Hero or Villain: The Data Controller in Privacy Law and Technologies

CLAUDIA DIAZ,* OMER TENE† & SEDA GÜRSES‡

TABLE OF CONTENTS

I. INTRODUCTION 923
II. THE AMBIGUOUS CONCEPT OF "TRUST" IN PRIVACY FRAMEWORKS 926
III. SURVEILLANCE DEFINED 934
IV. PETS DEFINED 939
V. PETS CLASSIFIED 944
A. *Category I: PETs Implemented by Data Controller* 944
1. *Privacy-Preserving Pay-as-You-Drive Tolling* 944
2. *Privacy-Preserving Smart Metering* 946
3. *Other Applications* 948
B. *Category II: Client-Side Software Deployed by a User While Using a Service Offered by a Data Controller* 950
C. *Category III: Collaborative Applications Without a Data Controller* 953
D. *Policy Implications* 959
VI. CONCLUSION 963

I. INTRODUCTION

Constitutional privacy law in Europe and the United States establishes the right to privacy as freedom from government surveillance.[1] It is based on

* Assistant Professor at the KU Leuven Department of Electrical Engineering, COSIC (Computer Security and Industrial Cryptography), Belgium.

† Vice Dean of the College of Management Haim Striks School of Law, Israel; Affiliate Scholar at the Stanford Center for Internet and Society; Senior Fellow at the Future of Privacy Forum. I would like to thank the College of Management Haim Striks School of Law research fund and the College of Management Academic Studies research grant.

‡ Postdoctoral Research Fellow at Media Culture and Communications and Information Law Institute at NYU.

The authors would like to thank Caspar Bowden, Ian Brown, Joris van Hoboken, and Susan Landau for helpful comments and critique.

[1] A note about terminology: We refer to privacy protections under the Fourth Amendment to the U.S. Constitution as well as the European Convention of Human Rights as "constitutional privacy." Another term, more commonly used in Europe, for these laws is "fundamental rights" protection. The defining characteristic of "constitutional privacy" is protection from unlawful or disproportionate government surveillance. Protection of privacy, much like any fundamental right, is not absolute; it is balanced against other fundamental rights (e.g., freedom of speech) and important public interests (e.g., national security and law enforcement and freedom of information). Information privacy, which we contrast with

suspicion of power and distrust in the state, which can unleash ominous intrusions into the private sphere to crush dissent and stifle democratic discourse and free speech. Over the past forty years, an additional legal framework has emerged to protect information privacy. Yet unlike the constitutional framework, information privacy law provides little protection against the risk of surveillance by either governments or private sector entities. Indeed, such organizations are assumed to be trusted entities acting as stewards of individuals' rights, essentially "information fiduciaries."[2]

This Article demonstrates that an analysis of the assumptions and principles underlining privacy enhancing technologies (PETs) highlights the gap between the constitutional and information privacy frameworks. It argues that by embracing PETs, information privacy law can recalibrate to better protect individuals from surveillance and unwanted intrusions into their private lives.

Conversely, if the law continues on its current trajectory, emphasizing organizational accountability and marginalizing data minimization and transparency, PETs would become unviable and individuals would become subject to increasingly stifling digital oversight. The recent revelations about the scope and depth of mass surveillance employed by the NSA and partner intelligence agencies have painted a grim picture concerning the state of privacy in the digital world.

The term "PETs" has been used loosely to describe a broad range of privacy technologies. In this Article, it is restricted to technologies specifically aimed at enabling individuals to engage in online activities *free from surveillance and interference*. PETs allow individuals to determine what information they disclose and to whom, so that *only* information they *explicitly* share is available to *intended* recipients. They are based on three common principles: eliminating the *single point of failure* inherent in a single trusted data controller, *minimizing data collection*, and subjecting system protocols to community based *public scrutiny*.

This Article shows that while PETs are aligned with the objectives of the constitutional framework, they are not always in tune with the assumptions, principles, and goals of the information privacy framework. Over the past two decades, the information privacy framework has shifted to imposing information stewardship ("accountability") obligations on data controllers, who act as custodians of personal data. The notion of the data controller as a *trusted party* is ill at ease with the anti-surveillance gist of constitutional privacy and

---

constitutional privacy, also has strong constitutional (or fundamental right) properties. In Europe, it is protected under the Charter of Fundamental Rights of the European Union and various national constitutions. Charter of Fundamental Rights of the European Union, art. 8, 2000 O.J. (C 364) 10. Yet, as discussed below, it harbors assumptions that are incongruent with—and indeed may be diametrically opposed to—those of the constitutional privacy framework.

[2] Ian Brown points out that this may be an overstatement as far as the European information privacy framework is concerned. The Article addresses this tension, *infra* notes 23–24 and accompanying text.

PETs. In fact, the technological community researching PETs departs from a diametrically opposed perception of a data controller as an *adversary*. Under this approach, information disclosed to a data controller is compromised and can no longer be viewed as private. Proponents of this view point out that after disclosure, it is almost impossible to control how personal information is used, concluding that PETs should limit information disclosure.

This Article asserts that policymakers should recognize and expand by appropriate regulatory measures the role of technologies that enable individuals to enforce their right to privacy as freedom from surveillance. Given that the legal framework is focused on the roles and obligations of data controllers, this Article categorizes PETs depending on the degree of data controller involvement.

The first category consists of PETs that require active implementation by a data controller. This includes PETs, such as private information retrieval or zero-knowledge protocols, which enable a data controller to provide a service that takes as input private user information without the controller becoming privy to such information. Yet if the controller does not invest in a privacy enhancing architecture that integrates these protocols, individuals cannot by themselves benefit from the privacy protections afforded by them. The second category comprises client-side software deployed by a user while using a service offered by a data controller. These include encryption tools that maintain the confidentiality of the contents of emails or social networking posts, including *vis-à-vis* the data controller, and proxies that enable users to anonymously access an online service. Here, controller implementation is not required; yet data controllers offering an online service can (and actually do) try to limit deployment of PETs within their service. The third category consists of PETs, which are collaborative applications where users act as the service providers, that is, without the involvement of an actual data controller in the provision of the service. For example, the Tor network relies on a decentralized architecture run by volunteers to enable users to communicate anonymously. We note, however, that collaborative applications rely on the Internet infrastructure for their communications. Thus, Internet Service Providers (ISPs) have the ability to prevent users from accessing and participating in these services. The recent NSA revelations have shown that powerful national security agencies, including the NSA and British GCHQ, have invested significant effort in trying to undermine Tor.[3] This comes in addition to reports of governments in various countries trying to block the use of Tor.[4]

---

[3] James Ball, Bruce Schneier & Glenn Greenwald, *NSA and GCHQ Target Tor Network That Protects Anonymity of Web Users*, GUARDIAN, Oct. 4, 2013, http://www.theguardian.com/world/2013/oct/04/nsa-gchq-attack-tor-network-encryption.

[4] *See, e.g.*, Mike Masnick, *Police in Japan Are Asking ISPs To Start Blocking Tor*, TECH DIRT (Apr. 19, 2013, 5:04 AM), http://www.techdirt.com/articles/20130418/17210122754/police-japan-want-isps-to-block-tor.shtml; *see also Censorship Wiki*, TOR, https://trac.torproject.org/projects/tor/wiki/doc/OONI/censorshipwiki (last visited Oct. 9,

After classifying the PETs and examining their trust assumptions, design principles, objectives, and strategies, this Article assesses the policy considerations involved in reforming the legal framework to tolerate, facilitate, or indeed mandate their use. This Article concludes by arguing that the current information privacy framework fails to adequately address surveillance concerns. Embracing PETs would signal a marked departure from government efforts to disrupt and prevent their widespread deployment.[5] Such an approach would recalibrate public policy to focus on core concerns that underlie the genesis of information privacy law on the ruins of totalitarian regimes in twentieth-century Europe.

II. THE AMBIGUOUS CONCEPT OF "TRUST" IN PRIVACY FRAMEWORKS

The recent revelations over the massive scope of data collection, analysis, and use by the NSA and similar national security organizations[6] have crystallized privacy advocates' concerns of "sleepwalking into a surveillance society."[7] Over the course of the twentieth century, Europe has been torn by wave after wave of totalitarian regimes terrorizing their populations with elaborate infrastructures of mass surveillance.[8] Much like the prisoners in Jeremy Bentham's *Panopticon*,[9] citizens of a surveillance society inhibit their speech, behavior, political participation, religious beliefs, social interactions, and life aspirations, in the face of what Michel Foucault called the police state's "disciplinary gaze."[10] The human rights abuses of the Gestapo in Germany, KGB in the USSR, and the Stasi in East Germany are a testament to the ominous risks of excessive intelligence agencies' powers turned against their

---

2013) (documenting attempts to censor access to the Tor network in China, Iran, Kazakhstan and Syria).

[5] *See* Nicole Perlroth, Jeff Larson & Scott Shane, *N.S.A. Able To Foil Basic Safeguards of Privacy on Web*, N.Y. TIMES, Sept. 5, 2013, http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html.

[6] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN, June 5, 2013, http://www.guardian.co.uk/world/2013/jun/06/nsa-phone-records-verizon-court-order; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN, June 6, 2013, http://www.guardian.co.uk/world/2013/jun/06/us-tech-giants-nsa-data.

[7] Press Release, Info. Comm'r Office, Waking Up to a Surveillance Society (Nov. 2, 2006), *available at* http://www.ico.org.uk/upload/documents/pressreleases/2006/waking_up_to_a_surveillance_society.pdf.

[8] *See* Edward J. Eberle, *The Right to Information Self Determination*, 2001 UTAH L. REV. 965, 975–76; Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1934 (2013).

[9] Jeremy Bentham, *Panopticon; or, the Inspection-House*, *in* JEREMY BENTHAM, THE PANOPTICON WRITINGS 29, 35–37 (Miran Božovič ed., 1995).

