William Prosser built upon the Warren and Brandeis foundation, standardizing intrusions on privacy resulting from non-trespassory activities, such as wiretapping and Peeping Tom cases.[40] However, scholars around that time also criticized the formulation of such torts, given their relative imprecision both in demonstrating a prima facie case and in articulating potential damages.[41] More contemporary scholars, including Neil M. Richards and Daniel J. Solove, have criticized the ineffectiveness of Prosser's privacy torts to remedy issues regarding collection, use, and dissemination.[42]

Despite the relative ineffectiveness of historically established privacy torts, legally recognized confidential relationships have continued to enjoy special protection under the law, creating a narrow privacy protection for sensitive information.[43] As early as 1849, English courts recognized a breach of confidentiality action as a breach of "trust, confidence, or contract."[44] In 1894, a

---

property which remains in the writer, even when the letters have been sent to, and are still in the possession of the correspondent." *Id.* Courts did not recognize this and other opinions often because contents of correspondence did not fit traditional notions of personal property. *See id*. at 203. Consent was featured heavily in relation to intentional privacy torts and articulated as a principle. *Id*. at 218.

[40] William L. Prosser, *supra* note 37 at 389–406.

[41] *Id*. at 334. One major concern regarded potential injuries without broad recognition of emotional damages, as most privacy torts would implicate different types of damages than successful tort actions traditionally award. "It remains odd to give recovery for emotional disturbance without any showing that plaintiff suffered or was upset." *Id.*

[42] *See* Neil M. Richards & Daniel J. Solove, *Prosser's Privacy Law: A Mixed Legacy*, 98 CAL. L. REV. 1887, 1889 (2010) (describing Solove, Citron, Whitman, and Friedman's criticism of Justice Warren and Justice Brandeis's privacy torts as lacking the initial momentum to realize their potential and their subsequent failure with new technology, including online environments).

[43] The law often referenced these as fiduciary relationship, or special relationships of trust, which create specific duties, including, frequently, a duty of confidentiality as well as a duty of loyalty. *See* Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 14 (2020).

[44] *See* G. Michael Harvey, *Confidentiality: A Measured Response to the Failure of Privacy*, 140 U. PENN. L. REV. 2385, 2396 (1992) (quoting Prince Albert v. Strange, 41 Eng. Rep. 1171 [Ch. 1849]).

Massachusetts court identified a "violation of confidence" related to duplication of private photographs.[45]

In the 1920s, a breach of confidence tort began to emerge in the United States.[46] However, most courts embraced the Warren and Brandeis torts instead, stalling the development of breach of confidentiality torts.[47] Unlike broad confidentiality agreements, which often focused on private information about an organization, special relationships focused on a relationship of trust between two parties, where information would be exchanged.[48] The common law breach of confidentiality tort required no explicit contractual agreement, as these understandings were typically implied contractual terms under a pre-existing contractual relationship.[49] The recent popularity of the breach of confidentiality tort likely extended from a failure to establish an effective privacy tort for personal information disclosure.[50] As such, protection for narrowly defined

---

[45] *See id*. at 2397 (quoting Corliss v. E.W. Walker Co., 64 F. 280 [C.C.D. Mass. 1894]).

[46] *See, e.g.,* Simonsen v. Swenson, 177 N.W. 831, 832 (Neb. 1920) (recognizing confidentiality obligations between a physician and his patient).

[47] *See* Harvey, *supra* note 44, at 2398–99.

[48] Specially defined confidential relationships, although between two natural persons, extend to the organization of one of the natural persons, such as the hospital rather than just the medical professional working with a given individual.

[49] *See* Harvey, *supra* note 44, at 2400 n.79 (quoting Peterson v. Idaho Nat'l Bank, 367 P.2d 284, 290 (Idaho 1961)) (describing the existence of an implied term of an agreement not to disclose information related to a financial customer's account). Certainly, confidential relationships could (and often were) memorialized via contract for clarity. However, the law generally does not require existence of a confidentiality agreement, but rather only evidence that a confidential relationship has formed for relationships traditionally bound by a duty of confidentiality, namely professional relationships and those in which a fiduciary duty exists. *Id.* at 2429 n.208. Increasingly, states require consent for financial, medical, and other special relationships to expressly communicate the professional's obligation to the individual, although written notice and consent were not originally required at common law.

[50] *Id.* at 2413. The public disclosure of private facts tort does not effectively protect two-party interests and district court attention has instead focused on media defendants rather than professional service providers. Similarly, the Supreme Court has focused on First Amendment values as they pertain to information disclosure, especially the legitimate interest of the public in receiving relevant information. This signals a similar approach to the lower courts.

confidential relationships enjoyed a resurgence in popularity while privacy torts have waned, despite Warren and Brandeis's early cautions.[51]

The concept of consent is not unique to privacy torts. Consent has also provided an effective affirmative defense for other torts, such as battery, although such a defense has raised considerable questions over whether a lack of consent is also required to establish a prima facie case.[52] Although actual and apparent consent are specific legal standards in battery, explicit and implicit consent in privacy regulations illustrate both the regulatory standard and the procedural mechanism for facilitating consent.[53] When a defendant establishes a reasonable belief that the plaintiff has consented, often the defendant cannot be found to have "intended" to commit a battery.[54] Similarly, explicit consent processes facilitate active, affirmative consent and provide evidence that an individual actively consented to some further action in relation to personal information (e.g., access, collection, transfer, sharing, aggregation, use, sale).[55] Consent in this way acts as nearly a rebuttable presumption—when an individual has consented to certain terms of a privacy notice, and those terms are accurate, it is tremendously difficult to argue that an invasion of privacy has occurred.[56]

What does this brief history of consent in torts indicate about consent in the United States? First, it may suggest that consent has

---

[51] *See id*. at 2399. Warren and Brandeis's article contemplated a confidentiality-based approach to privacy law and ultimately rejected it on the grounds that it might be too narrowly defined: confidence based on contract or special confidence. *See id.* at 2398.

[52] *See* Nancy J. Moore, *Intent and Consent in the Tort of Battery: Confusion and Controversy*, 61 AM. U. L. REV. 1585, 1627 (2012) (discussing consent as part of intentional battery torts, including traditional battery and medical battery).

[53] *See id.* at 1605.

[54] *Id.*

[55] *See* Jay Cline, *Privacy Consent Glossary,* IAPP (Sept. 1, 2009), https://iapp.org/news/a/2009-09-privacy-consent-glossary/ [https://perma.cc/EW7R-N2NR].

[56] This illustrates the difficulty of privacy torts: informational privacy is usually subject to privacy notices or terms of use that were provided at some point in time. This, then, creates an intersectionality of law between tort and contract in commercial relationships and complicates clear legal direction in either of these areas. *See infra* Part II (C) and accompanying notes.

been positioned as a functional approximation of individual choice for at least 120 years, potentially as far back as Ancient Greece, serving as a means of navigating transitions between private and public environments. Second, the U.S. reinforcement of consent as a limiting factor for bringing a successful tort lawsuit (or at least the option of an affirmative defense) showcases the tremendous importance of consent in the U.S. legal system as a visible approximation of individual choice, even when consent does not lead to a positive result for the individual consenting. Finally, these history-based, accretive conceptions of consent, combined with broad solicitation of personal information in commercial relationships, has led to consent's intransigence in privacy law. As this Article discusses in Part II, this intransigence does no favors for actual consumers.

B. Contract Law: Consent as Accepting a Contract of Adhesion

Like tort law, contract law evolved over time to manage exchanges of personal information via commercial contractual relationships, though frequently personal information was a condition of the broader contract itself.[57] Variations of contractual agreement, including contracts implied in fact and quasi contracts, were recognized as early as Roman-era law and evolved as commercial market participation increased.[58] Under English law, the

[57] Consider, for example, doctor-patient relationships, wherein a contract was for medical care and identifiable health data was collected to fulfill the contract in place. Or, for example, a construction contract where information about an individual's home address was used to ensure construction occurred at the right location. In these cases, personal information was secondary or conditional within the contract but not necessarily a material term of it.

[58] J. B. Ames, *The History of Assumpsit*, 2 HARV. L. REV. 1, 2 (1888), https://www.jstor.org/stable/pdf/1321512.pdf [https://perma.cc/D3PB-QW5T]. The concept of *indebitus assumpsit* was a variation of implied contract, in that a contract was created to provide equitable remedy when the participation of two parties evidenced some bargain without a contract. *Id.* However, this contract was created precisely because something occurred that caused damage, impeding performance of the implied contract. *Id.* This concept operates similar to tort in that a party has undertaken a duty, yet the foundation for the duty is a contractual-type relationship.

King recognized two types of contracts: covenant and debt.[59] The King's courts focused heavily on debt, or when one party received a benefit without giving value in return.[60]

Under the common law that eventually developed, agreement by explicit memorialization, by implication of reciprocal promises, or undertaking a responsibility, established a commitment between two or more parties, often positioned as reciprocal promises.[61] The four requirements of contract at common law included: (1) parties capable of contracting; (2) parties' consent (either explicit or implied); (3) a lawful object (or lawful subject matter); and (4) cause or consideration.[62]

The growth of market conditions to include transfer of personal information as part of commercial relationships likely introduced the concept of consent in contract.[63] Contracts, therefore, likely resulted from a brokering of negotiating personal autonomy for products and services when private life converged with commercial enterprise, a blend of consent and offer acceptance. Indeed, all

---

[59] *See* Timothy J. Sullivan, *The Concept of Benefit in the Law of Quasi-Contract*, 64 GA. L. REV. 1, 2 (1975).

[60] *Id.*

[61] *See* Joseph L. Lewinsohn, *Contract Distinguished from Quasi Contract*, 2 CAL. L. REV. 171, 172 (1914). Contracts are divided fairly simplistically into: (1) explicit contract (memorialization); (2) implied in fact contract (no evidence but action); and (3) implied by law (equitable remedy, applicable as in unjust enrichment or indebitus assumpsit).

[62] *See id*. Arguably, consent is a crucial and historical aspect of contract formation, "the master concept that defines the law of contracts in the United States." *See* Chunlin Leonhard, *The Unbearable Lightness of Consent in Contract Law*, 63 CASE W. RSRV. L. REV. 57, 58–59 (2012). Contracts implied by fact became implied contracts, or *tacit* contracts, while contracts implied by law became quasi contracts. Both contract types were created as a protective measure: if an explicit agreement does not exist, nevertheless value could be given (or changed) which demonstrates the existence of such an agreement. *See also* Humphers v. First Interstate Bank of Oregon, 696 P.2d 527 (Or. 1985) (describing contract claims and other relationships which give rise to an understanding of confidentiality).

[63] A topic that is still under discussion is the degree to which privacy notices online will be, *de facto*, considered contracts wherein consent operates as assent in traditional common-law contract. *See* Gregory Klass*, Empiricism and Privacy Policies in the Restatement of Consumer Contract Law*, 36 YALE J. ON REG. 45, 48 (2018).

contractual "commitments are enforceable because the promisor has 'willed' or freely chosen to be bound by his commitment."[64] If contracts are viewed as an exchange of consent, it is not a surprise that consent*ing* is the procedural method (either by overt action or inaction) favored for supplying personal information in commercial settings primarily governed by contracts.

Privacy interests involving consent usually include two parties in a commercial relationship, with singular or repeat disclosures and subsequent personal information management obligations.[65] For example, personal information might be provided in exchange for access to an online service. However, for that online service to run effectively, continuous information may need to be supplied. This means that any relationship is governed in real time by the contract and consent previously memorialized.[66] Although the concept of continuous service within a contract is not new or unusual, especially between sophisticated parties, there are several concerns when such a relationship involves disproportionate bargaining power and a desire to change the terms without notice or reconsenting.[67]

Privacy notices (to which an individual consents) are a hybrid of two kinds of contracts: confidentiality agreements and traditional contracts based on exchange of promises.[68] For consumer contracts, the commitments are somewhat asymmetrical, yet the role of privacy is not usually an explicit promise made, though the exchange of promises regarding data may not be part of the primary

---

[64] Randy E. Barnett, *Contract Is Not Promise; Contract Is Consent*, 45 SUFFOLK U. L. REV. 647, 650 (2012).

[65] *See* Klass, *supra* note 63, at 57 (describing unilateral changes of privacy notices, illustrating that the relationship between an organization and a consumer is an ongoing one).

[66] *Id.*

[67] *Id.* at 52 (describing the one-sided aspect of adhesive bargaining, including information asymmetries and unequal bargaining power).

[68] *Id.* at 94 (explaining Loeffler v. The Ritz-Carlton Hotel Co., No. 2:06CV 0333 ECR LRL, 2006 WL 1796008 (D. Nev. June 28, 2006), wherein the Nevada District Court described the relationship as one both of confidentiality and contract).

goods or services agreement.[69] Take, for example, the following excerpt from a modern privacy notice:

> To provide the Facebook Products, we must process information about you. The types of information we collect depend on how you use our Products. You can learn how to access and delete information we collect by visiting the Facebook Settings and Instagram Settings. . . .
>
> Information and content you provide**.** We collect the content, communications and other information you provide when you use our Products, including when you sign up for an account, create or share content, and message or communicate with others. This can include information in or about the content you provide (like metadata), such as the location of a photo or the date a file was created. . . .
>
> We use the information we have (subject to choices you make) as described below and to provide and support the Facebook Products and related services described in the Facebook Terms and Instagram Terms. . . .
>
> We'll notify you before we make changes to this policy and give you the opportunity to review the revised policy before you choose to continue using our Products. . . .[70]

Importantly, in the example above, typical for most Privacy Notices, Facebook only informs about what it does and what it will do, rather than making any actual commitments. For example, Facebook makes no commitments about safeguarding information or limiting its activities with "will not" language. More than anything, a Privacy Notice (or, indeed, a privacy section of a Terms of Use) is informative rather than demonstrating any real commitment. If consent is the procedure used to signal acceptance of terms, the fact that no real commitment has been made casts doubt on the enforceability of the contract itself.[71]

Despite some key differences between a traditional contract and consenting to a privacy notice, and some question as to whether a privacy notice is a contract, in the event such notices are interpreted

---

[69] *Id.* at 50.

[70] *Data Policy*, FACEBOOK, https://www.facebook.com/about/privacy [https://perma.cc/9MYC-CGH6**]** (last visited Jan. 11, 2021).

[71] *See* RESTATEMENT (SECOND) OF CONTRACTS § 2(1) (AM. L. INST. 1981). It should be noted that although privacy notices *may* be viewed by some courts as contracts, this is not as overwhelming as previously believed. *See* Klass, *supra* note 63, at 51 (challenging the ALI's comment regarding privacy policies treated by courts as contracts using case analysis and reproducing such results).

as contracts, the common law may apply in important ways. First, imperfections in the contracting process and inherent unfairness in a contract's terms certainly can render such agreements voidable via the unconscionability doctrine.[72] Unconscionability in most states requires both substantive unconscionability, which could include unfair terms (the "what"), and procedural unconscionability, unfairness in how the contract is presented, communicated, or how acceptance is induced (the "how").[73] This dual requirement often makes it difficult to prove unconscionability for contracts of adhesion (inherently one-sided contracts), commonly used for privacy notices and terms of use agreements.[74] Consent in this model may objectively evidence acceptance but may not actually result in autonomous choice. Furthermore, interpreting privacy notices as contracts may actually make it more difficult to prove bad behavior of the more powerful party.[75]

Contracts of adhesion, by definition, involve unequal bargaining power, often between a sophisticated business and consumers or some product or service.[76] Courts have identified contracts of adhesion as demonstrating procedural unconscionability due to the inherent nature of one-sided terms in "take it or leave it" contracts.[77] Although contracts of adhesion can form a legitimate legal basis for a relationship as recognized by law, the individual often does not have an opportunity to negotiate. However, when contracts of adhesion are used in repeat-play or ongoing exchanges, such as using a site like eBay, privacy has a relational underpinning: the contracts are intended to embody trust between the parties.[78] Trust, although a core part of contracting, unfortunately may be misplaced.[79]

---

[72] *See* RESTATEMENT (SECOND) OF CONTRACTS § 208 (AM. L. INST. 1981).

[73] *Id.*

[74] Dov Waisman, *Preserving Substantive Unconscionability*, 44 SW. L. REV. 297, 299 (2014).

[75] *See* Klass, *supra* note 63, at 57 (describing that enforcing privacy notices as part of a contract will likely benefit commercial organizations than consumers).

[76] *See* David A. Hoffman, *Relational Contracts of Adhesion*, 85 U. CHI. L. REV. 1395, 1452 (2018).

[77] *See* 8 WILLISTON ON CONTRACTS § 18:9 (4th ed.).

[78] *Id.* at 1454.

[79] *See infra*, Part III and accompanying notes.

What is especially problematic, though, is that the inducement to provide personal information is something more than a typical commercial exchange: individuals provide personal information that is only created by existing as a human being; information that, once lost or misused, cannot be returned, replaced, or deleted.[80] And when one of the parties takes some action that harms trust, due to information asymmetries and power differentials, the impact will be felt by the consumer, likely not the organization.[81]

Further, the act of consenting to a privacy notice is something more than accepting a traditional contractual agreement when it involves personal information.[82] Although consent-as-agreement simply demonstrates agreement to follow something, usually terms of use, consent to a privacy notice is actually quite different. Privacy notices are typically one-sided communication of an organization's behaviors with respect to data, which means that consent is only agreement to an implication: "I consent to you doing those things you said you would do."

---

[80] Danielle Keats Citron and Daniel Solove have explained the potential types of harm resulting from data misuse or breach. *See generally* Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CAL. L. REV. 1805, 1847 (describing the evolution of harms to financial vulnerabilities associated with the release of sensitive persona information); Danielle Keats Citron & Daniel J. Solove, *Privacy Harms*, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3782222 [https://perma.cc/U6DQ-R4CN] (proposing a taxonomy of privacy harms). Central to this argument, however, is that personal data are somehow exceptional—namely that they are about a person, the entire reason privacy law exists in the first place and correspondingly why it is difficult to effectively compensate their misuse or loss. *See* Felix T. Wu, *How Privacy Distorted Standing Law*, 66 DEPAUL. L. REV. 439, 450–51 (2017). The personal nature of these data, then, are what makes them worth protecting and potentially damaging if misused or breached.

[81] *See* Hoffman, supra note 76, at 1453. Hoffman describes this as "sharing of benefits and burdens," which, at least for contracts of adhesion, often result in fewer benefits and greater burden to the consumer. *Id.*

[82] This is where privacy actions, especially consenting to a privacy policy, illustrate something between contract and tort. In tort, not abiding by commitments in the policy might evidence a "wrong," whereas breaching the privacy policy as a contract does not evidence a wrong but triggers some remedy. Consent as a function, then, super-charges the effects of a contract of adhesion. The harm is potential of a different character than for traditional commercial contracts.

Even more, consent is not necessarily consent to just one activity. Many organizations do not collect, use, and retain data for only one purpose.[83] Although it may appear that personal information will be collected primarily for a service the consumer desires, often data are used for other purposes, exchanged with third parties, and, in many cases, aggregated and sold.[84] A privacy notice or terms of use agreement with privacy terms usually communicate these secondary uses, but the use of a contract of adhesion renders consent applicable to all potential uses.[85]

In bundled privacy policies and terms of use agreements that include privacy terms, individuals who do read the terms might find it difficult to separate secondary uses from primary uses (uses specific to the product or service desired by the consumer).[86] For example, an individual may not wish to permit their data to be shared with third-party data aggregators or brokers, but this is bundled with other primary uses required to use the service, such as registering for an account. A contract of adhesion, although not illegal or unethical on its face, creates a higher likelihood of unconscionable or at least unfair practices in relation to personal information for these reasons.[87]

In addition to privacy policies that reference primary and secondary uses, creating a type of coercive contracting for personal information, many privacy notices also contain some language giving the organization the right to change the terms at any time.[88]

---

[83] Uses outside the primary purpose for collection, namely providing goods or services, are typically called *secondary uses*, and frequently these uses are bundled in privacy notices. *See* Tschider, *The Consent Myth*, *supra* note 20, at 1515.

[84] *See Your Data Is Shared and Sold . . . What's Being Done About It?*, KNOWLEDGE@WHARTON (OCT. 28, 2019), https://knowledge.wharton.upenn.edu/article/data-shared-sold-whats-done/ [https://perma.cc/UN46-EYNR].

[85] *See generally* Carol M. Hayes & Jay P. Kesan, *Privacy, Law, and Cloud Services*, *in* ENCYCLOPEDIA OF CLOUD COMPUTING 245 (San Murugesan & Irena Bojanova eds., 2016), https://doi.org/10.1002/9781118821930.ch20 [https://perma.cc/XDD9-K593] (describing the challenges of managing privacy with the inclusion of third parties, secondary uses, and data transfer).

[86] *See* Tschider, *The Consent Myth, supra* note 20, at 1520.

[87] *Id.* at 1520 n.78.

[88] *See* Klass, *supra* note 63, at 56–57.

In the United States, contract law does not limit an organization's ability to change material terms, or require any re-consenting to new terms.[89] And, if the consumer does not want their data to be collected, used, and retained pursuant to new terms, the only option for that consumer is to stop service. This means that the actual terms hardly matter to the enforceability of the agreement, so long as consent is gathered at some time. It is clear, then, that actual acceptance of the terms of the agreement and, following, assent, is truly not important; consent is. If consent, then, has less power than assent in contract law, what value does it really have?

Consent is even more ineffectual as a proxy for consumer choice in contract law than in tort law, in part due to its essential position in contract formation. First, the relational position of the consumer versus the organization makes for an inherently one-sided relationship,[90] one in which no promises are actually made, and where even the terms provided to induce consent can be changed at the election of one party.[91] These contractual issues occur across a background where unconscionability is already very difficult to prove in a court of law and where parties have to rely on courts to determine what is and is not unconscionable.[92] Indeed, as Paul Bennet Marrow suggests, "it's a bit like religion: unconscionability

---

[89] Indeed, the Restatement (Third) of Contracts proposed language includes the reporters' observation that additional requirements regarding assent in privacy notices would result in increased transactions costs without real benefit. *Id.* at 53–54.

[90] It should be noted here that the duties of a party in contract are specified in the contract rather than in tort, where duties are based on a similarly situated or reasonably prudent organization. Part III describes how this divergence between these two bodies of law has resulted in a call for a unique form of fiduciary relationship: the information fiduciary. While the Author does not believe an overt requirement for information fiduciary status is warranted, the recommendation in Part IV illustrates how enhanced obligations as an alternative to consent can nevertheless inure to specific kinds of parties collecting, using, and retaining personal information.

[91] *See* Klass, *supra* note 63, at 56–57.

[92] Paul Bennett Marrow, *Contractual Unconscionability: Identifying and Understanding Its Potential Elements*, 72 J. N.Y. BAR ASS'N 18, 20 (2000). Much more can be said about unconscionability, but the takeaway here is that as a way to find a privacy notice unenforceable, this is unlikely to render a positive outcome for plaintiffs.

exists in the minds of true believers. This seems to leave the draftsman with the charge of predicting the whims of mysterious forces."[93] The question, then, is why does consent have any real value when what an individual consents to might not even represent any actual commitment? If it can represent some commitment, how can consent to unfair, one-sided, readily changeable terms actually represent real choice? While a consumer's consent might demonstrate an intention to be bound, the organization's privacy notice communication does not.

C. Federal Statutes Including Consent

The United States has, at least for sectoral laws, included consent, whether explicit or implied, in federal and state law.[94] It is possible that such state legislatures and Congress recognized the challenges of integrating informational privacy within the traditional common law system of tort and contract. More likely, it resulted from a recognition of potential consequentialist risks inherent in using personal information within computerized systems, such as disclosure of sensitive data to parties adverse to the interests of the individual.[95]

National discussions around consent in federal law began in the late 1960s, spurred by national initiatives for statistical data gathering.[96] The Fair Credit Reporting Act of 1970 ("FCRA") first established a consent requirement for medical record access.[97]

---

[93] *Id.*

[94] *See* Tschider, *The Consent Myth*, *supra* note 20, at 1515 (describing authorization under the Health Insurance Portability and Accountability Act); TSCHIDER, *supra* note 26, at 88 n.89.

[95] These are the types of risks typically recognized in privacy harm analysis, as in Danielle Keats Citron and Daniel Solove's work. *See generally* Citron & Solove*, supra* note 80 (identifying consequentialist risks as harms).

[96] INTERNAL REVENUE SERV., STATISTICAL USES OF ADMINISTRATIVE RECORDS: RECENT RESEARCH AND PRESENT PROSPECTS 472 (1984).