[10] MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON 174 (Alan Sheridan trans., 1977). *See generally* Yofi Tirosh & Michael Birnhack, *Naked in Front of the Machine: Does Airport Scanning Violate Privacy?*, 74 OHIO ST. L.J. 1263 (2013).

own citizenry and portraying dissent as "terrorism" or "mutiny."[11] Moreover, as individuals' daily lives have increasingly become mediated by mass-market technologies, the government apparatus has joined private sector entities to create a "surveillant assemblage."[12] The specter of a government–business handshake, long recognized in academic scholarship, has become salient with the striking revelations about the collaboration of telecom and online providers with intelligence agencies in the PRISM and telecom metadata cases,[13] as well as the introduction by vendors—at the behest of the NSA—of backdoors and security vulnerabilities into their software and hardware products.[14]

The law has historically responded to the risks of government surveillance with constitutional protections for the right to privacy. For the past sixty years in Europe, privacy was considered a fundamental human right. Article 8 of the European Convention of Human Rights (ECHR) limits the power of the state to interfere in citizens' privacy, "except such as is in accordance with the law and is necessary in a democratic society."[15] Constitutional privacy protection is also grounded in the Fourth Amendment to the United States Constitution, which provides for "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[16] Hence, both the ECHR and the U.S. Constitution establish the right to privacy at a high level of abstraction as *freedom from undue government surveillance*. For differing historical and cultural reasons—the harsh lessons of tyranny in Europe and the endemic suspicion of government in the United States[17]—the constitutional frameworks on both sides of the Atlantic view centralized power with distrust and require effective checks, balances, and safeguards.

Protections from surveillance risks have arisen not only in law but also in technology. New tools and systems have been developed to ensure that

---

[11] *See, e.g.*, PHILIPP FREIHERR VON BOESELAGER WITH FLORENCE & JÉRÔME FEHRENBACH, VALKYRIE: THE STORY OF THE PLOT TO KILL HITLER, BY ITS LAST MEMBER 163–73 (Steven Rendall trans., 2009).

[12] Kevin D. Haggerty & Richard V. Ericson, *The Surveillant Assemblage*, 51 BRIT. J. SOCIOLOGY 605, 608–09 (2000) (building on concepts developed in GILLES DELEUZE & FÉLIX GUATTARI, A THOUSAND PLATEAUS 385–87 (Brian Massumi trans., 1987)). *See generally* Gus Hosein & Caroline Wilson Palow, *Modern Safeguards for Modern Surveillance: An Analysis of Innovations in Communications Surveillance Techniques*, 74 OHIO ST. L.J. 1071 (2013).

[13] *See* Waking Up to a Surveillance Society, *supra* note 7.

[14] *But see* Glenn Greenwald et al., *Microsoft Handed the NSA Access to Encrypted Messages*, GUARDIAN, July 11, 2013, http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data.

[15] Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, E.T.S. No. 5. This formulation was repeated fifty years later in Article 7 of the European Union's Charter on Fundamental Rights. Charter of Fundamental Rights of the European Union, *supra* note 1, art. 7. The Charter came into force under the Treaty of Lisbon. Treaty of Lisbon art. 6, Dec. 17, 2007, 2007 O.J. (C 306) 13.

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

[17] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1189, 1211 (2004).

individuals can create an autonomous sphere free of surveillance. These mechanisms are known in the engineering community as PETs.[18] While the term PETs has been used loosely to describe a broad range of privacy technologies,[19] this Article uses it to mean *technologies specifically aimed to protect individuals' communications and personal information from surveillance and interference*. PETs allow individuals to determine what information they disclose and to whom, so that *only* information they *explicitly* share is available to *intended* recipients.

Over the past forty years, a specific regulatory framework has emerged to protect *information privacy*.[20] Unlike the constitutional framework, which remains at a high level of abstraction and has roots going back more than two

---

[18] Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, *in* TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 125, 125 (Philip E. Agre & Marc Rotenberg eds., 1997).

[19] *See, e.g.*, Ira S. Rubinstein, *Regulating Privacy by Design*, 26 BERKELEY TECH. L.J. 1409, 1420–21 (2011) (categorizing ad-preference, cookie managers, advertising icons, and "do not track" tools as PETs).

[20] The first version of the fair information practice principles appeared in the United States, in a 1973 report sponsored by the Department of Health, Education and Welfare (HEW). DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS xxiii–xxxv (1973). The main building blocks of the current framework consist of the Org. for Econ. Co-operation & Dev. [OECD], *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data*, C(80)58/FINAL (Sept. 23, 1980) [hereinafter *OECD Guidelines*], *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm; Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data art. 1, Jan. 28, 1981, E.T.S. No. 108; Council Directive 95/46/EC 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; and, in the United States, a collection of sector specific legislation including the Gramm Leach Bliley Act (GLBA) of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (financial information); the Children's Online Privacy Protection Act (COPPA) of 1998, Pub. L. No. 105-277, 112 Stat. 2681–2728 (children's information); Health Insurance Portability and Accountability Act (HIPAA) of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (health information); Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (personal information collected by the Federal government). All of the major frameworks are undergoing review. *See Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 final (Jan. 25, 2012), *available at* http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf; THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 1–3 (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf; FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS iii–vi (2012), *available at* http://ftc.gov/os/2012/03/120326privacyreport.pdf. *See generally* Andrew Clearwater & J. Trevor Hughes, *In the Beginning . . . An Early History of the Privacy Profession*, 74 OHIO ST. L.J. 897 (2013).

centuries (in the case of the United States), information privacy law is a construct of the technological age.[21] Alas, as currently interpreted, it provides little protection against the risk of surveillance and interference by either government—which benefits from explicit exemptions—or private sector organizations, which are assumed to be trusted parties.[22]

The legal framework for protection of information privacy is organized around a set of "fair information practice principles" (FIPPs), which apply to "data controllers," business or government organizations that collect, store, use or disclose personal information. The FIPPs contain an inner tension between principles that assume that data controllers are *trusted entities*, cognizant and respectful of individual rights (e.g., the principles of choice, purpose limitation, security and accountability), and principles that, in a similar vein to the constitutional framework, treat data controllers with distrust (namely data minimization and collection limitation).[23] In recent years, with the advent of "big data" and increasing pervasiveness of computing in everyday life, data minimization requirements together with the attendant "distrust" assumption, have been marginalized, making room for an emphasis on "notice and choice" and "accountability."[24]

While Alan Westin's canonical conceptualization of privacy concerns individual control over information,[25] the FIPPs provide individuals with very little *de facto* control, usually presented as "notice and choice."[26] This means that controllers are obligated to be "transparent" with respect to their information practices and to offer individuals choices concerning the scope of information collection and use. In reality, however, notice and choice is of little consequence for users.[27] Individuals fail to review, let alone understand,

---

[21] Michael Birnhack, *Reverse Engineering Informational Privacy Law*, 15 YALE J.L. & TECH. 24, 27 (2012).

[22] To be sure, private sector entities are not blindly trusted, as they are laden with auditing requirements and regulatory oversight. Yet the thrust of the information privacy framework, as applied and interpreted in practice, is conditioned on a high degree of trust, particularly when contrasted with the assumptions made by the engineering community.

[23] For the sake of simplicity, this Article calls both of these principles "data minimization." *See generally* Bartosz M. Marcinkowski, *Privacy Paradox(es): In Search of a Transatlantic Data Protection Standard*, 74 OHIO ST. L.J. 1167 (2013).

[24] Omer Tene & Jules Polonetsky, *Big Data for All: Privacy and User Control in the Age of Analytics*, 11 NW. J. TECH. & INTELL. PROP. 239, 242, 260 (2013); *see also* Danielle Keats Citron, *Technological Due Process*, 85 WASH. U. L. REV. 1249, 1249–58, 1281–82 (2008).

[25] ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

[26] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE ii–iii, 4 (2000) (focusing on the principles of notice, choice, access, and security).

[27] *See* Daniel J. Solove, *Introduction: Privacy Self-management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883 (2013); Pedro Giovanni Leon et al., *What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?*, *in* PROCEEDINGS OF THE 2012 ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 19,

organizations' information disclosures; and choice is rarely truly voluntary, informed, and meaningful.[28] Transparency, too, leaves much to be desired, with industry data analysis techniques remaining opaque and mired by a veil of secrecy.[29]

Another pervasive aspect of information privacy law includes a focus on anonymization (also known in some policy circles as de-identification)[30] of personal information, a method viewed skeptically by proponents of PETs given its well-documented technical shortcomings.[31] The current debate around the specifics of a "Do Not Track" (DNT) standard to curb online tracking[32] highlights the fragility of notice, choice, and anonymization. Even in the best-case scenario, if industry players broadly agreed upon a DNT standard, it would remain subject to the goodwill of layers upon layers of information intermediaries who have no relationships with individual data subjects and are subject to little oversight or accountability controls.[33]

Given the fickle controls on information collection, the legal framework has shifted to imposing information stewardship obligations on data controllers, who act as custodians of personal information. These obligations, increasingly grouped under the title "accountability," include devising a privacy compliance program; appointing a chief privacy officer; conducting "privacy impact

---

27 (2012), *available at* http://www.cylab.cmu.edu/files/pdfs/tech_reports/CMUCyLab12008.pdf.

[28] Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE "INFORMATION ECONOMY" 341, 358–67 (Jane K. Winn ed., 2006); *see also* Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure*, 159 U. PA. L. REV. 647, 657 (2011).

[29] Omer Tene & Jules Polonetsky, *Judged by the Tin Man: Individual Rights in the Age of Big Data*, 11 J. ON TELECOMM. & HIGH TECH. L. (forthcoming 2013); *see also* Neil M. Richards & Jonathan H. King, *Three Paradoxes of Big Data*, 66 STAN. L. REV. ONLINE 41, 42–43 (2013), http://www.stanfordlawreview.org/sites/default/files/online/topics/66_StanLRevOnline_41_RichardsKing.pdf.