[97] 15 U.S.C. § 1681a(i). The primary reason for requiring individual consent for medical record disclosure was due to a concern over medical data interpretation without counsel of a qualified practitioner and retention of the traditional physician-patient relationship. *See The Fair Credit Reporting Act: Are Business Credit Reports Regulated?,* 1971 DUKE L.J. 1229, 1233 n.21 (1971). Since 1970,

Congress commissioned further inquiry via the Professional Standards Review Organizations ("PSROs") and the Privacy Protection Study Commission in 1972 and 1977, respectively, which both explored the concept.[98]

In 1972, Congress created the PSROs to monitor appropriateness, quality, and outcomes of services provided to government health program beneficiaries.[99] The propensity for people to move and the increased use of medical records in legal proceedings (especially in malpractice suits) buoyed development and concentrated focus on medical record-keeping.[100] Participants in the subsequent Factual Service Bureau's medical records hearings criticized consent and authorization procedures used traditionally by medical care providers.[101] Commission witnesses described how a patient form effectively results in a patient "signing away all control over what is disclosed and what may be done with it thereafter," and that such disclosures are broadly worded.[102]

1. Government Studies on Privacy – The 1970s

In 1973, the U.S. Department of Health, Education, and Welfare ("HEW") drafted an advisory report, *Records, Computers, and the Right of Citizens*, which informed much of the Privacy Act of 1974 governing federal privacy guarantees.[103] Importantly, HEW first raised a principle of consent in relation to purposes outside those communicated to an individual: "[t]he agency should 'assure that no use of individually identifiable data is made that is not within the stated purposes of the system as reasonably understood by the

---

the FCRA now requires various types of consent for different activities, such as an affirmative consent requirement to access medical information for insurance purposes and a written consent requirement for employment background checks. *See* 15 U.S.C. § 1681a.

[98] PRIV. PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977). The PSROs initially focused on consistency for cost control and quality assessment, recognizing the tradeoffs between service and personal privacy.

[99] *See id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] *See* INTERNAL REVENUE SERV., *supra* note 96, at 472.

individual, unless the informed consent of the individual has been explicitly obtained.'"[104] Explicit consent usually requires some overt manifestation of consent, such as clicking a button or providing a signature, and HEW's focus on "explicit consent" at that time likely conveyed a seriousness in relying on consent as representative of individual choice.[105]

Moreover, HEW first created an advisory committee, the Advisory Committee on Automated Data Systems ("Advisory Committee"), to identify information practices that could reduce individual privacy risk.[106] The Advisory Committee proposed the following "fair information practice principles" ("FIPPs") with respect to personal information (broadly defined):

> 1) No . . . record-keeping systems whose very existence is secret [Transparency]; 2) a way for an individual to find out what information about him is in a record and how it is used [Access]; 3) a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent [Choice]; 4) a way for an individual to correct or amend a record of identifiable information [Correction]; 5) any organizations creating, maintaining, using, or disseminating records . . . must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data [Security].[107]

These FIPPs were adopted by the Federal Trade Commission ("FTC") in its evaluation of unfair or deceptive trade practices, which are now considered guidance informing the FTC's interpretation of what constitutes unfair or deceptive trade practices under Section 5 of the FTC Act.[108]

---

[104] *Id.* at 473.

[105] *See* TSCHIDER, *supra* note 26, at 15.

[106] Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIV. F. (Dec. 19, 2007), https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/ [https://perma.cc/V77V-VLGD].

[107] *Id.*; Letters from Willis W. Ware and Caspar W. Weinberger (July 1, 1973), https://www.epic.org/privacy/hew1973report/foreword.htm [https://perma.cc/QP8F-2EAJ].

[108] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE ii–iii (May 2000), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf

Anticipating a computerized future on the horizon, Congress created the Privacy Protection Study Commission in 1977 ("Commission") to broadly consider privacy in data banks, automatic data processing programs, and information systems, including private organizations.[109] The Commission specifically cautioned against reliance on individual authorizations for privacy in medical record-keeping:

> One tends to forget that a patient usually has no way of knowing what is in a medical record about him, no way of controlling the accuracy or pertinence of the information it contains . . . As indicated earlier, consent to the disclosure of medical-record information about oneself is rarely voluntary . . . [A]n authorization can serve as a means of controlling the disclosure of information about oneself but never as a means of giving voluntary consent, and it can only serve as a means of control if the patient knows what it is he is authorizing to be disclosed.[110]

The Commission observed that patients should have the ability to pursue their own privacy objectives outside a basic authorization, including: the ability to access and correct medical record contents, improved awareness of consent and medical record uses, and the ability to "control not only the amount and type of information that is disclosed to other types of users, but also the conditions under which such disclosures are made."[111]

The Commission eventually recommended seven authorization requirements, including that such authorization occur prior to information disclosure, in writing, signed by the individual.[112] The contents of the disclosure include information about the recipients of the information, the nature of the information disclosed, the purposes for information use at time of disclosure and in the future, and an expiration date not to exceed two years.[113]

Special focus on general privacy began with HEW's advisory report in 1973,[114] but until 1996, Congress did not commission any

---

[https://perma.cc/8EMY-MT8A]; The Fed. Trade Comm'n Act of 1938, 15 U.S.C § 45 [hereinafter FTC Act].

[109] *See* PRIV. PROT. STUDY COMM'N, *supra* note 98.

[110] *Id.*

[111] *Id.*

[112] *Id.*

[113] *Id.*

[114] *See* INTERNAL REVENUE SERV., *supra* note 96, at 472–73.

additional inquiry for health sector privacy, especially for private entities.[115] By the mid-1980s, Congress focused on communications privacy, passing the Electronic Communications Privacy Act ("ECPA") in 1986 to broadly regulate modern digital communications over the Internet.[116] The ECPA, importantly, included a consent exception for a broad prohibition on accessing electronic communications, including a federal standard of one-person consent that could grant access to providers.[117]

2. The Health Insurance Portability & Accountability Act ("HIPAA")

The most significant sectoral privacy developments for the United States included the Health Insurance Portability and Accountability Act ("HIPAA"), which echoed a similar model in the financial sector, the Gramm-Leach Bliley Act ("GLBA").[118] HIPAA was originally the brainchild of the Workgroup for Electronic Data Interchange Committee ("WEDI"), which was commissioned to reduce healthcare administrative costs by the first Bush Administration in 1991.[119] The U.S. Department of Health and Human Services ("HHS") developed the HIPAA Privacy Rule ("Privacy Rule") over the course of three years, after substantial comments and changing perspectives on whether consent was

---

[115] *See*, *e.g.*, The Government in Sunshine Act of 1977, 5 U.S.C. § 552b; The Computer Matching and Privacy Protection Act of 1988, Pub. L. 100-503, Pub. L. 101-56 (1988) (amended 1989); The Paperwork Reduction Act of 1995, 44 U.S.C. § 3501.

[116] The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510, 2701. The ECPA provided an option for explicit consent to overcome providers accessing electronic communications. *See id.*

[117] *Id.* The consent exemption under the ECPA is so broad you can drive a truck through it, so to speak. And, for criminal law scholars, the ECPA's consent exemption helped to mobilize the oft-publicized third-party doctrine, wherein (with some limits) law enforcement could lawfully access personal information shared with a third-party like an electronic communications service provider pursuant to consent. *See* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 572 (2009).

[118] Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 117 YALE J. HEALTH POL'Y, L. & ETHICS 143, 149–50 (2017).

[119] Joseph Conn, *HIPAA, 10 Years After*, MODERN HEALTHCARE (Aug. 7, 2006, 1:00 AM), https://www.modernhealthcare.com/article/20060807/NEWS/608070324/hipaa-10-years-after; *About Us*, WEDI (2018), https://www.wedi.org/about-us [https://perma.cc/NEU4-FX73].

integral to the Privacy Rule.[120] Ultimately, HHS did not integrate consent for all healthcare activities into the Privacy Rule.[121]

As the name might suggest, HIPAA's first draft pivoted a broad administrative goal into a bipartisan insurance reform agenda.[122] Senators Nancy Landon Kassebaum and Edward M. Kennedy originally designed HIPAA to allow portability of insurance between employers with protection for preexisting conditions, so-called "job lock."[123] The bi-partisan HIPAA bill passed unanimously in the Senate in 1996, establishing requirements for the digitization and standardization of electronic health data record-keeping.[124] However, the crucial Privacy Rule was not passed until seven years later, with considerable challenges.[125]

HHS developed the first version of the Privacy Rule at the end of 2000, with the final version effective in April of 2003.[126] HHS had developed the Privacy Rule because Congress had failed to create a privacy rule with sufficient support by August of 2000, when HHS was triggered to develop the rule.[127] The Privacy Rule, in its original form, which had stripped out consent requirements, received 54,000

---

[120] *See* GINA STEVENS, CONG. RSCH. SERV. RS20934, A BRIEF SUMMARY OF THE HIPAA MEDICAL PRIVACY RULE , at CRS-5 (2003).

[121] *Id.* at CRS-6.

[122] Jane Hiebert-White, *Who Won What in the Kassebaum/Kennedy Struggle?* HEALTH PROGRESS (Oct. 1996), https://www.chausa.org/docs/default-source/health-progress/health-policy---who-won-what-in-the-kassebaumkennedy-struggle-pdf.pdf?sfvrsn=0 [https://perma.cc/8V6L-UEJ9].

[123] *Id.*

[124] *See* STEVENS, *supra* note 120; *HIPAA – the Federal Medical Privacy Rule*, CITIZENS' COUNCIL FOR HEALTH FREEDOM [hereinafter CITIZENS' COUNCIL], http://www.cchfreedom.org/cchf.php/268 [https://perma.cc/Q8SZ-M8CQ] (last visited Apr. 1, 2018).

[125] *Id.*

[126] *See* The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, August 21, 1996, 110 Stat 1936; CITIZENS' COUNCIL, *supra* note 124. The first version of HIPAA required that Congress develop a privacy rule by August 1999. Failing this, HHS would have to draft a privacy rule.

[127] The Health Insurance Portability and Accountability Act of 1996, Pub. L. 104–191, August 21, 1996, 110 Stat 1936; *see* CITIZENS' COUNCIL, *supra* note 124.

public comments, with eighty percent of comments referencing "losing control" over access to record data.[128]

As a result of the commentary, HHS reversed its position and reintroduced consent language.[129] In 2001, the Bush Administration reopened the comment period and received an additional 24,000 comments.[130] The majority of comments favored consent, and the Bush Administration retained the consent provision.[131] By 2002, however, the Bush Administration had removed consent from the Privacy Rule and received an additional 11,000 comments favoring consent.[132] It appears that organizations providing health services were concerned about operationalizing a consent requirement when many steps of healthcare provisioning occur in advance of actual patient treatment.[133] In August 2002, the Privacy Rule was passed without incorporating consent, instead introducing a reasonable acknowledgement of receipt and explicit written authorization for secondary data uses.[134]

HIPAA is unique in that it combines both implied consent for primary data uses (treatment, payment, and healthcare operations) and explicit consent to balance market interests in administrative

---

[128] *See* Conn, *supra* note 119.

[129] *See* CITIZENS' COUNCIL, *supra* note 124.

[130] *Id.*

[131] *Id.*

[132] *Id.*

[133] *See Why Was the Consent Requirement Eliminated from the HIPAA Privacy Rule, and How Will It Affect Individuals' Privacy Protections?*, U.S. DEP'T OF HEALTH & HUM. SERVS. (July 26, 2013), https://www.hhs.gov/hipaa/for-professionals/faq/193/why-was-the-hipaa-privacy-rule-consent-requirement-removed/index.html [https://perma.cc/364R-LJ5R].

[134] *See* Conn, *supra* note 119. In recent developments, HHS has now moved towards eliminating the reasonable acknowledgement requirement in its proposed rule changes along with bolstering other privacy commitments, such as timely fulfillment of access requests. *See* Anna D. Kraus, Libbie Canter, Rebecca Yergin & Tara Carrier, *HHS Announces Proposed Changes to HIPAA's Privacy Rule*, COVINGTON DIGIT. HEALTH BLOG (Dec. 21, 2020), https://www.covingtondigitalhealth.com/2020/12/hhs-announces-proposed-changes-to-hipaas-privacy-rule/ [https://perma.cc/98UB-CGWZ].

efficiency with privacy for protected health information ("PHI").[135] However, unlike other laws establishing a ceiling for privacy obligations with express preemptive power, HIPAA created a floor, permitting state legislatures to pass more restrictive laws applicable to PHI.

3. The Gramm-Leach-Bliley Act

The GLBA quickly followed HIPAA's initial passage in 1996, establishing privacy requirements in 1999.[136] The goal of GLBA was to modernize financial transactions in light of new mergers that would have enabled unrestricted access to personal information from a variety of different organizations, such as insurers, banks, stockbrokers, and other financial institutions.[137] GLBA sought to include more of these merged organizations by applying GLBA broadly to "financial institutions."[138]

GLBA is interesting because it begins with a statutorily created obligation: "each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."[139] This statutorily created duty removed any question regarding the nature of duties pursuant to financial contracts between customers and their financial institutions.[140]

---

[135] There is no consent requirement under HIPAA for treatment, payment, and healthcare operations, only required acknowledgement. 45 C.F.R. § 164.520(e) (2013). Consent is required for authorizing secondary data uses. 45 C.F.R. § 164.508(a)(2)–(a)(4), (b)(5) (2013).

[136] *See* The Gramm-Leach-Bliley Act of 1999, 15 U.S.C. § 6801 [hereinafter GLBA]. After GLBA was passed, the law was copied and applied to investment brokerages by the Securities Exchange Commission under Regulation S-P (Reg S-P). *See* 7 C.F.R. § 248.1 (2004).