[30] *See, e.g.*, Robert Gellman, *The Deidentification Dilemma: A Legislative and Contractual Proposal*, 21 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 33, 33–34 (2010).

[31] Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1716 (2010); *see also* Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *in* 2008 IEEE SYMP. ON SECURITY & PRIVACY 111, 124 (May 18–21, 2008).

[32] *See, e.g.*, Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 MINN. J.L. SCI. & TECH. 281, 284–86, 334–35 (2012); *see also* Omer Tene, *Privacy Law's Midlife Crisis: A Critical Assessment of the Second Wave of Global Privacy Laws*, 74 OHIO ST. L.J. 1217, 1234–37 (2013).

[33] Mike Perry, *Do Not Beg: Moving Beyond DNT Through Privacy by Design* 1–2 (presented at the W3C Workshop: Do Not Track and Beyond, Nov. 26–27, 2012), *available at* http://www.w3.org/2012/dnt-ws/position-papers/21.pdf ("[E]very privacy property that DNT:1 aims to provide through regulatory enforcement can be better provided through technical changes to browser and network behavior during private browsing modes. We therefore suggest that the W3C standards body focus on standardizing these technical measures, rather than attempting to broker negotiations over regulatory policy and law.").

assessments;" notifying regulators and individuals about data security breaches; maintaining a record retention policy; and more.[34] A network of privacy enforcement authorities oversees compliance; although outside the United States, enforcement actions have seldom amounted to a disruption of business practices.[35]

Accountability measures implicitly assume that the data controller is a *trusted party*, essentially a fiduciary for individual rights. Even the concept of "privacy by design," which some initially thought was meant to embed principles of data minimization and anonymization into product engineering, is increasingly translated to introducing FIPPs compliance into organizational processes.[36] In other words, privacy by design too has become an "accountability" tool, which assumes data controllers are duly incentivized to protect individual rights.

The notion of the data controller as a trusted party is ill at ease with the anti-surveillance gist of constitutional privacy, the FIPPs' principle of data minimization, and PETs. The technological community researching PETs departs from a diametrically opposed perception of a data controller, that of an *adversary*.[37] Under this approach, information disclosed to a data controller is compromised and can no longer be viewed as private, given that the data controller itself may subject individuals to persistent surveillance. Moreover, data controllers may breach their accountability obligations even without intending to do so, for example, in cases of data breach, coerced government access,[38] or wrongdoing by a rogue employee. The assumption underlying PETs is that once a data controller collects personal information it can—or may be forced to—use it in unforeseen ways, possibly to the detriment of the individuals concerned. Proponents of this view point out that after disclosure, it is almost impossible to control how personal information is used, concluding that PETs should prevent—or at least limit—information disclosure.

In stark contrast to information privacy law, the U.S. Supreme Court's "third party doctrine" has traditionally regarded data controllers as inherently

---

[34] Article 29 Data Prot. Working Party, *Opinion 03/2010 on the Principle of Accountability*, 00062/10/EN. WP 173, at 3, 4, 7, 11, 12 (July 13, 2010).

[35] Consider the resolution of the investigation of Facebook's data practices by the Irish data protection commissioner. OFFICE OF THE DATA PROT. COMM'R, FACEBOOK IRELAND LTD.: REPORT OF AUDIT 5–20 (2011), *available at* http://dataprotection.ie/documents/facebook%20report/final%20report/report.pdf.

[36] Seda Gürses, Carmela Troncoso & Claudia Diaz, Engineering Privacy by Design 17–19 (presented at the Fourth International Conference on Computers, Privacy, and Data Protection, Jan. 25–27, 2011), *available at* https://www.cosic.esat.kuleuven.be/publications/article-1542.pdf.

[37] *See, e.g.*, Omer Tene, *PETs, Law and Surveillance*, CONCURRING OPINIONS (Oct. 8, 2012, 2:36 AM), http://www.concurringopinions.com/archives/2012/10/pets-law-and-surveillance.html.

[38] *See, e.g.*, *Yahoo CEO Fears Defying NSA Could Mean Prison,* FOX NEWS (Sept. 12, 2013), http://www.foxnews.com/tech/2013/09/12/yahoo-ceo-fears-defying-nsa-could-mean-prison.

untrustworthy.[39] Much maligned by privacy scholars[40] and increasingly challenged by a reality where third parties store massive troves of digital information about individuals, the third-party doctrine is in fact based on an assumption similar to that underlying PETs, namely that *third parties are not to be trusted*. In the words of the Supreme Court, "It is well settled that when an individual reveals private information to another, he assumes the risk that his confidant will reveal that information to the authorities, and if that occurs the Fourth Amendment does not prohibit governmental use of that information."[41] According to the Supreme Court, any legitimate expectation of privacy is eviscerated when an individual confides his or her information to a third party, based on an "assumption of risk" rationale.[42]

Hence, PETs are aligned with the assumptions and objectives of the constitutional framework,[43] which given its level of abstraction is not tech-oriented, while not always in tune with the assumptions and goals of the tech-oriented information privacy framework.[44] In other words, PETs are trapped in a regulatory limbo between a framework that recognizes their goals but not their means, and one that recognizes their means but not their goals.

This is not to say that information privacy law is misguided or irrelevant. It deals with important privacy issues that arise in numerous circumstances where an individual is obliged to share information with a trusted party, such as a family physician or a bank. In such situations, preventing information flow is not an option: a patient would not *want* to be treated by a physician who has no

---

[39] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009).

[40] Trying to document criticism of the third-party doctrine in a footnote, Orin Kerr notes: "A list of every article or book that has criticized the doctrine would make this the world's longest law review footnote." *Id.* at 563 n.5. The thrust of the criticism is that technology dictates that individuals' digital identities are curated by third parties including financial institutions, healthcare providers, education institutions, online providers, retailers, government agencies, etc. *See also* A. Michael Froomkin, *"PETs Must Be on a Leash": How U.S. Law (and Industry Practice) Often Undermines and Even Forbids Valuable Privacy Enhancing Technology*, 74 OHIO ST. L.J. 965, 971–73 (2013).

[41] United States v. Jacobsen, 466 U.S. 109, 117 (1984); *see also* Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[42] *Cf. Smith*, 442 U.S. at 749 (Marshall, J., dissenting) ("But, even assuming, as I do not, that individuals 'typically know' that a phone company monitors calls for internal reasons, it does not follow that they expect this information to be made available to the public in general or the government in particular." (citation omitted)).

[43] Including, in the United States, the third-party doctrine. *See* Kerr, *supra* note 39, at 563–64.

[44] Joris van Hoboken points out that PETs pursue a more absolutist agenda than even constitutional privacy: providing individuals with unfettered liberty from surveillance. Constitutional privacy frameworks recognize the legitimate interest of the state to carry on surveillance in certain contexts, as long as such activity is proportional and regulated by law. Hence, constitutional privacy can be depicted as a constant balancing act, while PETs—perhaps appropriately as a "weapon of the weak"—stack the deck against any form of surveillance. *See infra* note 138 and accompanying text.

information about her symptoms and medical history, nor would a bank be willing to offer credit to a counterparty it does not know.

Similarly, PETs do not aspire to address the full gamut of privacy problems. They do not deal with the subtle privacy issues that arise in social contexts, such as those derived from information sharing within a family or group of friends;[45] with privacy concerns arising after disclosure of information to trusted parties, such as a family physician; or with issues relating to identity construction and self-presentation.[46] At the same time, PETs *do* address an important facet of privacy and therefore merit a policy response. Given the thrust of the constitutional privacy framework and the genesis of information privacy law in fears about surveillance, which have become salient over the past few months, policymakers should recognize and expand by appropriate regulatory measures the role of technologies that enable individuals to enforce their right to privacy as freedom from surveillance. At the very least, PETs should not be prohibited or undermined; in certain cases, they should be mandated by law.

The current framework's treatment of PETs is not the result of regulatory oversight. It is precisely the capacity of PETs to limit surveillance that has caused them to clash with powerful state interests, particularly in law enforcement and national security.[47]

Recent disclosures depict the NSA as being responsible for introducing backdoors and security weaknesses in electronic components, standards, back-end systems, and communications, for the purpose of collecting surveillance information on a massive scale—all in the name of national security.[48] Experts in the computer security research community have long warned that weakening the infrastructure of information and communications technology through backdoors and security vulnerabilities is in fact *detrimental* to national security. The damage done by making systems susceptible to surveillance and attack—by multiple, potentially unintended, actors—far outweighs the advantages gained by exploiting such vulnerabilities to collect intelligence.[49] Furthermore, such

---

[45] *See* Kashmir Hill, *Oops. Mark Zuckerberg's Sister Has a Private Facebook Photo Go Public*, FORBES (Dec. 26, 2012, 8:52 AM), http://www.forbes.com/sites/kashmirhill/2012/12/26/oops-mark-zuckerbergs-sister-has-a-private-facebook-photo-go-public.

[46] Seda Gürses & Claudia Diaz, *Two Tales of Privacy in Online Social Networks*, 11 IEEE SECURITY & PRIVACY 29, 33 (2013).

[47] *See, e.g.*, Lisa Vaas, *FBI Claims that Tor Stymied Child Abuse Investigation*, NAKED SECURITY (June 14, 2012), http://nakedsecurity.sophos.com/2012/06/14/fbi-tor-child-abuse-investigation.

[48] James Ball, Julian Borger & Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, GUARDIAN, Sept. 5, 2013, http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[49] Whitfield Diffie and Susan Landau have written extensively about this issue. They argue that national security depends on the security of commercial and other non-military systems and data. *See* WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 79 (1998). They also warn that "communication is fundamental to our species; private communication is fundamental to both our national security and our democracy." Whitfield Diffie & Susan Landau, *Internet Eavesdropping: A*

backdoors and security weaknesses negatively affect some of the guarantees offered by PETs, to the detriment not only of individual PET users, but also of law enforcement and national security personnel.[50]

Private sector entities, too, have been lukewarm about the deployment of PETs. Businesses that thrive on the collection and use of personal information have little incentive to deploy technological tools that limit information flows.[51]

However, the information privacy framework must guarantee that the principles underlying constitutional privacy are not discarded with ease. Moreover, information privacy law could refocus on data minimization, or at least not discount this principle entirely. The existing focus on data use, as opposed to data collection, assumes that data controllers are benevolent and always in control. In reality, misuses of personal information and unanticipated access by third parties through data breaches or government access abound, and prove these assumptions wrong.

III. SURVEILLANCE DEFINED

Today, surveillance capabilities are no longer restricted to the realm of states. As more and more daily activities are mediated by technology, private sector organizations have gained the ability to conduct surveillance at an unprecedented scale, meticulously documenting individuals' communications, online and offline purchases, financial activities, travel, energy consumption, geo-location, and health.[52] As one commentator notes: "Coupled with the

---

Brave New World of Wiretapping, SCI. AM. (Aug. 22, 2008), http://www.scientificamerican.com/article.cfm?id=internet-eavesdropping. More recently, as a reaction to the revelations on NSA and GCHQ surveillance, a group of UK security researchers argued in an Open Letter,

> By weakening cryptographic standards, in as yet undisclosed ways, and by inserting weaknesses into products which we all rely on to secure critical infrastructure, we believe that the agencies have been acting against the interests of the public that they are meant to serve. We find it shocking that agencies of both the US and UK governments now stand accused of undermining the systems which protect us. By weakening all our security so that they can listen in to the communications of our enemies, they also weaken our security against our potential enemies.

Nigel Smart et al., *Open Letter from UK Security Researchers*, BRISTOL CRYPTOGRAPHY BLOG (Sept. 16, 2013, 1:40 PM), http://bristolcrypto.blogspot.co.uk/2013/09/open-letter-from-uk-security-researchers.html.

[50] *See CALEA 2 and Tor, Law Enforcement*, TOR (May 9, 2013), https://blog.torproject.org/category/tags/law-enforcement.

[51] *See* LONDON ECON., STUDY ON THE ECONOMIC BENEFITS OF PRIVACY-ENHANCING TECHNOLOGIES (PETS) 30–31 (2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf.

[52] Roger Clarke has called this "dataveillance." Roger Clarke, *Introduction to Dataveillance and Information Privacy*, DATAVEILLANCE & PRIVACY, http://www.anu.edu.au/people/Roger.Clarke/DV/Intro.html#DV (last updated Aug. 7, 2006); *see also* Tal Z.

private sector's attractiveness as a convenient repository of information is its legal allure, notably in instances when private data gathering is subject to less stringent regulation than what the government faces."[53]

Companies like Google, Apple, Facebook, Microsoft, and Amazon have become vertically integrated up and down the digital value chain, offering devices, operating systems, app stores, browsers, geo-location services, social networks, ad targeting, tailored content, and many more data intensive products and services.[54] Indeed, Apple has cemented its position as a market icon by offering a seamlessly cohesive user experience based on well-designed, fully integrated software and devices. As users have shifted from desktop to mobile platforms, Google has begun to provide a mobile experience featuring an operating system, search engine, map service, and app store. Even Microsoft, which has long adhered to a strategy of selling software for computers of every make, has launched its own tablet and refocused its business model to package "devices and services."[55]

This means that private sector entities are increasingly privy to an ever-growing compilation of individuals' personal information and devices. Moreover, with the shift to an ecosystem of cloud computing, individuals store, process, and retrieve their entire data portfolio through infrastructure (e.g., Dropbox), platform (e.g., Google Apps), and software (e.g., Evernote) service providers online. Governments can remotely access these massive troves of personal information or interfere in communications with—or sometimes without—legal process.[56]

Consequently, government institutions increasingly assert surveillance powers in concert with private sector entities, constituting what some authors call a "surveillant assemblage."[57] This "invisible handshake,"[58] which has recently come to (partial) light as a result of the NSA leaks, risks wholesale

---

Zarsky & Norberto Nuno Gomes de Andrade, *Regulating Electronic Identity Intermediaries: The "Soft eID" Conundrum*, 74 OHIO ST. L.J. 1335 (2013).

[53] Jon D. Michaels, *All the President's Spies: Private–Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 908 (2008).

[54] Not all of the companies offer all of the specified services but the trend is toward greater integration. *See* Jules Polonetsky & Omer Tene, *It's Not How Much Data You Have, but How You Use It: Assessing Privacy in the Context of Consumer Data Integration* 1 (presented to FTC Workshop: The Big Picture: Comprehensive Online Data Collection, Dec. 6, 2012), *available at* http://www.futureofprivacy.org/wp-content/uploads/FPF-White-Paper-Its-Not-How-Much-Data-You-Have-But-How-You-Use-It_FINAL1.pdf.

[55] Letter from Steven A. Ballmer, Chief Exec. Officer, Microsoft, To Our Shareholders, Customers, Partners, and Employees 1–2 (Oct. 9, 2012), *available at* http://www.microsoft.com/investor/reports/ar12/shareholder-letter/index.html.

[56] *See generally* 2 INT'L DATA PRIVACY L. No. 4 (Nov. 2012), http://idpl.oxfordjournals.org/content/2/4.toc (special issue surveying systematic government access to private-sector data in nine countries).

[57] Haggerty & Ericson, *supra* note 12, at 608.

[58] Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VA. J.L. & TECH. 6, 14–16 (2003).

circumvention of constitutional and legislative privacy safeguards. It may result in a highly efficient and largely unaccountable surveillance infrastructure posing an ominous threat to democratic institutions.

For governments, the surveillant assemblage has numerous advantages. First, it is highly efficient to use existing organizations, capabilities, and technologies for surveillance—through outsourcing,[59] legal obligations, voluntary cooperation, coercion,[60] or infiltration[61]—instead of establishing them anew. In addition, individuals do not interface with the government in the same ways or with the same frequency as they do with the private sector, creating ample opportunity for information collection. Today, surveillance has become so cheap and ingrained into technology architecture that businesses often need to invest in order *not* to subject their users to surveillance.[62] Large-scale technological infrastructures are particularly prone to large-scale surveillance risks.[63]

Second, the state can—and actually does[64]—co-opt "Big Brother's Little Helpers"[65] into its surveillance efforts through a combination of carrots and sticks. The carrots for companies include a sense of patriotism or good citizenship; relationships with government decision-makers and regulators; international protection and promotion; and assistance in bids for government

---

[59] NSA whistleblower Edward Snowden himself worked for Booz Allen Hamilton, a large government contractor in this space. According to the *New York Times*, "Edward J. Snowden's employer, Booz Allen Hamilton, has become one of the largest and most profitable corporations in the United States almost exclusively by serving a single client: the government of the United States." Binyamin Appelbaum & Eric Lipton, *Leaker's Employer Is Paid To Maintain Government Secrets*, N.Y. TIMES, June 9, 2013, http://www.nytimes.com/2013/06/10/us/booz-allen-grew-rich-on-government-contracts.html. John M. McConnell, who was Director of National Intelligence under the Bush Administration, is a senior executive at Booz. James R. Clapper Jr., who fills the same role for the Obama Administration, is a former Booz executive. *Id.*

[60] *See, e.g.*, Kerr, *supra* note 39, at 590–91; John J. Biggs, *Lavabit Founder Details Government Surveillance of Secure Email While Documents Disclose Epic Trolling of Feds*, TECH CRUNCH (Oct. 3, 2013), http://techcrunch.com/2013/10/03/lavabit-founder-details-government-surveillance-of-secure-email-while-documents-disclose-epic-trolling-of-feds.

[61] *See* Ryan Gallagher, *How the NSA Is Trying To Sabotage a U.S. Government-Funded Countersurveillance Tool*, SLATE (Oct. 4, 2013, 5:04 PM), http://www.slate.com/blogs/future_tense/2013/10/04/tor_foxacid_flying_pig_nsa_attempts_to_sabotage_countersurveillance_tool.html.

[62] *See* LRDP KANTOR LTD. & CTR. FOR PUB. REFORM, COMPARATIVE STUDY ON DIFFERENT APPROACHES TO NEW PRIVACY CHALLENGES, IN PARTICULAR IN THE LIGHT OF TECHNOLOGICAL DEVELOPMENTS 12–14 (2010), *available at* http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf.

[63] *See* Olga Khazan, *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, ATLANTIC (July 16, 2013, 1:55 PM), http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855.

[64] *See* Greenwald & MacAskill, *supra* note 6; Greenwald et al., *supra* note 14.