[137] *The Gramm-Leach Bliley Act*, EPIC (2021), http://epic.org/privacy/glba/default.html [https://perma.cc/E6GA-LPNG].

[138] 15 U.S.C. § 6801; 12 U.S.C. § 1813.

[139] 15 U.S.C. § 6801(a).

[140] This imprecision regarding relational duties in organization to consumer contracts is specifically the challenge associated with determining commitments in a privacy notice within common law contract disputes. *See supra* Part II(D)(2).

Despite creating a duty, consent was not required under GLBA.[141] Although Senator Richard H. Bryan of Nevada proposed an amendment "to give customers notice and choice about how their financial institutions share or sell personally identifiable sensitive financial information," the amendment was ultimately withdrawn.[142] Rather, a financial institution's customer could "opt-out" of certain data transfers to third parties after being provided notice.[143] Opt-outs, here, worked by creating consent by implication: if a customer did not opt-out, it was presumed the customer consented.[144] GLBA did restrict additional downstream data uses beyond the initial third-party disclosure subject to the opt-out, which limited, at least in some respects, additional data use beyond what was originally disclosed.[145] Furthermore, prohibitions on disclosure were subject to a broad exemption, wherein "consent at the direction of the consumer" would remove any general prohibitions.[146]

HIPAA and GLBA represent some of the largest and most comprehensive privacy legislation, albeit sectoral, established in the United States.[147] Both illustrate various approaches to consent.[148]

---

[141] 15 U.S.C. § 6802(b) (stating that even though consent is required for sharing with an unaffiliated third party, consent is implied for the original privacy notice displayed).

[142] S. 900, S. Amdt. 316, 106th Cong. (1999–2000), https://www.congress.gov/amendment/106th-congress/senate-amendment/316?r=3&s=a [https://perma.cc/WM2T-GB9G].

[143] 15 U.S.C. § 6802(b)(1).

[144] This is consent by implication. *See* TSCHIDER, *supra* note 26, at 15.

[145] 15 U.S.C. § 6802(c).

[146] H.R. REP. NO. 106-434 (1999-2000); 15 U.S.C. § 6801(e)(2).

[147] Both laws include not only privacy obligations but also information security requirements in the form of, respectively, the Security Rule and Safeguards. *See* DEREK E. BAMBAUER, JUSTIN (GUS) HURWITZ, DAVID THAW & CHARLOTTE A. TSCHIDER, CYBERSECURITY: AN INTERDISCIPLINARY PROBLEM 414 (2021); TSCHIDER, *supra* note 26, at 277–78.

[148] As previously described, HIPAA requires authorization and GLBA may require explicit consent in the transfer of data to third parties outside the scope of primary service-based activities. However, neither require explicit consent for an individual to receive primary services. *See* U.S. DEP'T OF HEALTH & HUM. SERVS., *supra* note 133; Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COL. L. REV. 583, 600–04 (2014) (describing the expansion of jurisdiction and FTC enforcement creating a *de facto* role of the FTC as primary privacy authority).

Despite these various approaches in both laws for HIPAA authorization and GLBA consumer-directed consent, explicit consent is the preferred method for overcoming restrictions to personal information collection and use, especially for downstream parties.[149]

4. The FTC Act Section 5

Although several laws, such as the Children's Online Privacy Protection Act ("COPPA") and the Telephone Consumer Protection Act ("TCPA"), illustrate the interesting and sometimes divergent U.S. procedural models for consent, the most powerful influencer of privacy behaviors is arguably the FTC.[150] In its prosecution of unfair and deceptive trade practices under Section 5, the FTC has occupied a role as primary privacy regulator in the United States, despite few judicial decisions to show for it.[151] The FTC is also responsible for sole rulemaking and enforcement under COPPA, partial rulemaking and enforcement of GLBA, and promulgation of rules applicable to the similar activities regulated under TCPA.[152]

---

[149] *See* BAMBAUER ET AL., *supra* note 147; *see* TSCHIDER, *supra* note 26.

[150] *See* The Children's Online Privacy Protection Act of 1998 (COPPA), 15 U.S.C. § 6501(9) (requiring consent from parents prior to processing personal information over the Internet for children under age 13); 16 C.F.R. § 312.5(a)(1) (2013) (requiring parental reconsent when proposed collection and use changes); The Telephone Consumer Protection Act of 1991 (TCPA) 47 U.S.C. § 227. (permitting opt-out consent revocation rather than upfront consent to receive marketing calls and texts).

[151] Solove & Hartzog, *supra* note 148, at 600–04 (describing the expansion of jurisdiction and FTC enforcement creating a *de facto* role of the FTC as primary privacy authority).

[152] *Id.* at 602. Despite the authors' description of the FTC's enforcement arm regarding GLBA as "past," the FTC still has enforcement authority under the Dodd-Frank Act. *See* H.R. Rep. No. 111-517, Title X, § 1024(c)(3)(A). Further, FTC obligations under GLBA to create regulations for safeguarding personal information still apply under Subtitle A. *Id.* The FTC co-manages the "Do Not Call Registry," which was created by administrative rule. FED. TRADE COMM'N, NATIONAL DO NOT CALL REGISTRY (June 2019), https://www.consumer.ftc.gov/articles/0108-national-do-not-call-registry [https://perma.cc/Z9K8-X2E3]. Similarly, the FTC enforces the Telemarketing Sales Rule. 16 C.F.R. § 310 (2010).

Congress passed the FTC Act in 1914 as part of the Clayton Act.[153] In the original version of the FTC Act, Section 5 stated "[u]nfair methods of competition in commerce are hereby declared unlawful."[154] As originally enacted, legislative history demonstrates that Congress intended to give the FTC broad authority to enforce against a wide variety of conduct, not limited by specifically enumerated practices or categories of practices.[155] In *FTC v. R.F. Keppel & Bro., Inc.*,[156] the Supreme Court interpreted Section 5 as applicable to consumers rather than only applicable to anti-competitive activities.[157] The Wheeler-Lea Amendments of 1938 made the FTC's consumer focus explicit.[158] The current text gives the FTC broad rulemaking and enforcement authority over unfair or deceptive trade practices ("UDAP") authority.[159]

At the federal level, generalized "privacy law" is often enforced by the FTC under Section 5 of the FTC Act, which enables the FTC to enforce against UDAP.[160] In addition to prosecuting for inaccurate product labels, the FTC has adapted Section 5 to information privacy and security, arguably creating a body of law through enforcement actions and settlements that is somewhat consistent, producing some degree of predictability.[161] The FTC's FIPPs, although non-binding in their authoritative function, in addition to

---

[153] *See* Peter C. Carstensen & Nina H. Questal, *Use of Section 5 of the Federal Trade Commission Act to Attack Large Conglomerate Mergers*, 63 CORNELL L. REV. 841, 850 (1978).

[154] *Id.* at 850–51.

[155] *Id.* at 851. Scholars have criticized the extremely broad nature of FTC enforcement, especially as it applies to unfair commercial practices. *See* Teresa M. Schwartz, *Regulating Unfair Practices under the FTC Act: The Need for a Legal Standard of Unfairness*, 11 AKRON L. REV. 1, 2 (describing the FTC as an "aggressive and imaginative rule-maker, particularly in exploring and expanding the definition of 'unfair acts or practices.'").

[156] FTC v. R.F. Keppel & Brother, Inc., 291 U.S. 304 (1934).

[157] *See* Carstensen & Questal, *supra* note 153, at 852.

[158] CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 3–4 (2016).

[159] 15 U.S.C. § 45(a).

[160] *See generally* Solove & Hartzog, *supra* note 148, at 600–04 (describing, in detail, the role of the FTC under Section 5 as the default privacy regulator in the United States).

[161] *See id.* at 619.

the FTC's consent orders and settlements, give some sense of how the FTC interprets UDAP in relation to privacy.[162] Notably, the FIPPs denote notice and "choice" as appropriate mechanisms, absent any discussion of contextual or other relational imperfections that could render consent ineffective.[163]

The FTC's focus on investigation and enforcement under UDAP rather than legislative development has led scholars such as Daniel J. Solove and Woodrow Hartzog to call the FTC's enforcement activity the "New Common Law of Privacy."[164] Not only has the FTC established an informal precedential function in its collective of consent decrees, but it has also developed a "soft law" of sorts with guides, guidelines, reference documents, and reports. These not only govern future FTC enforcement activities but also put the community of privacy professionals and organizations on notice via publicly posting these materials.[165]

The FTC, through regulatory oversight of federal laws, collaborative oversight over others, and a broad consumer protection directive under the FTC Act, has certainly embraced its default position as the primary privacy regulator, enforcing UDAP.[166] Since 1995, the FTC has heavily focused on protecting

---

[162] *See* FTC Act § 45.

[163] It should be noted that although the word "choice" is used, consent is contextually how the choice requirement is fulfilled. *See* HOOFNAGLE, *supra* note 158, at 5–6. The FTC has a variety of mechanisms for enforcing against unfair or deceptive trade practices including injunctive relief, equitable relief, or fine structures, typically finalized via a consent decree, or settlement.

[164] *See* Solove & Hartzog*, supra* note 148, at 619.

[165] *See id.* at 625–27.

[166] The FTC has specific, not general enforcement authority within the Children's Online Privacy Protection Act of 1998 ("COPPA"). *See* 15 U.S.C. §§ 6502(a), 6503, 6505. The FTC also enjoys co-extensive regulatory enforcement with the Federal Communications Commission over The Telephone Consumer Protection Act of 1991 ("TCPA"). *See* 15 U.S.C. § 6102(c)(2), and the FTC's Telemarketing Sales Rule ("TSR"). The FTC, along with the Department of Commerce, are also positioned to receive EU complaints on behalf of the United States, though it is unknown what future the FTC has with respect to cross-geographic data transfer arrangements after the recent *Schrems I* & *Schrems II* cases. *See* GUIDE TO THE EU-U.S. PRIVACY SHIELD*,* EUR. COMM'N 12 (2016), https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf

sensitive consumer information, and beginning in 2002, the FTC protected data security practices as an extension of privacy.[167] In 2001, the FTC shifted away from seeking new privacy legislation to enforcing existing consumer protection statutes as its primary objective.[168]

The sectoral, statutory, and UDAP approaches to privacy law in the United States illustrate that regardless of whether consent is explicit or implied, consent is the primary mechanism for legally permitting collection and use of personal information, a functional proxy for choice. Indeed, although many privacy laws include other management requirements, such as providing for access requests to personal information and the ability to correct personal information, notice and consent continue to be a lodestar in U.S. privacy law.

III. THE EU'S DATA PROTECTION HISTORY

The EU's data protection laws originated as an extension of civil rights commitments after World War II.[169] From early developments, consent was an important (but not exclusive) part of EU law.[170] Importantly, consent was not the only lawful basis for processing data under the Data Protection Directive of 1995, even before the GDPR came into effect in 2018.[171] Consent in the EU, as one of multiple lawful bases for processing, was not necessarily

---

[https://perma.cc/6QZ5-AV4Q]; Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650 (E.C.J.); Data Protection Comm'r v. Facebook Ireland Ltd., 2018 E.C.R. 559 (E.C.J.).

[167] GINA STEVENS, CONG. RSCH. SERV., R43723, THE FEDERAL TRADE COMMISSION'S REGULATION OF DATA SECURITY UNDER ITS UNFAIR AND DECEPTIVE ACTS OR PRACTICES (UDAP) AUTHORITY 1–3 (2014).

[168] *Id.* at 3. This movement likely inspired Daniel Solove and Woodrow Hartzog's investigation of FTC enforcement strategies. *See also* Solove & Hartzog, *supra* note 148, at 588 (describing the FTC as "reigning over more territory than any other agency that deals with privacy"). *Cf.* Justin (Gus) Hurwitz, *Data Security and the FTC's UnCommon Law,* 101 IOWA L. REV. 955, 980 (2016) (arguing that although the FTC has developed "common law" through potentially coherent rules does not necessarily mean this less or "un" common law effectively reflects effective judicial practices, particularly when FTC activities remove other decision-making bodies from the process).

[169] *See infra* Part III(A) and accompanying notes.

[170] *See infra* Part III(B) and accompanying notes.