[65] Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*, 29 N.C. J. INT'L L. & COM. REG. 595, 636–37 (2004).

contracts. The sticks may include legal action or regulatory scrutiny, and warning of dire national or business consequences in case of refusal. A recent survey conducted on systematic government access to private sector data in nine jurisdictions found that "the most frequent way that governments obtain systematic access to private-sector information is by asking for it, what one workshop participant labeled 'systematic volunteerism.'"[66] In short, corporate officers are unlikely to resist when approached by secret intelligence agencies with compelling letterheads. Moreover, enrollment in the government's intelligence operation can prove to be a lucrative business opportunity in its own right. In fact, the U.S. government may be the biggest customer of corporate data aggregators such as Acxiom and LexisNexis.[67] According to an ACLU report: "The government is not just dipping into a preexisting commercial marketplace to purchase data; companies are actually creating and reshaping their products to meet the needs of government security agencies."[68]

Third, private sector entities are not subject to the constitutional privacy protections that constrain the state. By keeping the surveillance apparatus at arm's length, governments can have their cake and eat it too: conducting surveillance with little safeguards or judicial and legislative scrutiny. As noted by the ACLU: "[Private sector enrollment] offers what is often a path of least resistance to working around privacy laws."[69] Consider a recent case where a federal court entered an order requiring Twitter to turn over to the government subscribers' non-content information, including names, addresses, dates, times, and IP addresses of Twitter activity. The court rejected the subscribers' Fourth Amendment challenge, stating: "If Twitter decided to record or retain this information, any privacy concerns were the consequence of private action, not government action. The mere recording of IP address information by Twitter and subsequent access by the government cannot by itself violate the Fourth Amendment."[70]

Fourth, in the past, a clear legal barrier separated the collection of data for domestic law enforcement and foreign intelligence gathering. In contrast, recent disclosures indicate that the FBI and the NSA have been working closely

---

[66] Fred H. Cate, James X. Dempsey & Ira S. Rubinstein, *Systematic Government Access to Private-Sector Data*, 2 INT'L DATA PRIVACY L.J. 195, 198–99 (2012), *available at* http://idpl.oxfordjournals.org/content/2/4/195.full.pdf+html.

[67] U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-674, PERSONAL INFORMATION: KEY FEDERAL PRIVACY LAWS DO NOT REQUIRE INFORMATION RESELLERS TO SAFEGUARD ALL SENSITIVE DATA 7 (2006).

[68] ACLU, THE SURVEILLANCE-INDUSTRIAL COMPLEX: HOW THE AMERICAN GOVERNMENT IS CONSCRIPTING BUSINESSES AND INDIVIDUALS IN THE CONSTRUCTION OF A SURVEILLANCE SOCIETY 26 (2004) (citation omitted), *available at* http://www.aclu.org/files/FilesPDFs/surveillance_report.pdf.

[69] *Id.* at 2.

[70] *In re* Application of the U.S. for an Order Pursuant to 18 U.S.C. § 2703(d), 830 F. Supp. 2d 114, 132–33 (E.D. Va. 2011).

together to assemble a giant communications database.[71] This phenomenon is not unique to the United States.[72] In the United Kingdom, for example, the Counter-Terrorism Act of 2008 explicitly provides: "Information obtained by any of the intelligence services in connection with the exercise of any of its functions may be used by that service in connection with the exercise of any of its other functions."[73] Hence, "function creep" has allowed information collected by the private sector to find its way to national security authorities, which then repurpose the data for law enforcement or intelligence use.

Fifth, there is an international side to privatized surveillance, with large service providers (typically based in the United States) increasingly storing data about a global user base and being approached by multiple national law enforcement agencies.[74] This is evident particularly in the context of cloud computing, with the blurring of jurisdictional lines between states, service providers, and individuals.[75] Another aspect is the exchange of personal information not only between private and public sector entities but also among intelligence agencies around the globe. Finally, even those (few) legal safeguards that exist with respect to the monitoring of a state's citizens do not apply to non-nationals, thereby subjecting them to practically unfettered surveillance.[76]

---

[71] Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES, July 6, 2013, http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.

[72] *See* IAN BROWN & DOUWE KORFF, FOUND. FOR INFO. PRIVACY RESEARCH (FIPR), UK INFORMATION COMMISSIONER STUDY PROJECT: PRIVACY & LAW ENFORCEMENT 30–33 (2004), *available at* http://eprints.ucl.ac.uk/3880/1/3880.pdf.

[73] Counter-Terrorism Act of 2008, § 19, 12(5) HALS. STAT. (4th ed.) 613, 635–36 (Eng.); *see also* Ian Brown, *Government Access to Private-Sector Data in the United Kingdom*, 2 INT'L DATA PRIVACY L.J. 230, 233 (2012).

[74] *See, e.g.*, Peter Swire, *From Real-Time Intercepts to Stored Records: Why Encryption Drives the Government To Seek Access to the Cloud*, 2 INT'L DATA PRIVACY L.J. 200, 205–06 (2012); Tanguy Van Overstraeten & Ronan Tigner, *Yahoo! Saga Continues: Yahoo! Must Not Hand Over Personal Data to the Public Prosecutor*, LINKLATERS (Jan. 30, 2012), http://www.linklaters.com/Publications/Publication1403Newsletter/TMT-Newsletter-January-2012/Pages/9_Belgium-Yahoo!-saga-continues-Yahoo-personal-data-public-prosecutor.aspx.

[75] Joris van Hoboken, Axel Arnbak & Nico van Eijk, Obscured by Clouds or How To Address Governmental Access to Cloud Data from Abroad 17–18 (presented at Privacy Law Scholars Conference, June 6–7, 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2276103.

[76] While the European Court of Human Rights (ECHR) has applied ECHR protections to foreign nationals outside of Europe, it has done so strictly in the specific context of a territory subject to belligerent occupation by an EU Member State. This situation is not parallel to the application of U.S. constitutional protection, for example, to EU residents in the EU, given that the EU is not subject to U.S. military occupation. Similarly, it is doubtful that European Courts would apply ECHR protections to, say, residents of Yemen, who may be subject to surveillance by EU national security agencies. *See* Al-Jedda v. United Kingdom, 2011 Eur. Ct. H.R. 1092; Al-Skeini v. United Kingdom, 2011 Eur. Ct. H.R. 1093. *See also* Press Release, Office of the Dir. of Nat'l Intelligence, DNI Statement on Activities

The surveillant assemblage heightens the importance of the untrusted controller paradigm. To paraphrase the *Miranda* warning, "information collected may and will be used against you." Companies are not shy about disclosing this risk in their privacy statements.[77] Policymakers should respond to the architecture of surveillance with a mix of appropriate legal and technological tools. The law should not always assume that data controllers are trustworthy and it should promote—or at the very least not hamper—the deployment of PETs.

IV. PETS DEFINED

"PETs" has become a common reference term in policy circles, referring to a variety of technology-driven privacy solutions. However, not all solutions adhere to the same definition of privacy, nor do they translate privacy problems into a uniform solution space. This should come as no surprise, given that the term "privacy" itself is notoriously hard to define.[78] Accordingly, researchers

---

Authorized Under Section 702 of FISA (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa ("Section 702 is a provision of FISA that is designed to facilitate the acquisition of foreign intelligence information concerning non-U.S. persons located outside of the United States. It cannot be used to intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States."); *see also* Caspar Bowden, *PRISM: The EU Must Take Steps To Protect Cloud Data from US Snoopers*, INDEPENDENT (July 10, 2013), http://www.independent.co.uk/voices/comment/prism-the-eu-must-take-steps-to-protect-cloud-data-from-us-snoopers-8701175.html.

[77] For example, Facebook's privacy policy states: "We may access, preserve and share your information in response to a legal request (like a search warrant, court order or subpoena) if we have a good faith belief that the law requires us to do so." *Facebook Data Use Policy: Some Other Things You Need To Know*, FACEBOOK, https://www.facebook.com/about/privacy/other (last updated Dec. 11, 2012). Google's privacy policy states: "We will share personal information . . . if we have a good-faith belief that access, use, preservation or disclosure of the information is reasonably necessary to: meet any applicable law, regulation, legal process or enforceable governmental request." *Google Privacy Policy*, GOOGLE, https://www.google.com/intl/en/policies/privacy (last updated June 24, 2013). LinkedIn states: "We will not disclose personal information . . . unless LinkedIn has a good faith belief that disclosure is permitted by law or is reasonably necessary to: (1) comply with a legal requirement or process, including, but not limited to, civil and criminal subpoenas, court orders or other compulsory disclosures." *LinkedIn Privacy Policy*, LINKEDIN, http://www.linkedin.com/legal/privacy-policy (last updated May 13, 2013). These non-disclosure exceptions are broad, not limited to compliance with a court order or subpoena but rather any "legal request" (Facebook), "enforceable governmental request" (Google) or "other compulsory disclosures" (LinkedIn).

[78] For notable attempts to define privacy see Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 214–19 (1890); *see also* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 103–26 (2010); WESTIN, *supra* note 25, at 24–26; Ruth Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 428–40 (1980); William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 386–89 (1960); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 479–90 (2006).

from various sub-disciplines within the computer science community have proposed a broad range of technologies to address different aspects of privacy in digital systems.

In defining PETs, this Article focuses on technologies that address the privacy issues raised by mass collection of data and its possible repurposing for conducting surveillance or subjecting individuals to intrusive practices, such as censorship. This restricts the scope of PETs to technologies designed to provide privacy protection from untrusted and potentially adversarial data controllers. The presumption that privacy guarantees must not depend on the goodwill of a powerful centralized entity follows a tradition of research in cryptography and security engineering, which defines a "trusted system or component" as "one which can break the security policy" (a definition that ironically originates with the NSA).[79] More specifically, this Article restricts PETs to technological solutions that combine three principles: *elimination of the single point of failure* inherent with any centralized trusted party; *data minimization*; and subjecting protocols and software to community driven *public scrutiny*. The justification and relative importance of each of these three objectives varies depending on the relevant application.

PETs *minimize data disclosure*, for example through use of advanced cryptographic protocols, so that, ideally, only information that users explicitly share is made available to intended recipients. This guarantees minimization of data collected and consequently mitigates risk of data misuse for surveillance purposes.

In some cases, collaborative action is needed. For example, for a user to be able to communicate anonymously, other users must provide cover for her by forming an anonymity set.[80] Collaborative PETs require that trust be distributed among multiple entities to *avoid a single point of failure*. In other words, privacy guarantees must hold even if a subset of peers are malicious and collude with each other to collect information about the user.

Finally, the elimination of the single point of failure inherent to the "trusted service provider" model also requires the delegation of trust to other system components, including protocols, software implementations, and end user

---

[79] Ross Anderson, *"Trusted Computing" Frequently Asked Questions*, UNIV. OF CAMBRIDGE COMPUTER LAB. (Aug. 2003), http://www.cl.cam.ac.uk/~rja14/tcpa-faq.html. Ross Anderson argues:

> The fundamental issue is that whoever controls the [Trusted Computing] infrastructure will acquire a huge amount of power. Having this single point of control is like making everyone use the same bank, or the same accountant, or the same lawyer. There are many ways in which this power could be abused.

Id.; *see also* Dieter Gollmann, *Why Trust Is Bad for Security*, 157 ELECTRONIC NOTES IN THEORETICAL COMPUTER SCI. 3, 7 (2006) (discussing the concept of "trusted computing").

[80] "Anonymity is the state of being not identifiable within a set of subjects, the anonymity set." Andreas Pfitzmann & Marit Köhntopp, *Anonymity, Unobservability, and Pseudeonymity—A Proposal for Terminology*, *in* DESIGNING PRIVACY ENHANCING TECHNOLOGIES 1, 2 (Hannes Federrath ed., 2009).

devices. In order to prevent PETs from simply transforming the "trust the service provider" model into a "trust the protocol" (i.e., the engineers) model, it is necessary to enable experts and the public at large to verify that trust assumptions are not misplaced. This means that protocol design and software implementations need to be *publicly available* and open to scrutiny not only by development teams but also by outsiders. This requirement is well aligned with the security engineering community's culture of continuously exploring attacks on theoretical protocol designs and deployed systems, and publishing the results, as well as with the open source and free software culture that many PETs developers subscribe to.

The importance of these three principles has become even more apparent in light of the recent NSA revelations. Programs like PRISM highlight the importance of avoiding centralized single points of failure with access to massive amounts of data. The leaked NSA presentation entitled "Tor Stinks" states that the NSA and GCHQ are operating some nodes in the open Tor network precisely for the purpose of collecting surveillance information and undermining the privacy protections afforded by the system.[81] Their limited success is due to the fact that their nodes constitute only a small fraction of existing Tor relays.[82] Finally, many of the vulnerabilities in existing open source privacy technologies that are exploited by the NSA according to recently leaked documents had already been independently discovered by the academic research community.[83] In some cases, this has led to certain systems and algorithms not being recommended, and in others, to security updates that successfully eliminated the vulnerabilities.

A tight definition of PETs, which relies on these three principles, leaves out of scope various technologies that are designed to mitigate privacy concerns not directly related to surveillance. This includes, for example, privacy-preserving data publishing[84] and differential privacy[85] that can be applied to enable the sharing and analysis of datasets of personal records while protecting the identity of individuals whose data is included in the dataset. These technologies do not fit this Article's definition of PETs, since they rely on a model in which *a trusted centralized entity* is charged with protecting users' personal information, thereby constituting *a single point of failure*.[86] This trusted entity, the owner of

---

[81] *"Tor Stinks" Presentation—Read the Full Document*, GUARDIAN, Oct. 4, 2013, http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document.

[82] *See id.*

[83] *See id.*

[84] Benjamin C.M. Fung et al., *Privacy-Preserving Data Publishing: A Survey of Recent Developments*, 42 ACM COMPUTING SURV. art. 14, at 2–3 (2010), *available at* http://www.cs.sfu.ca/~wangk/pub/FWCY10csur.pdf.

[85] Cynthia Dwork, *Differential Privacy: A Survey of Results*, *in* PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON THEORY AND APPLICATIONS OF MODELS OF COMPUTATION (TAMC'08) (Manindra Agrawal et al. eds., 2008).

[86] Recent research explores the possibilities of applying differential privacy techniques in a distributed setting, moving away from the centralized curator model. *See, e.g.*, Ruichuan

the database, called the "curator" in the case of differential privacy, by definition has access to all of the information in the database and is in a position to repurpose it for surveillance or categorizations that intrude upon individual or group rights.[87]

Similarly, technologies that aim to restrict use of information that has been collected by a data controller, such as purpose-based access control models, rely on the data controller to define "reasonable" restrictions on its uses of data and to effectively enforce them through technological means.[88] While such technologies can help an organization prevent its employees from accessing personal information for unauthorized purposes, they do not offer protection from the organization itself, which constitutes *a single point of failure* with respect to surveillance concerns.

Other technologies, such as the Platform for Privacy Preferences (P3P),[89] aim to provide users with means to communicate their preferences to organizations and make such organizations' privacy practices more transparent. In addition, in line with the third PETs objective stated above, P3P is a public standard that is open to public scrutiny. Yet, P3P does not provide mechanisms to ensure that user preferences are respected or to guarantee that the actual practices of organizations comply with those expressed in their P3P policies.[90] Thus, P3P fails to minimize default data disclosure towards a centralized entity that is in a position to conduct surveillance. The same is true for privacy settings and other signaling mechanisms, such as DNT.[91]

Finally, this Article's definition of PETs leaves out technologies that address privacy-relevant decision-making or concerns related to intrusive practices. Technologies that focus on helping users make better privacy choices are complementary to the PETs discussed in this Article, as they assist users in deciding when and how to voluntarily share data with others.[92] However, until

---

Chen et al., *Towards Statistical Queries over Distributed Private User Data*, *in* 9TH USENIX CONFERENCE ON NETWORKED SYSTEMS DESIGN AND IMPLEMENTATION (2012), *available at* https://www.usenix.org/sites/default/files/conference/protected-files/pddp-talk-nsdi12.pdf.

[87] *See, e.g.*, Omer Reingold, *Occupy Database—Privacy Is a Social Choice*, WINDOWS ON THEORY (Feb. 28, 2012), http://windowsontheory.org/2012/02/28/occupy-database-privacy-is-a-social-choice.

[88] Ji-Won Byun, Elisa Bertino & Ninghui Li, *Purpose Based Access Control of Complex Data for Privacy Protection*, *in* THE TENTH ACM SYMPOSIUM ON ACCESS CONTROL MODELS AND TECHNOLOGIES 102, 108 (2005), *available at* http://dl.acm.org/citation.cfm?id=2046564.

[89] Joseph Reagle & Lorrie Faith Cranor, *The Platform for Privacy Preferences*, 42 COMMS. ACM, Feb. 1999, at 48, 49.

[90] Lorrie Faith Cranor, *Internet Explorer Privacy Protections Also Being Circumvented by Google, Facebook, and Many More*, TAP BLOG (Feb. 18, 2012), http://www.techpolicy.com/Cranor_InternetExplorerPrivacyProtectionsBeingCircumvented-by-Google.aspx.

[91] *Tracking Protection Working Group*, W3C, http://www.w3.org/2011/tracking-protection; *see also* Tene & Polonetsky, *supra* note 32, at 325.

[92] Yang Wang et al., *From Facebook Regrets to Facebook Privacy Nudges*, 74 OHIO ST. L.J. 1307 (2013).

now, the privacy problem addressed by these technologies is mainly related to social privacy concerns rather than to surveillance. The options a user has in making a decision vary between not disclosing certain information or using privacy controls to limit its dissemination, as opposed to solutions that leverage PETs to limit service providers' access to the data.[93] Further, technologies that protect users from intrusive practices, like ad blockers, do not necessarily limit the data that is disclosed to service providers and thus do not diminish their surveillance capabilities either.[94]

In defining PETs, this Article takes into consideration not only the nature of the technology but also its application context; namely, the roles—and power relations—of the stakeholders involved. For example, this Article considers encryption algorithms that allow users to protect their personal information as PETs. When those same algorithms are used by organizations to protect their own (e.g., military, corporate) secrets, then they are out of the scope of the PET definition. In another example, Private Set Intersection protocols, which help people find common friends without revealing to each other their entire list of friends are considered PETs. Yet, when used to compare and find matches between passengers and no-fly lists, similar protocols are not considered PETs, since in this context their goal is not to ensure freedom from surveillance, but rather, to maintain the confidentiality of a dataset kept by a controller towards another organization.[95]

Various authors have used the term PETs differently. Rubinstein, for example, distinguishes between "substitute PETs" (which block or minimize data collection); "complementary privacy-friendly PETs" (which enhance notice and choice in a privacy-friendly manner); and "complementary privacy-preserving PETs" (which enable ad targeting without allowing an ad network to track consumers).[96] This Article limits the definition of PETs to Rubinstein's first, and for the most part, third categories, including anonymous communication tools as well as solutions to provide provable guarantees of privacy through cryptographic protocols. Rubinstein's second category, comprising "privacy-friendly PETs," such as advertising icons and cookie managers, are out of scope of this Article's definition for PETs, as they rely on a centralized trusted controller.

In her earlier work on "privacy research paradigms," Gürses defines PETs as solutions that stem from security engineering communities aiming to "minimize collection of data during communications"—which mostly coincides with this Article's definition of PETs—as well as solutions that allow users to

---

[93] Gürses & Diaz, *supra* note 46, at 32–33.

[94] *See, e.g.*, *Add-ons*, MOZILLA, https://addons.mozilla.org/en-us/firefox/addon/adblock-plus.

[95] Emiliano De Cristofaro, Jihye Kim & Gene Tsudik, Linear-Complexity Private Set Intersection Protocols Secure in Malicious Model 1 (presented at the 16th IACR Conference on the Theory and Application of Cryptology and Information Security, Dec. 5–9, 2010), *available at* http://eprint.iacr.org/2010/469.pdf.

[96] Rubinstein, *supra* note 19, at 1420–21.

"control data post-data collection" (which are not considered PETs in this Article). Her definition of PETs focuses on the commonalities of solutions that target confidentiality, data minimization or anonymity, while making abstraction of the differences in trust assumptions inherent to different solutions, especially towards data controllers, which constitutes the main criteria for a classification of PETs in this Article.

V. PETS CLASSIFIED

To provide protection from surveillance and interference, PETs rely on different models for the distribution of responsibilities among individuals, data controllers, and third parties, depending on the relevant trust model. Given the focus of the legal framework on data controller responsibilities, this Article first proposes a categorization of PETs based on the role of the data controller. Next, it addresses the attendant policy implications.