[171] *See infra* Part III(B) and accompanying notes.

used as a proxy for choice.[172] Rather, consent facilitates a data subject's personal risk acceptance for the benefit of an organization (public or private).[173] Today, consent is one of multiple means for brokering decisions related to personal information, including balancing tests like legitimate interest balancing.[174]

A. Data Protection Origins in Civil Rights

In Europe, organized commitments to common human rights resulted from atrocities in World War II, when governments used personal information about citizens to arrest and kill them simply based on their status, including ethnic origins, religious affiliations, and disability status. The Universal Declaration of Human Rights, adopted on December 10, 1948, and actively promoted by the United States through Eleanor Roosevelt's position on the drafting committee,[175] memorialized a common commitment to "the inherent dignity and inalienable rights of all members of the human race in the foundation of freedom, justice, and peace in the world."[176] The UN Declaration formed the basis for developing informational privacy law:

> No one shall be subjected to arbitrary interference with his privacy, family home *or correspondence*, nor to attack upon his honour and reputation. Everyone has the right of the protection of the law against such interference or attacks. [. . .] Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, *receive and impart information and ideas through any media and regardless of frontiers*.[177]

Although the United States strongly influenced the development of this crucially important declaration, soon after, the United States began to distance itself from similar international human rights

---

[172] *See infra* Part III(D)–(E) and accompanying notes.

[173] *See infra* Part III(D) and accompanying notes.

[174] *See infra* Part III(D) and accompanying notes.

[175] Marie Wilken, *U.S. Aversion to International Human Rights Treaties*, GLOB. JUST. CTR. BLOG (June 22, 2017), https://www.globaljusticecenter.net/blog/773-u-s-aversion-to-international-human-rights-treaties [https://perma.cc/QVJ2-BWNP].

[176] G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948).

[177] *Id.* at art. 12, art. 19 (emphasis added) (citation omitted).

commitments.[178] The Council of Europe, however, continued to solidify its commitment to privacy in successive conventions and laws. The Council of Europe and European signatories confirmed many of the commitments of the Universal Declaration of Human Rights and prohibited government interference in these rights.[179] These rights, however, even for European signatories, were not absolute, noting:

> The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society . . . for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence . . . .[180]

Following technological developments and an increased concern for informational privacy, the Council of Europe published Recommendation 509 on human rights, and in 1973 and 1974 focused on the role of data banks with respect to privacy commitments.[181]

B. European Country Developments

After the Council of Europe provided broad recommendations, individual countries began to develop individualized approaches to privacy by passing both bars on the government use of personal information and commitments to privacy in their Constitutions.[182] A state in Germany was the first to pass such a commitment to informational privacy as statute in 1970, followed by a national statute in 1977, the Gesetz zum Schutz vor Mißbrauch

---

[178] Notably, the United States was the ninety-eighth signatory on the Convention on the Preservation and Punishment of the Crime of Genocide, finally signing in 1980 under the leadership of President Carter, despite the original Convention being drafted in 1948. *See* Wilken, *supra* note 175; Jimmy Carter, Genocide Convention Message to the Senate Recommending Ratification (May 23, 1977).

[179] *See* Sian Rudgard, *Origins and Development of European Data Protection Law*, *in* EUR. DATA PROT. L. & PRAC. 1, 5–6 (Eduardo Ustaran et al. eds., 2nd ed. 2018).

[180] Convention for the Protection of Human Rights and Fundamental Freedoms art. 10(2), Nov. 4, 1950, 213 U.N.T.S. 221.

[181] *See* Rudgard, *supra* note 179, at 7.

[182] *Id.*

personenbezogener Daten bei der Datenverarbeitung, or the Bundesdatenschutzgesetz.[183] The first European country to actually have a national data privacy authority was Sweden, as early as 1976.[184]

France similarly passed a national statute in 1978, the Act No. 78-17 of January 6, 1978, on Data Processing, Data Files, and Individual Liberties, simultaneously creating the first information privacy regulator, the Commission Nationale de L'informatique et des Libertés.[185] These two countries' early approaches likely influenced the development of later European commitments to information privacy, including those of other member states and the highly influential Organisation for Economic Co-operation and Development ("OECD") Guidelines.[186]

Notably, the original Bundesdatenschutzgesetz of 1977 in Germany explicitly references consent as the primary means of permitting access to personal information, generally by physical signature.[187] However, it also describes transfer of personal information being permitted when it is necessary for "lawful performance of the tasks under the responsibility of the transmitting body" or if the recipient can demonstrate a "legitimate interest" in the data being transmitted, when the rights of the data subject are not diminished.[188]

Similarly, in France, Act No. 78-17 required consent when processing data that are sensitive in nature, such as racial origins,

---

[183] *See* TSCHIDER, *supra* note 26, at 8.

[184] *See* ABRAHAM L. NEWMAN, PROTECTORS OF PRIVACY REGULATING PERSONAL DATA IN THE GLOBAL ECONOMY 87 (2008).

[185] *Id.*

[186] *See infra* Part III(C) and accompanying notes; Hon. Michael Kirby, *The History, Achievement and Future of the 1980 OECD Guidelines on Privacy*, 1 INT'L DATA PRIV. L. 6, 9–10 (2011) (describing the involvement of representatives from France and Germany).

[187] Gesetz zum Schutz vor Mißbrauch personenbezogener Daten bei der Datenverarbeitung [Bundesdatenschutzgesetz – BDSG] [Federal Data Protection Act], Jan. 27, 1977, BUNDESGESETZBLATT [BGBI] at 7 201, § 3, as amended Nov. 2019, BGBI 1626 (Ger.), http://www.gesetze-im-internet.de/bdsg_2018/BDSG.pdf (describing the writing requirement as only not being required due to special circumstances).

[188] *Id*. at § 11.

political, philosophical, or religious opinions, and union membership.[189] Although the French government did not introduce the concept of legitimate interest or other lawful processing, it did establish a regulatory model where organizations are responsible for registering themselves and the details of their processing activities with the government agency.[190] This registration activity presumably would have provided some ability to examine what organizations are doing, and whether what was disclosed matches what they are actually doing with respect to consumers.

C. The OECD Guidelines

As early as 1976, the European Commission was asked by the European Parliament to begin directing a harmonized data protection approach as countries like Germany and France began passing their own laws, while others passed Constitutional amendments.[191] Around the same time, the OECD worked in tandem with the European Commission to develop the OECD Guidelines while the Council of Europe held the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.[192] The OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ("OECD Guidelines") was completed in 1979, which were initiated by the Data Bank Panel as early as 1969.[193] The OECD Guidelines, created in 1980, have greatly influenced international laws on information privacy, including outside the EU, likely in part due to careful co-operation with the Council of Europe.[194]

The OECD Guidelines are tremendously helpful not only in what they contain, a blueprint for privacy principles, but for what

---

[189] Loi 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés [Data Protection Act], JOURNAL OFFICIEL DE LA RÉPUBLIQUE FRANÇAISE [J.O.] [OFFICIAL GAZETTE OF FRANCE], Jan. 7, 1978, p. 227 (Fr.).

[190] *Id.* at § 19.

[191] *See* Rudgard, *supra* note 179, at 7.

[192] *Id.*

[193] *See* TSCHIDER, *supra* note 26, at 9–10; ORG. FOR ECON. CO-OPERATION & DEV., GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), *reprinted in* OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA 11 (2003).

[194] *See* Kirby, *supra* note 186, at 10.

they do not include, which would be mirrored in country-specific privacy models.[195] Absent from the Guidelines are any reference to direct legal conditions for processing, instead focusing on steps an organization must take, such as limiting data use and disclosure for purposes specified upon its collection, and only permitting uses outside these purposes "with the consent of the data subject; or by the authority of law."[196] Further, the OECD Guidelines explained that "[t]here should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject."[197]

Notably, in the OECD Guidelines principles, the OECD recognized "the economic value of information and the importance of protecting 'data trade' by accepting rules of fair competition."[198] Despite a focus on civil rights, the OECD Guidelines seemed to contemplate the dual needs for individual choice *and* commercial development.

In the early 1980s, nearly two-thirds of European countries had some national privacy rules, but despite this, European community policymakers resisted formal consistency, instead calling for national legislation.[199] Finally, in 1989, consistency in a privacy approach became more desirable, and the national data protection authorities met in Berlin to collectively begin a coordinated approach.[200] The European Commission presented its privacy directive in 1992, and, in 1995, the EU Data Protection Directive was passed.[201]

---

[195] *See* TSCHIDER, *supra* note 26, at 8.

[196] *See* ORG. FOR ECON. CO-OPERATION & DEV., *supra* note 193, at 14.

[197] *Id.*

[198] *Id.* at 44.

[199] NEWMAN, *supra* note 184, at 84.

[200] *Id.* at 88.

[201] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31 ("Data Protection Directive"), https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=NL [https://perma.cc/WJ6T-53NY].

D. The Data Protection Directive of 1995

The Data Protection Directive ("the Directive") sought to adopt the OECD Guidelines and create uniformity between the EU member states.[202] The Directive permitted each country to pass a variation of the directive within each country's statutory system.[203] Although the Directive began as a legally enforceable framework, countries were not bound to pass the Directive as written.[204] The Directive ultimately was duplicated by several countries outside of the EU.[205]

The now-superseded Directive referenced consent in three articles. First, Article 7(a) of the Directive referenced consent as one of multiple lawful bases for processing.[206] As one of multiple lawful mechanisms for data processing, consent could demonstrate that organizations lawfully could process data, but it was one of many options, not the sole mechanism.[207] Next, under Article 8(2)(a), when sensitive personal information was collected, or specifically enumerated "special categories" of data, explicit consent was required.[208] Finally, according to Article 26(1)(a), data could be transferred to countries without an adequate level of protection according to EU standards if consent was unambiguous.[209]

---

[202] *See id.*

[203] *Difference between a Regulation, Directive and Decision*, U.S. DEPT. OF AGRIC. (Dec. 21, 2016), https://www.usda-eu.org/eu-basics-questions/difference-between-a-regulation-directive-and-decision/ [https://perma.cc/7RR8-H3WG].

[204] *Id.*

[205] *See* TSCHIDER, *supra* note 26, at 10.

[206] *See* Data Protection Directive, *supra* note 201, at art. 7.

[207] *Id.*

[208] *Id.* at art. 8(2)(a).

[209] *Id.* at art. 26(1)(a). One foundational element of the EU system was a broad prohibition on data transfer outside the EU unless one of three conditions was satisfied: 1) transfer to a third country determined to be "adequate" under formal Article 29 Working Party determination, 2) use of standard contractual clauses to contractually bind private entities to employ data protection mechanisms that were identical to the EU Data Protection requirements, and 3) formal review and approval of binding corporate rules ("BCRs"), which held organizations accountable to EU standards through their business practices. *Id.* The unambiguous consent requirement actually become disfavored for lawful data transfer such as the standard contractual clauses and adequacy determinations. *Id.*

The Data Protection Directive is named as such because the Directive commits to not only informational privacy protections but also reasonable security protection for data.[210] The combined model sought to place the data subject at the center of decision-making with respect to their information, by giving that individual a variety of tools to self-manage their privacy while also providing regulatory oversight for activities that are less visible to individuals, commonly referred to as data subject rights.[211]

Under the Directive, the various mechanisms listed, including *consent*, *explicit consent*, and *unambiguous consent* were used for a single purpose: to overcome a barrier to processing by prompting individuals to accept risk via their consent.[212] Indeed, although multiple lawful bases for processing were specified, Recital 33 seemed to direct member countries towards consent, with nationally adopted deviations (derogations) requiring specific notation based on need:

> Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundation the purpose of which is to permit the exercise of fundamental freedoms.[213]

The Directive appears to permit information collection and use to occur when otherwise the risk might be high by involving the individual in the decision. For example, the privacy notice was an important requirement under the Directive and, if organizations relied on consent as the lawful basis for processing, consent was relative to what information was provided in the notice.[214] When

---

[210] *See id.* at art. 1–17.

[211] *Id.* § V.

[212] *See id.* §§ II–III. Logically, this follows due to the positioning of consent—specifically used both as an option for lawful processing but also in situations rife with potential for abuse, such as in relation to sensitive data or when transferring to countries not deemed adequate in their privacy laws.

[213] *See id.* at recital 33.

[214] *See id.*

related to sensitive data, the Directive appears to presume that sensitive, protected classes of data are especially likely to involve risk to an individual, which is why the Directive requires explicit consent, or consent manifested in a tangible way.[215] Finally, for data transfer, consent operates to overcome inherently risky data transfers to countries that offer no legal data protection guarantees.[216]

From this perspective, consent, at least as established by the Directive in 1995, can be understood as facilitating individual risk acceptance for purposes of forming a relationship with an organization. This key difference under EU law—consent as risk acceptance—may not have been described in this manner under the Directive.

The overall multi-faceted nature of the Directive, wherein personal rights guarantees are enumerated separately, illustrates why consent alone does not promote individual autonomy or animate individual choice with respect to personal information. Rather, minimizing data collection, use, and disclosure, registering data processing activities, and fulfilling individual rights requests actually functioned to reinforce individual privacy rights, supporting "self-help" and enabling regulatory oversight.[217] The Directive was tremendously sophisticated not because it included a consent requirement and applied it broadly within a model of individual civil rights, but because the multi-faceted data protection framework it enshrined effectively brokered private and public relational models.