A. *Category I: PETs Implemented by Data Controller*

The first category comprises PETs based on advanced cryptographic protocols that must be run jointly by a user and a data controller, and thus require controllers to actively integrate them into service design and implementation. In other words, users cannot deploy these PETs unilaterally; their deployment is contingent on active participation by the data controller. The goal of these PETs is to enable the provision of a service that takes as input private user information without the controller becoming privy to such information. Some examples follow.

1. *Privacy-Preserving Pay-as-You-Drive Tolling*

In October 2009, the European Commission announced that a European Electronic Toll Service (EETS) would substitute the flat road tax systems that existed for decades in EU Member States.[97] Electronic Toll Pricing (ETP) calculates the road taxes to be paid by drivers based on parameters such as the distance they drove, the type of roads used, and the time of usage.[98] The expected benefits of migrating towards a pay-as-you-drive system include the ability to apply congestion charges, lower costs for occasional drivers, and incentivizing environmentally friendly driving practices.[99] At the same time, most of the proposed ETP architectures rely on massive collection of drivers' location data by the Toll Service Provider (TSP) to periodically compute

---

[97] Commission Decision on the Definition of the European Electronic Toll Service and Its Technical Elements, 2009 O.J. (L 268) 11.

[98] Josep Balasch et al., *PrETP: Privacy-Preserving Electronic Toll Pricing*, *in* PROCEEDINGS OF THE 19TH USENIX SECURITY SYMPOSIUM 63, 63 (2010), *available at* https://www.usenix.org/legacy/events/sec10/tech/full_papers/security10_proceedings.pdf.

[99] *Id.*

fees.[100] The collection of this information would enable the TSP to infer sensitive private information with respect to individual drivers.[101] Hence, in this configuration, ETP systems unwittingly become infrastructures of mass surveillance.

To enable the benefits of variable toll pricing while minimizing privacy costs, a group of scientists at KU Leuven devised PrETP, a system based on advanced cryptographic protocols that ensures that drivers pay road taxes according to their usage *without revealing to the TSP the location information* that was used to calculate the fee.[102] With PrETP, location data is stored locally on a user device that computes the fee to be paid at the end of each billing period.[103] The TSP receives only "commitments" that are computed based on drivers' location data.[104] Cryptographic commitments have two important properties: "hiding" and "binding."[105] The hiding property ensures that the location points traversed by a driver are encrypted so that the TSP cannot read their values.[106] The binding property guarantees that users cannot modify the location values they have committed to after their submission to the TSP.[107] In order to ensure that all locations have been used in the computation of a fee, PrETP relies on random spot-checks.[108] This involves requiring a user to prove (by "opening" its corresponding commitment) that she has included (and correctly paid for) locations at which she has been spotted, e.g., by a road camera or radar.[109] The practical feasibility of PrETP was demonstrated with a prototype implementation that runs on a low-cost standard embedded device.[110]

The PrETP architecture minimizes the information disclosed to a TSP by default to only subscriber registration and payment data.[111] Although fees are computed based on users' location traces, such traces are available only to users themselves on their personal device—and not revealed to the TSP.[112] This design considerably lowers the level of trust that users must place in the TSP with respect to their private information. Even if such a controller is malicious or subject to data breaches or government requests, it cannot access or reveal the location trail of its users. Thus, with respect to user privacy, the TSP does not constitute *a single point of failure*.

---

[100] *Id.* at 64.

[101] John Krumm, *Inference Attacks on Location Tracks*, *in* PROCEEDINGS OF PERVASIVE COMPUTING: 5TH INTERNATIONAL CONFERENCE 127, 127, 141 (Anthony LaMarca et al. eds., 2007) (Toronto, Canada, May 13–16, 2007).

[102] Balasch et al., *supra* note 98, at 63–64.

[103] *Id.* at 63.

[104] *Id.*

[105] *Id.* at 65.

[106] *Id.*

[107] *Id.*

[108] Balasch et al., *supra* note 98, at 64.

[109] *Id.* at 64–65.

[110] *Id.* at 63, 72.

[111] *Id.* at 64, 71–72.

[112] *Id.* at 64, 72.

The reliance on random spot-checks for fraud detection implies that some location points are occasionally disclosed to the TSP. However, such disclosure requires active engagement by the user, who is asked to open a commitment to prove that a fee computation for a specific location point at which she had been spotted has been recorded.[113] The need for user collaboration serves as a check on the data controller's power. If the TSP requests that a user open a disproportionate number of commitments, the user can spot such a practice and challenge it as an illegitimate attempt to compile a detailed location trace. The specification of the PrETP protocols and associated security proofs are available in a published academic article, and thus open to *public scrutiny*. This also means that it is possible to discuss further legal or social aspects of the proposed solution, e.g., for evaluating its implications for the burden of proof. Deploying a privacy-preserving electronic toll system based on such protocols also requires that the software implementation is made available for review, to ensure that it follows the protocol specifications and is implemented securely. Further, the privacy guarantees of the system require end user devices to be secure, since unauthorized access by an adversary to the data on the device would compromise the confidentiality of the recorded location trail. Hence, the privacy guarantees in this system are also contingent on public scrutiny of the security of end user devices.

2. *Privacy-Preserving Smart Metering*

Protocols similar to those employed in privacy preserving electronic toll pricing have been devised to implement privacy-preserving smart metering. Smart metering allows utilities to charge variable energy prices based on accurate readings and flexible pricing schemes; for example, charging higher prices during peak consumption periods.[114] Other advantages of a smart grid infrastructure include better forecasting of energy needs; more accurate settlement of costs between energy suppliers and producers; as well as customized energy efficiency advice.[115] Most smart grid projects rely on an architecture requiring the delivery of fine-grained household measurements to utilities.[116] These architectures suffer from severe security and privacy

---

[113] *Id.* at 65.

[114] INFO. & PRIVACY COMM'R OF ONT. & FUTURE OF PRIVACY FORUM, SMARTPRIVACY FOR THE SMART GRID: EMBEDDING PRIVACY INTO THE DESIGN OF ELECTRICITY CONSERVATION 8–9 (2009), *available at* www.ipc.on.ca/images/Resources/pbd-smartpriv-smartgrid.pdf.

[115] *Id.* at 4–6.

[116] Ross Anderson & Shailendra Fuloria, *On the Security Economics of Electricity Metering* 1–2 (presented at the Ninth Workshop on the Economics of Information Security (WEIS 2010), June 7–8, 2010), *available at* http://weis2010.econinfosec.org/papers/session5/weis2010_anderson_r.pdf.

problems.[117] Consumer privacy concerns have already jeopardized the deployment of smart meters in the Netherlands, leading to a deadlock.[118]

The seemingly irreconcilable tension between privacy and the functionality of smart meters can be resolved through the use of cryptographic protocols, such as those proposed by Rial and Danezis.[119] Their proposed system guarantees to the utility provider that the fee paid by a user is correctly calculated based on the energy consumed, while ensuring that the only information revealed to the data controller is the final fee, as opposed to fine-grained energy consumption data.[120] Their design supports flexible, complex pricing policies, and has been proven feasible through efficient prototype implementations.[121]

Further work in the area of privacy-preserving smart metering includes protocols by Kursawe and others to privately compute aggregate meter measurements, allowing for fraud and leakage detection, real-time prediction of demand, and further statistical processing of meter measurements—all without revealing information about individual meter readings.[122] Cavoukian and Kursawe argue that these protocols are a good example of "Privacy by Design," as they allow for the protection of privacy without compromising the quality of smart grid operations.[123] While guaranteeing the accuracy of payments, the protocols *minimize the data* disclosed to a utility provider to include subscriber data; household fee due at the end of a billing period; and aggregate consumption per neighborhood.[124] Customized energy advice solutions do not need to run at the data controller's back-end; they can be installed locally on the meter, which is only accessible within a household and has unlimited access to highly granular user data.[125]

The protocols do *not* reveal fine-grained energy consumption data that could be used to infer sensitive personal information related to customers'

---

[117] *Id.* at 2.

[118] Colette Cuijpers & Bert-Jaap Koops, *Smart Metering and Privacy in Europe: Lessons from the Dutch Case*, *in* EUROPEAN DATA PROTECTION: COMING OF AGE 269, 270 (Serge Gutwirth et al. eds., 2013).

[119] Alfredo Rial & George Danezis, *Privacy-Preserving Smart Metering*, *in* PROCEEDINGS OF THE 10TH ANNUAL ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 49, 49–50 (2011), *available at* http://dl.acm.org/citation.cfm?id=2046564.

[120] *Id.* at 49.

[121] *Id.*

[122] Klaus Kursawe, George Danezis & Markulf Kohlweiss, *Privacy-Friendly Aggregation for the Smart-Grid*, *in* PROCEEDINGS OF PRIVACY ENHANCING TECHNOLOGIES: 11TH INTERNATIONAL SYMPOSIUM 175, 175 (Simone Fischer-Hübner & Nicholas Hopper eds., 2011) (July 27–29, 2011).

[123] Ann Cavoukian & Klaus Kursawe, Implementing Privacy by Design: The Smart Meter Case 1 (presented at the 2012 IEEE International Conference on Smart Grid Engineering (SGE 2012), Aug. 27–29, 2012), *available at* http://ieeexplore.ieee.org/xpl/articleDetails.jsp?reload=true&arnumber=6463977.

[124] *See* Kursawe, Danezis & Kohlweiss, *supra* note 122, at 175.

[125] *Id.* at 176.

lifestyle and daily activities.[126] Thus, with respect to privacy, the trust model is identical to that employed in the existing (non-smart) infrastructure. In other words, these protocols facilitate the modernization of the infrastructure without introducing new surveillance risks.