Notably, lawful bases under the Directive included but were not limited to consent. Additional lawful bases included processing in furtherance of a contract, out of legal necessity, such as due to an emergency, where an important public interest requires it, and when the recipients have a "legitimate" interest in the data.[218] Recitals 30, 45, 50, and 58, as well as Articles 6(1)(f), 15(2)(a)–(b), 18(3), 21(3), and 26(1)(f) all reference legitimate interests, although primarily the

---

[215] *See id.*
[216] *See id.*
[217] *See id.*
[218] *Id.* recital 58.

interest of the data subject is referenced.[219] Most interesting are the justifications for processing listed in the Recitals, specifying alternatives for further processing after data are collected.[220] Data processing may be permitted for historical, statistical, scientific purposes: with "consent of the data subject;" if "necessary for the conclusion or performance of a contract binding on the data subject;" when carried out to protect the life of the individual; for tasks in the public interest or official authority; and in the legitimate interests of a natural or legal person.[221]

In 2014, the Article 29 Working Party, or the primary EU data protection authority until the passage of the GDPR, issued guidance related to legitimate interest as a lawful basis for data processing.[222] In it, the Working Party drafted an official opinion for determining legitimate interest from the perspective of controllers (organizations determining the purpose and use of collected data) under the Directive.[223]

The Article 29 Working Party made some important observations regarding legitimate interest as part of the Directive's Regime and in preparation for the new GDPR in draft form at the time.[224] First, the Working Party references Convention 108, which was opened for signature in 1981 and was developed in tandem with the OECD Guidelines, to promote an important distinction: processing does not always interfere with privacy.[225] Rather, processing must fulfill certain conditions to ensure rights and freedoms are protected. This distinction is an important one: processing personal information is simply part of participating in society and negotiating between private and public spheres; what matters is that organizations do not abuse the privilege.

---

[219] *Id.* recitals 30, 45, 50, 58; arts. 6(1)(f), 15(2)(a)–(b), 18(3), 21(3), 26(1)(f).

[220] *Id.* recitals 27–32.

[221] *Id.* recitals 27–32.

[222] Opinion of the Working Party on the Protection of Individuals with Regard to the Processing of Personal Data No. 06/2014 of 9 April 2015, 844/14/EN WP 217, at 3, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf [https://perma.cc/5NMH-5T4K].

[223] *Id.*

[224] *See id*. at 8–9.

[225] *Id.* at 6–7.

The Article 29 Working Party describes the legitimate interests of the controller (usually the organization collecting personal information) as the last lawful basis for data processing.[226] This option calls for a balancing test where the legitimate interests of the controller must be balanced against the "interests or fundamental rights and freedoms of the data subject."[227] What is perhaps most striking, however, is the Article 29 Working Party's perception of consent and other lawful bases under the Directive:

> The first five grounds of Article 7 rely on the data subject's consent, contractual arrangement, legal obligation or other specifically identified rationale as ground for legitimacy. When processing is based on one of these five grounds, it is considered as a priori legitimate and therefore only subject to compliance with other applicable provisions of the law. There is in other words a presumption that the balance between the different rights and interests at stake — including those of the controller and the data subject — is satisfied — assuming, of course, that all other provisions of data protection law are complied with.[228]

The Working Party goes on to explain how the legitimate interest test requires a specific inquiry, including a balancing test.[229] What is perhaps the most remarkable of these comments is the automatic assumption that, when consent is used, it is considered *a priori* legitimate.[230] The issues with consent, described in Part IV demonstrate why a more specific test may actually be more legitimate, either in addition to explicit consent or in lieu of consent in limited scenarios.

The Article 29 Working Party also explains how a legitimate interest test could work in practice.[231] First, the interest could "be compelling and beneficial to society at large," whereas other interests could be less compelling, such as a private company learning about its customers for targeted advertisement.[232] Although organizations have to engage in a balancing test, at a minimum, interests must meet the following requirements:

---

[226] *Id.* at 9.
[227] *Id.*
[228] *Id.*
[229] *Id.* at 28, 30–33.
[230] *Id.* at 9.
[231] *See id.* at 25–26.
[232] *Id.* at 24.

> In order to be relevant under Article 7(f), a 'legitimate interest' must therefore: - be lawful (i.e. in accordance with applicable EU and national law); - be sufficiently clearly articulated to allow the balancing test to be carried out against the interests and fundamental rights of the data subject (i.e. sufficiently specific); - represent a real and present interest (i.e. not be speculative).[233]

One important observation of the Working Party is that the concept of legitimate interest is highly contextual. An interest may be legitimate if a controller can pursue the interest in a way that complies with the law.[234] Considering this concept more broadly, the Working Party also seems to suggest that minimal impact to the rights and freedoms of data subjects might also result in the likelihood of interest legitimation.[235] Although the Working Party does not ultimately create a formulaic test, its interpretation of legitimate interest certainly offers perspective as to its creation as an alternative to other specifically enumerated lawful bases for processing, such as consent.

E. The General Data Protection Regulation

In 2018, the GDPR became effective for organizations that did business with EU residents, including extra-territorial organizations.[236] This expansive, long-arm application introduced EU law to U.S. companies, either through direct regulation as data controllers or indirect regulation as third-party processors for these controllers, such as technology third parties.[237] The broad application of the GDPR influenced how many organizations managed privacy, the most persuasive involving the fine structure: for U.S. companies not complying with the GDPR, the Data Protection Authorities have the ability to fine an individual company up to four percent of its total global revenue.[238]

The GDPR did not radically change the lawful basis model introduced under the Directive. Under Article 6(1)(f), the GDPR similarly included legitimate interest analysis as an alternative to

---

[233] *Id.* at 25.
[234] *See id.*
[235] *See id.* at 36.
[236] *See* Commission Regulation 2016/679, 2016 J.O. (L 119) 19-22 (EC).
[237] *Id.*
[238] *Id.* at 83.

other lawful basis, and notably, no guidance by the European Data Protection Board (which superseded the Article 29 Working Party) has been issued.[239] Specific countries have developed models for analyzing legitimate interest within the confines of the GDPR's text.

Although privacy scholars have advocated for privacy models that embody a more comprehensive regulatory approach such as the GDPR (and, previously, the Directive), very few have considered how the concept of legitimate interest may be a necessary ingredient for a fairer, less consent-reliant privacy framework in the United States.[240] The EU's privacy developments illustrate not only an omnibus, or broadly applicable (sector-agnostic), framework for privacy, but also demonstrate an evolution from a focus on consent to a multi-dimensional privacy model, which acknowledges the rights and freedoms of data subjects from multiple perspectives. While consent may still be used heavily under the GDPR and within country laws, the viability of legitimate interest perhaps offers an approach the United States can use to better balance individual and commercial interests.

IV. LEARNING FROM THE EU MODEL

The EU model, in particular the GDPR, has been heralded as the most privacy-protecting law in the world.[241] The United States, however, has struggled to negotiate the prominence of commercial behavior and privacy interests, instead focusing sectorally on protecting the most sensitive of transactions.[242] The United States can balance interests structurally by focusing on the relative

---

[239] *Id.* at 36.

[240] *See generally* Tschider, *Regulating*, *supra* note 18 (describing the absence of legitimate interest discussions while relying primarily on consent as the vehicle for legitimacy of collection and use).

[241] *See* Paul Lechner, *GDPR: Three Ways the World Has Changed in the Privacy Law's First Two Years*, CPO MAG. (July 7, 2020), https://www.cpomagazine.com/data-protection/gdpr-three-ways-the-world-has-changed-in-the-privacy-laws-first-two-years/ [https://perma.cc/7E9S-8ACS].

[242] Daniel J. Solove, *The Growing Problems with the Sectoral Approach to Privacy Law*, PRIV. + SEC. BLOG (Nov. 13, 2015), https://teachprivacy.com/problems-sectoral-approach-privacy-law/ [https://perma.cc/D6WY-PRNT] (describing, as early as 2015, why the sectoral approach creates new problems due to gaps in protection under this approach).

interests of both consumer and organization, while simultaneously promoting transparency and without replicating an EU model that may not be readily accepted into American conceptions of privacy. Legitimate interest balancing, assessment, and sharing, offers an opportunity to place more of the onus on organizations while simultaneously relieving privacy fatigue and enabling more effective individual rights of self-protection.

A. Relational Constructs and Negotiation Between Private and Public Spheres

Philosophy provides some insight into how individuals negotiate their relationships with others to make decisions and why relational models, such as legitimate interest balancing, are more useful in understanding the concept of choice. Relationship dynamics help to interpret and evaluate legal approaches to privacy. Jürgen Habermas, a German philosopher in the critical theory and pragmatic traditions, wrote extensively on the relationship of individuals with outside parties, including the government and other individuals, in his evaluation of the "public sphere."[243] Habermas defines the public sphere, or the *Öffentlichkeit*, as a variety of different public spheres, including the *politische Öffentlichkeit* (political public sphere)*, literarische Öffentlichkeit* (literary public sphere, or commentary), and *representative Öffentlichkeit* (or the display of inherent power or dignity before an audience).[244] These definitions provide a more granular understanding of the Aristotelian *oikos* and *polis*.[245]

Habermas views the connected relationship between individuals and spheres as a change from a privately oriented lifestyle to one where "commodity exchange burst out of the confines of the household economy," introducing public activity into the private sphere.[246] Following this portrayal, privacy has similarly connected public activities, defined as any activities outside the private realm, to the private sphere, and vice-versa, a negotiation between spheres

---

[243] *See* HABERMAS, *supra* note 1, at 3.
[244] *Id.* at xv (Translator's Note).
[245] *Id.* at 3–4. *See* DECEW, *supra* note 1.
[246] *Id.* at 28, 141–42.

through commercial activity, usually negotiated via contractual activity.[247] Privacy, then, can be understood as relationship or overlap in private and public spheres, with these spheres negotiated between the individual and other participants.[248]

Habermas posited that the quality of an individual's interactions in the public sphere could increase or decrease self-determination, or the ability of an individual to make choices that do not involve damage to others.[249] These interactions, from a privacy perspective, presume personal information transfer as part of negotiating between private and public spheres.[250]

Unlike clear demarcations of "public" and "private" under the law, Habermas focused on relationships connecting the private individual with activity outside the purely personal and private realm. Negotiations between spheres necessarily included both action and communicative mechanisms oriented towards successful outcomes *or* reaching an understanding, with reaching an understanding being the more beneficial goal.[251] Mechanisms for reaching an understanding may also be considered a process of agreement, or *Einigung*.[252] Agreement cannot be achieved by "outside influence, it has to be accepted or presupposed as valid by

---

[247] *See supra*, Part II(C) and accompanying notes.

[248] While philosophically negotiation can be understood as the influence of participants on each other, and rhetoric describes it as communicative activity, the law has defined it through contextual relationships: contract, tort, and statutory duties and obligations. *See supra* Part I and accompanying notes.

[249] Fabio Macioce, *What Can We Do? A Philosophical Analysis of Individual Self-Determination*, 16 EIDOS 100 (2012), http://www.scielo.org.co/pdf/eidos/n16/n16a05.pdf [https://perma.cc/RD45-XLF3]. The concept of self-determination in its earliest conceptions involved freedom to make decisions free from state intervention. However, the concept of making decisions free from other types of intervention certainly applies as an important concept for interactions with non-state actors, such as corporations or other consumer-oriented entities.

[250] *See* THOMAS GUTMANN, THEORIES OF CONTRACT AND THE CONCEPT OF AUTONOMY 14 (2013), https://www.uni-muenster.de/imperia/md/content/kfg-normenbegruendung/intern/publikationen/gutmann/55_gutmann_-_contract_and_autonomy.pdf [https://perma.cc/U5ND-JW44] (describing contractual relationships and the need for inquiry into exploitive contractual relationships).

[251] *See* JÜRGEN HABERMAS, THE THEORY OF COMMUNICATIVE ACTION, VOL. 1 286-87 (Thomas McCarthy trans., 1984).

[252] *Id*. at 286.

participants."[253] Accordingly, action and communication together create understanding when non-coercive, and between individuals, action and communication evidence a continuing relationship rather than a transactional exchange.[254]

With understanding, an individual can exert autonomy, but coercive practices undermine consensus-forming communicative rationality, in that when contextual circumstances do not collectively promote individual choice overall, public and individual benefits cannot be realized.[255] Indeed, "coercion and deception infringe upon the voluntary character of an agent's actions."[256] So how must consent function to adequately operate as choice? First, consent must be non-coercive in how it is accomplished. Next, information provided must be comprehensive and informational enough to enable voluntary decision-making. Finally, there must be continuous opportunities to negotiate within this relational model so long as the relationship exists. As described in Part II, the current

---

[253] *Id.* at 287.

[254] Typically, in legal conceptions of agreement and, frequently, privacy mechanisms, the law often governs transactional relationships rather than continuous ones. For example, a privacy policy evidences a transactional exchange, albeit one which includes obligations that continuously must be honored. In contrast, fiduciary relationships and other trust relationships often include continuous expectations in addition to transactional exchanges. Although not explored at length here, continuing relationships rely on trust, which has recently been a subject of much consideration and scholarship. *See*, *e.g.*, Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap,* 126 YALE L. J. 1180, 1188–91 (2017) (positioning obfuscation as a lack of trust); Ari Waldman, *Privacy, Sharing, and Trust*, 67 CASE W.L. REV. 193, 206–07 (2016) [hereinafter Waldman, *Privacy, Sharing, and Trust*]; Rafi M. Goldberg, Giulia McHenry, Luis Zambrano Ramos & Celeste Chen, *Trust in Internet Privacy and Security and Online Activity* 3 (Nat'l Telecomm. & Info. Admin. Working Paper, 2016), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2757369 [https://perma.cc/5WGA-RMPC] (finding reduced trust results in less participation).

[255] Kirsten Wahlstrom & N. Ben Fairweather, *Privacy, the Theory of Communicative Action and Technology,* 2013 ETHICOMP CONF. PROCEEDINGS: THE POSSIBILITIES OF ETHICAL ICT 502, 504 (2013).

[256] *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 83 (2009) (describing the details of contextual models for privacy, including the context in which data subjects make decisions).

privacy notice and consent model used does not (and perhaps cannot) effectively meet these requirements.[257]

The shift from models of individual rights to relational models involving trust in U.S. privacy legal theory has certainly reinforced the need for consumers to continuously be able to make decisions representing their interests. As Neil Richards and Woodrow Hartzog have described, considering relational models of trust enables a shift from procedural mechanisms to ongoing commercial relationships.[258] Most challenging, though, is how privacy models, even relational ones, can appropriately reformulate ongoing commercial relationships when there are known and substantial issues with the notice and consent model used in relationship formation from the outset. In short: layering trust on a broken model cannot "cure" existing consent problems or result in a trustworthy relational model. Considering a new model to replace or supplement notice and consent could build a foundation worthy of trust-based and fiduciary relationships.[259]

B. The Consent Myth and Pathologies of Consent

A focus on consent as choice mistakes the idea that choice is a transaction, a one-time exchange, rather than an ongoing relational model. Here, choice represents a singular moment, similar to agreement in contract formation, when in reality, choice could be fulfilled by a variety of other means, distributed in time and performed by any number of parties involved in the relationship, from primary to third parties and organizations brokering these relationships.[260] Preference management, consent revocation and

---

[257] *See supra*, Part II and accompanying notes.

[258] Richards & Hartzog, *supra* note 25, at 452 (identifying the role of trust in information processing and associated duties of loyalty).

[259] *See* Balkin, *supra* note 43, at 13–14 (positioning a fiduciary model for privacy, due to the inherent asymmetry of bargaining power and access to relevant information).

[260] Several scholars have explored the dynamics of trust and relationships in privacy law. *See generally* Ari Ezra Waldman, *Privacy as Trust: Sharing Personal Information in a Networked World*, 69 U. MIA. L. REV. 559 (2015) (recontextualizing privacy law as enabling disclosure in social settings rather than individual rights); ARI EZRA WALDMAN, PRIVACY AS TRUST (2018) (examining

processing restrictions, enhanced security through privacy-enhancing technologies, reduced identifiability of data sets, and contextual user privacy controls and settings perform a complementary role to amplify choice with respect to a consumer's data and ongoing choices that may be made.[261]

The synonymous use of the word "consent" as "choice" has pervaded new efforts to reconsider privacy models.[262] Implicit in this concept of consent is a temporal linkage, based on the belief that: (1) notice should occur prior to both soliciting consent and collecting or using data, and (2) the temporal nexus of notice and consent to data use (i.e., the closer in time to the transaction in question), the more informed an individual can be.[263]

When a relationship is formed through a privacy notice and consent, it is questionable whether the relationship is based on trust. As Neil Richards and Woodrow Hartzog have noted, consent is most likely to be problematic when it is unwitting,[264] coerced,[265] or incapacitated.[266] Correspondingly, consent is most likely to be effective when it is infrequent,[267] describes risk vividly,[268] and gives incentives to take each request seriously.[269]

This Author has similarly observed the challenges with consent as a procedural mechanism, identifying five key problems, or myths, surrounding consent as a preferred proxy for choice.[270] First, privacy policies, as contracts of adhesion that do not permit active

---

the dynamics of trust in privacy law); Richards & Hartzog, *supra* note 254 (advocating for relational models embodying trust, including foundational commitments regarding trust in information processing).

[261] *See* Tschider, *The Consent Myth*, *supra* note 20, at 1534–35.

[262] *Id.* at 1506, 1516.

[263] *Id. See* Wahlstrom & Fairweather, *supra* note 255. The Author sees this change as a responsiveness to Helen Nissenbaum's considerable writing on the concept of context and how it shapes our understanding of data collection and use. *See* NISSENBAUM, *supra* note 256.

[264] Richards & Hartzog, *supra* note 20.

[265] *Id.* at 1486.

[266] *Id.* at 1490.

[267] *Id.* at 1492.

[268] *Id.* at 1494.

[269] *Id.* at 1496.

[270] *See* Tschider, *The Consent Myth*, *supra* note 20, at 1519.

bargaining and permit organizations to establish terms from a more powerful position, leave individuals with little choice and often few alternatives.[271] Although one might assume that consumers read the privacy policy, often a consumer does not have the time to read all privacy policies all the time, which is a structural limitation.[272]

When consumers do read the privacy policy, they often cannot understand what it means in a practical sense because it is tremendously difficult to describe privacy risk saliently, vividly, and materially, problems Ryan Calo, Neil Richards and Woodrow Hartzog, and this Author have advocated to solve.[273] Unlike salient descriptions of, for example, prescription side effects or risks of participating in clinical trial, describing the risk of data misuse or data breach and encapsulating the myriad of potential harms using explanations that are accurate, complete, and written to an appropriate reading level is tremendously difficult, if not impossible.[274] For this reason, relying completely on disclosures, and, following, as Daniel Solove dubs "privacy self-management," is not likely to promote individual autonomy.[275] However, it may increase how much organizations understand about their own practices, practices that are exogenous to most consumer transactions at the point of relationship formation.

Perhaps the most undertheorized and crucial consent problem is the exogeneity problem, or the inherently hidden and unimaginable nature of how information is used and flows downstream—what Daniel Solove deems from the consumer's perspective "assessing harms,"[276] and what Danielle Keats Citron and Daniel Solove position as harms that might demonstrate actual injury. Information

---

[271] *Id*. at 1519.

[272] *Id.* at 1521.

[273] Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027 (2012) (describing the need for visceral description or engagement related to notice, whether in a formal privacy notice or other notification vehicles). *See* Richards & Hartzog *supra*, note 263, at 1463; Tschider, *The Consent Myth*, *supra*, note 20, at 1530 (advocating for clear terms and obvious bargain related to secondary uses for personal information).

[274] *See* Tschider, *The Consent Myth*, *supra* note 20, at 1522–23.

[275] *See generally* Solove, *supra* note 20, at 1882 (describing the tension between self-management, which is largely ineffective, and paternalistic positive law).

[276] *Id.* at 1891.

about how information is used and flows through systems and to third parties and third countries is exogeneous because it is not readily available or understandable from the perspective of a consumer.

Inherent in this concept is that organizations are making decisions on behalf of individuals without their knowledge, resulting in unforeseeable risks unimaginable from the relational context in which a consumer makes decisions. Information regarding, for example, system infrastructure, detailed third-party affiliates and relationships, data flows across systems, and security approaches are usually considered confidential if not trade secrets, and therefore are not available to consumers. Furthermore, decisions about systems and practices are discretionary—they are fully under the control of an organization and involve cost/benefit analyses and other strategic organizational decision-making.

Ultimately, these decisions may increase or decrease risk to a consumer. Examples of such decisions include which third parties to engage, where to geographically store data, whether systems need certain upgrades, which security practices to use or not use, and who will ultimately handle personal consumer information, or a security framework.[277] Even if this information could be shared with consumers, organizations would encounter challenges succinctly, completely, and vividly communicating this information to consumers.[278] New technologies only intensify these issues as they use data continuously and in new and different ways from the purpose under which data were originally collected.[279]

---

[277] *See* BAMBAUER ET AL., *supra* note 147, at 494 (describing the NIST Cybersecurity Framework as one option for implementing a security model and making security decisions).

[278] *See* Tschider, *The Consent Myth*, *supra* note 20, at 1524. Explaining more details would extend the length of privacy notices exponentially, and the complexity of such practices may be tremendously difficult to understand. Indeed, organizations often negotiate and manage these decisions through their own contracts and negotiations with vendors, partners, and providers, and frequently organizational representative themselves do not always understand these practices. *Id.*

[279] *Id.* at 1526.

It is this exogeneity problem, combined with the other existing consent problems that ultimately makes it tremendously difficult for consent to mean something in the relational context. Rather than reinforcing trust, consent erodes it, masquerading as something that has meaning while being entirely devoid of the salient information and vulnerabilities which enable trust relationships.[280] So how might this consent problem be solved?

Practices that are necessary to provide a primary good or service may not actually need consent, as, by definition, the good or service will not be functional without providing personal information and using the infrastructure provided. For personal information collection, use, and retention strictly necessary to provide a service, usually the risk to an individual is comparatively less, because the potential risks are less attenuated. Therefore, organizations can make information available about their practices, as in a highly salient and layered privacy notice, for example, while also ensuring such practices are foreseeable and necessary with respect to the good or service to be provided. Although this scenario does not alleviate other privacy activities necessary to responsible data handling, such as security risk assessments on infrastructure and for third party systems that are part of management-level risk decision-making, it dramatically curtails abusive data collection and use.

Where more questions remain, however, is when data may be used for purposes beyond the immediate scope of providing a good or service, or secondary uses including sales or transmission to third parties, such as partners or affiliates; product improvement or new development; marketing or other analytics; and data aggregation and matching with purchased or public data sets. From the perspective of a consumer, these types of data uses and collection for these purposes are not usually directly beneficial.[281] Further, these uses have the potential to be highly coercive and more exogenous to the

---

[280] *See* Waldman, *supra* note 260, at 83–84.

[281] *Privacy Today: A Review of Current Issues,* PRIVACY RIGHTS CLEARINGHOUSE (Mar. 1, 2001), https://privacyrights.org/resources/privacy-today-review-current-issues [https://perma.cc/9R7L-RFTU] (showing how issues that were a problem 20 years ago are still prevalent at the time of this Article's writing).

relationship simply because they are not obvious with respect to the commercial exchange.[282]

Part of the challenge in shoe-horning consent into modern data collection, retention, use, transfer, and sharing models is that these models may or may not be effective, depending on the nature of data collection and use.[283] For example, perhaps consent is not necessary when data collected and used are specifically for the service or good being provided and only used for providing service to that individual.[284] This makes intuitive sense: although a privacy notice must be available, personal information collection and use should not be a surprise to a consumer when it is consistent with the service or goods provided. In that case, the need for consent is largely extraneous to the model. However, when data are collected and used in a manner inconsistent with provisioning basic goods and services, perhaps more is needed.[285]

Furthermore, completely offloading responsibility to lawmakers and positioning an organization as receiver of instruction does not necessarily create internal organizational models where consumer fairness is inherent in the calculus and decision-making of data management or where trust is a primary consideration.[286] Rather, facilitating fairness models within organizations should promote better behaviors while also promoting innovative solutions that balance data use with individual interests.

---

[282] *See* Tschider, *The Consent Myth*, *supra* note 20, at 1528–29.

[283] *Id.*

[284] *Id.*

[285] This Author has previously advocated for greater transparency and salience in bargaining for secondary data use. However, to meet the requirements necessary may be impossible under some circumstances, such as when the entity that has collected data no longer has the contact information of an individual person.

[286] It should be noted that the principle of information fiduciary is becoming increasingly more popular by formalizing the obligations organizations owe individuals from whom they collect personal information. This Article does not address this issue specifically but rather seeks to advance discussions around alternatives to consent which may become part of alternative models like an information fiduciary relational model. *See* WALDMAN, *supra* note 260, at 85–87.

C. Role of the State in Privacy Protection

If individuals acting in their own interests because of the inherent issues with consent cannot be relied on, what options are available? Restricting secondary use with positive law may not be the best answer for these high-context scenarios where exogeneity is a primary concern. Philosophers like Jürgen Habermas and legal scholars such as Daniel Solove have criticized the modern "welfare state," which results in "overprotection of interests."[287] In privacy law, this overprotection of interests, or privacy paternalism, reduces the potential of an individual and collective self-determination.[288] Technocracy emerges when individuals cannot influence policy in line with their own interests.[289] The net result of technocracy is a regime that creates predictability, yet reduces autonomy.[290] Superimposing strong mandates often provides predictability while reducing benefits to all players in the system, including consumers, who might benefit from low-cost services or enjoy the proceeds of larger public benefits.[291]

The result of overprotection and privacy paternalism, then, is that individuals do not have the opportunity to collectively self-determine, losing autonomy over decision-making. And concurrently, paternalistic models do not anticipate an individuals' choices in the event they actually knew of the potential benefits.[292] Instead, these models make assumptions about individuals collectively, which may or may not be accurate to the group or the individual, which results in individuals losing autonomy without much gain. Habermas would instead advocate that the "task of the state is . . . to encourage a rational debate on conflicting issues," or the opportunity for individuals to advocate for their own

---

[287] ERIK O. ERIKSEN & JARLE WEIGÅRD, UNDERSTANDING HABERMAS: COMMUNICATIVE ACTION AND DELIBERATIVE DEMOCRACY 154 (2003).

[288] *Id. See also* Solove *supra* note 274, at 1894.

[289] *See* ERIKSEN & WEIGÅRD, *supra* note 287, at 154.

[290] *Id.*

[291] Solove *supra* note 20, at 1882.

[292] *See* ERIKSEN & WEIGÅRD, *supra* note 287, at 154.

preferences.[293] This often takes the form of strategic bargaining, where strategically operating agents find compromise.[294]

Habermas fully accepted that the result of the bargain may be the same (e.g., agents may receive very similar outcomes), but the process for achieving that outcome could differ.[295] Practically speaking, two different individuals could consent to a particular privacy disclosure under different circumstances. One person receives very little information and ultimately consents to receive the service. Another person is provided enough information to think through the scenarios and decides to consent, as well. Although the result is the same, the individuals have vastly different experiences and the latter may have a more positive relationship with, and even more trust in, the organization over time. For Habermas, public and private relationships models, which include multiple discursive opportunities (not just one) should improve or reinforce individual autonomy.[296] Ultimately, this means that although some circumstances may require one-sided decision-making for fairness, individuals should have the ability to intervene or intercede in data processing activities.[297]

If the government mandates requirements, instead of advancing individual autonomy or at least balancing what consumers can decide and what organizations can do, this introduces other problems. Consumers will lose individual decision-making and gain

---

[293] *Id.* at 155.

[294] *Id.* at 226.

[295] *Id.* For example, one individual could accept all of the terms as initially presented in a privacy policy and consent to them, including secondary uses. Another individual could, given the chance, seek to review the various uses in more detail and consider each use separately. By offering certain inducements, such as extra services or perks (e.g., a ten percent off coupon), an individual might agree to roughly the same terms as the other individual, despite different bargaining processes. The net benefit is choice: individuals could effectively pursue their own interests.

[296] *Id.* at 154.

[297] This seems to suggest that perhaps data collection and use could use a mechanism other than consent, but that process would need to enhance fairness while simultaneously promoting individual and responsive decision-making, as in data subject rights and other user-interface-based controls. *See* Tschider, *The Consent Myth*, *supra* note 20, at 1534.

predictability, which may reduce available options, while an organization loses market flexibility and freedom to bargain. An effective model, even one involving personal information, will advance autonomy interests by promoting transparency in data processing, establish predictability to reduce confusion on the part of organizations and consumers, while simultaneously leaving organizations some flexibility in their business models and operations. This type of model is consistent with the history of consent as a relational model, and often a commercial one.

D. Pursuing Legitimate Interests as Part of a Multi-Dimensional Privacy System

The beauty of the EU data protection system is not necessarily in its focus on civil rights, but on the multi-dimensionality of data protection. There are relational roles between controllers and their processors, controllers and data subjects, even controllers and controllers (sometimes co-controllers, sometimes joint controllers).[298] The EU system embraces the relational model while also acknowledging that different relationships and different contexts may demand differing data protection safeguards to protect the individual rights and freedoms of EU residents.[299] For example, notice and consent is not the only commitment under the GDPR; the GDPR also requires individual consultation with potential data subjects about data processing activities.[300] Furthermore, amongst many other obligation, organizations must maintain a register of their activities, conduct risk assessments on their practices, employ appropriate security controls, and ensure that data subject rights requests are honored and fulfilled within a specific time period.[301]

---

[298] *See* TSCHIDER, *supra* note 26, at 35–37.

[299] *Id*. at 42. The clearest example of options under the GDPR are in lawful basis for data processing. Further, the GDPR permits risk-based determinations regarding security. Reg (EU) 2016/679 Recital 66, Art. 32(1), 2016 O.J. (L 119). Notably, the GDPR contemplates differing contextual scenarios, as in Reg (EU) 2016/679 Art. 6(4), calling for "necessary and proportionate" evaluation.

[300] Reg (EU) 2016/679 Recital 111, Art. 25(9), 2016 O.J. (L 119).

[301] *Id.* Recitals 65, 68, 71, Art. 40, Art. 5, Art. 13, Art. 7, Art. 20, Art. 21, Art. 17, 2016 O.J. (L 119).

Woodrow Hartzog has promoted dynamic privacy practices from a U.S. perspective, advocating for better privacy design appropriate to specific technologies, acknowledging the differing user interfaces (if they exist) and context users might experience.[302] Dr. Ann Cavoukian, Information & Privacy Commissioner for Canada's Ontario Province, created the Privacy by Design approach in the 1990s, acknowledging that building privacy into products and systems enabled better, more proactive privacy management that honored the experiences of actual individuals.[303] Privacy by Design is now encouraged formally as part of the GDPR, and organizations across the world have begun building privacy considerations into their products.[304]

An important question is whether consent is still useful in more contextual, contemplative models, or whether heavily relying on notice and consent promotes a false sense of trust and ultimately does more harm than good, like putting a glossy coat on a car that does not start.[305] The EU offers a useful model for alternatives to consent, which may advance conversations related to contextual privacy decision-making in-line with product-based design and complex technology implementations.[306] Specifically, the Article 29 Working Party recognized that certain requirements could be offset or bolstered with other more rigorous privacy protections. For example, extensive use of anonymization techniques, increased transparency, and more accessible opt-out models could offset more indirect lawful bases, such as relying on legitimate interest analysis rather than explicit consent.[307] Although it is important to recognize that consent is still an important part of EU data protection law, even

---

[302] *See generally* WOODROW HARTZOG, PRIVACY'S BLUEPRINT THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES (2018) (describing the need for privacy to be built into products rather than regulated as separate activities).

[303] INFORMATION & PRIVACY COMMISSIONER OF ONTARIO, *Privacy by Design* (Sept. 2013), https://www.ipc.on.ca/wp-content/uploads/2013/09/pbd-primer.pdf [https://perma.cc/P37N-EA52].

[304] Reg (EU) 2016/679 Recital 111, Art. 25, 2016 O.J. (L 119).

[305] A false trust may actually be more damaging than no trust at all. When the foundation of the model is broken, relational models are also broken.

[306] *See* Tschider, *Regulating*, *supra* note 18.

[307] *See* Opinion of the Working Party, *supra* note 222, at 41–42; Reg (EU) 2016/679 Art. 6(4), 2016 O.J. (L 119).

though some limits on consent render it slightly better than the U.S. model, consent is not designed to be effective in every context.[308]

E. How the EU's Lawful Bases Can Influence U.S. Conceptions of Consent and Advance Privacy

The Article 29 Working Party's 2014 Legitimate Interest opinion offers a model that could be included in privacy laws, or at the very least recognized as an alternative to consent under the FTC's FIPPs. If combined with consultation from representative consumers, legitimate interest balancing could require organizations to analyze scenarios from the perspective of a consumer, blending legitimate interest with some contextual input. This is properly employed when an organization desires personal information collection and use for secondary uses that may pose some risk of harm to the consumer.

The Working Party's document offers an outline for assessing interests that would be useful for an organization's documented risk analysis,[309] not markedly different from privacy and security assessments many organizations already complete. This model has been supplemented and summarized for purposes of rendering a trust-based, relational legitimate interest model:

1. Assessment of Impact: Determine the positive and negative consequences of processing on an individual person or class of people. Assessment includes impacts from third parties on decisions that may affect the individual; probability of discrimination, defamation, or social harms; or when reputation, negotiating power, or autonomy may be damaged. Such assessment should take into account cumulative impacts of these consequences holistically.[310] Likelihood of risk materializing, and severity of the

---

[308] *See supra,* Part II and accompanying notes. One key difference is consent in the EU usually has additional requirements, such as explicitness, unambiguousness, and especially non-coerciveness. Consent must be freely given, which means additional data processing beyond the primary purposes for which data are collected must be separately consented.

[309] *See* Opinion of the Working Party, *supra* note 233, at 37–41.

[310] *See id.* at 37.

consequences (Impact) are key to determining impact in this assessment.[311]

2. Nature of the Data: Determine what inherent risk certain data types have and, for example, what level of identifiability data sets provide, especially in big data forms or for databases feeding artificial intelligence systems. Biometrics, for example, might pose more risk due to their indelibility. Location data might pose more risk due to the connection with physical safety.
3. The Way Data Are Planned to Be Processed: Determine what the planned processing will look like, specifically the number and character of potential recipients, the need for reuse and access to data by a larger number of people who are disconnected from the original processing purposes. Consider, as well, security practices which may offer additional protections from unauthorized disclosure.
4. Reasonable Expectations of the Consumer: Consider expected behavior on the part of the organization from the perspective of the individual or consumer. Determine the range of behaviors that would have been relationally consistent with information previously disclosed (including the context of data collection), the nature of the relationship, and the need to enhance trust within the relationship. Engage with representative consumers to weigh-in on the value of such benefits to the individual, group, or community in a focus group or similar.
5. Status of the Organization and the Individual or Consumer: Observe potential relational differences in bargaining power and forced trust. Consider whether an individual's positional power might coerce individuals to make decisions they otherwise would not make. Relational differences should also be analyzed for specific groups, communities, and age groups where bargaining power might be even more diminished or the likelihood of coercion is high, such as

[311] *Id*. at 38.

provisioning healthcare or qualifying for entitlement programs.

6. Publish Results of Legitimate Interest Analysis: To reinforce transparency, organizations must be required to publish this analysis when they rely on it for secondary data processing, in addition to privacy notices already required under state laws. The analysis need not disclose confidential details but offer enough information to demonstrate, to consumers and regulators, that benefits to consumers outweigh benefits to the organizations. Such an analysis must be repeated when material terms regarding data collection and use change, as is required for posting privacy policies.

The question, though, is how a legitimate interest model like this could be implemented. First, legitimate interest could be voluntarily employed by ethically minded organizations as a limiting factor for further data processing, as in secondary use. With this model, organizations would rely on consent, but would validate their use after the fact. Of course, this model lacks the teeth often needed to change behavior, though organizations wishing to promote themselves as ethically minded could use this model to demonstrate it.

Second, legitimate interest could be positioned as a replacement for consent related to secondary uses, or required in addition to consent under the FIPPs, or used as a framework for the FTC's UDAP enforcement. Legitimate interest could formally be included in administrative laws like HIPAA either by enforcement discretion when there is no private right of action, or in new rewrites of privacy laws at the state and federal level. A legitimate interest analysis is an easy additional requirement consistent with privacy policy disclosure requirements currently required under many privacy laws. In fact, such an analysis could easily be included in a privacy policy if need be.

Finally, courts could use legitimate interest analysis as a factor-based inquiry for common-law privacy actions to assist in determining the likelihood of privacy harms at the time data were collected and used, as well as countervailing benefits anticipated. For breach of contract actions, for example, a lack of legitimate

interest analysis could be persuasive for courts finding unconscionability in the contracting process. In the event courts recognize alternative forms of injury or when states draft new privacy statutes, like the California Consumer Privacy Act, they will need a model for determining whether an organization performed appropriately with respect to individuals. Without a contextual and relational model for evaluation, ethical organizations may experience unfavorable results, while unethical organizations emerge unscathed. A legitimate interest balancing exercise may provide useful information for determining which organizations are indeed blameworthy. In the event an information fiduciary model becomes commonplace, legitimate interest analysis could also provide a true risk-based analysis that takes into account the relationship, justified expectations, and potential privacy harms.

V. CONCLUSION

This Article only scratches the surface of how legitimate interest analysis could be adopted within the United States. Indeed, the EU still has not developed a detailed model for practically completing this analysis, which illustrates its complexity. In line with recent scholarly discussions of relational privacy, privacy by design, trust, and fiduciary relationships, however, the United States should consider more effective models for negotiating relational and contractual relationships. By assessing actual risks to individuals, organizations have the ability to forge effective, trustworthy, and long-term relationships while simultaneously gaining more flexibility in data collection without the challenges and ineffectiveness of consent. The new world is a world with both data and privacy.