Whereas PrETP relies on random spot-checks for fraud detection, the trust model underlying privacy-preserving smart meter protocols assumes that the meters themselves are tamper-resistant.[127] This assumption, too, is similar to that used to detect energy fraud in existing non-smart infrastructures: physical inspection of a metering device to determine if it has been tampered with. Furthermore, by comparing aggregate energy consumption at the neighborhood level with payment data, utilities can get a good indication of whether energy fraud is taking place in a certain locality.[128]

The reliance on tamper-resistant devices for service integrity is, however, not an option in PrETP. Even if user devices cannot be tampered with, the input location data can be easily spoofed, for example, by feeding fake GPS data to the device. Additionally, the end user devices can simply be turned off, resulting in unrecorded or unpaid for road usage. By comparison, turning off a smart energy meter would interrupt the energy supply to the household.[129]

Similar to the PrETP, smart meter protocols are open to *public scrutiny* and the software running in deployed metering devices is available for review to ensure that fine-grained energy consumption data is not being leaked by the metering device.

3. *Other Applications*

Additional proposals for implementing PETs with active participation of a data controller include e-cash systems that provide privacy benefits of cash payments (strong anonymity) while preventing fraud, such as double spending of electronic coins;[130] search protocols allowing a search provider to return results that include search terms while learning neither the search terms nor the results;[131] and digital credential systems[132] that allow anonymous yet

---

[126] *See* Rial & Danezis, *supra* note 119, at 49.

[127] *See id.* at 51.

[128] *See* Kursawe, Danezis & Kohlweiss, *supra* note 122, at 175, 184, 186.

[129] *See, e.g.*, *Smart Meters*, ENEMALTA, http://www.enemalta.com.mt/index.aspx?cat=5&art=21&art1=55#Question1.15.

[130] Jan Camenisch, Susan Hohenberger & Anna Lysyanskaya, *Compact E-Cash*, *in* ADVANCES IN CRYPTOLOGY—EUROCRYPT 2005: PROCEEDINGS OF THE 24TH ANNUAL INTERNATIONAL CONFERENCE ON THE THEORY AND APPLICATIONS OF CRYPTOGRAPHIC TECHNIQUES 302, 302–03 (Ronald Cramer ed., 2005), *available at* http://link.springer.com.proxy.lib.ohio-state.edu/content/pdf/10.1007%2Fb136415.pdf.

[131] *See* Rafail Ostrovsky & William E. Skeith III, *Private Searching on Streaming Data*, 20 J. CRYPTOLOGY 397, 398, 401–02 (2007).

[132] Digital credentials are the digital equivalent of paper-based credentials such as passports, driver's licenses, membership cards, or tickets that give access to a service. Credentials are issued by an authority to an individual to certify attributes, qualifications,

authenticated and accountable transactions between users and data controllers, and can be used to build privacy-preserving identity management systems.[133]

As a common design principle, these PETs are designed to *minimize the information* that users disclose to a data controller in order to obtain a service, while guaranteeing the integrity of the service itself (e.g., ensuring that the parties participating in the system cannot cheat).[134] A crucial element is that the protocol specifications and their associated security proofs are *publicly available* for review by experts other than the systems' designers. Moreover, as users usually store their personal data locally, their personal devices need to be secured to prevent unauthorized access to the data they store. A benefit of locally storing personal information is that with probable cause, legitimate law enforcement investigations can target individuals (and their devices), while large-scale surveillance and data mining become impractical.

In some cases, multiple PETs need to be in place to ensure that the privacy guarantees hold. This is the case, for example, for PETs whose objective is to enable anonymity, such as anonymous credentials and payments, which require use of anonymous communication channels.[135] If this were not the case, the anonymity protection provided at the application layer would be compromised by the exposure of identifiers (e.g., IP addresses) at the network layer.[136]

Many of the PETs described in this Part have been demonstrated to work efficiently in standard devices. Alas, there has been little interest to adopt them on the part of data controllers. As discussed above, this is often the result of data controllers' thirst for users' information, which they are loath to forgo unless forced to do so by regulators or public pressure.[137] Surely, the (lack of) availability of advanced cryptographic expertise, the complexity of the

---

competences, or clearances that attach to that individual. Stefan Brands, *Towards Digital Credentials*, ERCIM NEWS (Apr. 2002), http://www.ercim.eu/publication/Ercim_News/enw49/brands.html.

[133] *See* Jan Camenisch & Els Van Herreweghen, *Design and Implementation of the* idemix *Anonymous Credential System*, *in* PROCEEDINGS OF THE 9TH ACM CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 21, 21–22 (Vijay Atluri ed., 2002), *available at* http://dl.acm.org/citation.cfm?id=586114. An identity management system refers to a set of technologies that can be used for enterprise or cross-network identity management. These systems typically comprise three types of entities: (1) Issuers, whose role is to issue credentials to users; (2) Users, who obtain credentials in order to access services; and (3) Verifiers, who rely on the credentials presented by users to grant access to their services. *See generally Oracle Database: Enterprise User Security Administrator's Guide*, ORACLE (June 2013), http://docs.oracle.com/cd/E11882_01/network.112/e10744.pdf.

[134] *See* Camenisch & Van Herreweghen, *supra* note 133, at 21–22.

[135] *Id.* at 22.

[136] Mary Rundle & Ben Laurie, Identity Management as a Cybersecurity Case Study 8–9 (presented at the Oxford Internet Institute Conference—Safety and Security in a Networked World: Balancing Cyber-Rights and Responsibilities, Sept. 2005), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=881107.

[137] Ian Brown, *Britain's Smart Meter Programme: A Case Study in Privacy by Design*, 27 INT'L REV. L. COMPUTERS & TECH. (forthcoming 2013), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2215646.

protocols, and the engineering implementation costs can also play a role in the decision-making process. Yet, some of these costs may be curbed if the protocols and algorithms underlying these systems are made open for public use.

B. *Category II: Client-Side Software Deployed by a User While Using a Service Offered by a Data Controller*

The second category of PETs comprises client-side tools and technologies that are deployed unilaterally by users to enhance their privacy while using a service offered by a data controller. Contrary to the previous category, these PETs require neither active engagement on the part of the data controller nor modification of its service.[138] Yet given its control of the surrounding environment, the data controller retains the power to disable or block the use of these PETs, and such actions may in fact be in its business interest.

Examples of PETs in this category include encryption tools that maintain the confidentiality of user content that is hosted or shared through a service offered by a data controller. For example, GnuPG allows users to encrypt and sign their email communications so that an email provider cannot access the content of the emails it hosts, which are available strictly to their intended recipients.[139] Mymail-Crypt is a Google Chrome browser extension that implements GnuPG for the popular webmail service Gmail.[140]

Similar tools have been developed to protect user-generated content shared in social networks such as Facebook. For example, through Scramble!, a Firefox browser extension, users can define a list of friends who are authorized to read a specific piece of content.[141] The tool encrypts a user's posts so that only her selected friends can read them.[142] Neither other users nor Facebook itself can access the content.[143] Obviously, in both of these applications, the intended recipients of the information (friends, email recipients) are trusted with its content.

Other tools, such as chat clients that integrate Off-the-Record (OTR) protocols, provide content confidentiality, perfect forward secrecy, and

---

[138] These PETs are also called "DIY" privacy tools. *See* Helen Nissenbaum, Keynote Address at 6th Workshop on Hot Topics in Privacy Enhancing Technologies: DIY Privacy with Obfuscation (July 12, 2013).

[139] *See The GNU Privacy Guard*, GNUPG, http://www.gnupg.org.

[140] *My-Mail Crypt for Gmail*, CHROME WEB STORE, https://chrome.google.com/webstore/detail/mymail-crypt-for-gmail/jcaobjhdnlpmopmjhijplpjhlplfkhba.

[141] Filipe Beato, Markulf Kohlweiss & Karel Wouters, *Scramble! Your Social Network Data*, *in* PRIVACY ENHANCING TECHNOLOGIES 211, 212 (Simone Fischer-Hübner & Nicholas Hopper eds., 2011), *available at* http://link.springer.com/content/pdf/10.1007%2F978-3-642-2263-4_12.

[142] *See id.* at 211.

[143] *Id.* at 212.

repudiability for instant messaging applications.[144] Perfect forward secrecy ensures that past messages, even those recorded by an adversary who has observed (encrypted) traffic, cannot be recovered retroactively even if communicating parties are coerced to reveal their cryptographic keys.[145] Repudiability, which is the opposite of the typical non-repudiation property offered by digital signatures, ensures that once a communication has ended, no one—not even the users involved in the chat conversation—can *prove* whether a user sent a particular message.[146] This protocol thus provides off-the-record properties for instant messaging communications that are similar to those of verbal conversations.

Open source implementations of OTR protocols are available in instant messaging clients, such as Adium,[147] Cryptocat,[148] Xabber,[149] IM+,[150] and many others, that provide secure chat applications for Android, iPhone, and other platforms. Interestingly, Gmail's Google Chat "Off the Record" settings[151] do not offer the privacy guarantees of a cryptographic OTR protocol. The term "Off the Record" is used by Google to mean that chat logs are not retrievable by end users.[152] Importantly, Google's policy on "Off The Record" chats does not state that Google itself does not record the logs on its back-end servers.[153]

This illustrates the most important difference between content encryption PETs and the privacy settings commonly offered by commercial data controllers, which provide communication and content hosting services. Both sets of tools protect content in the face of unauthorized users; but *PETs also provide protection from surveillance by the controller itself*, who is no longer privy to content communicated by a user. Thus, as opposed to privacy settings, the use of these PETs *minimizes data* disclosed to the controller, avoids relying on it as a trusted third party, and consequently, avoids a *single point of failure*. At the same time, these PETs may interfere with business models based on profiling users and monetizing their interests and preferences, a common business model for major email and social network providers.

---

144 *See* Nikita Borisov, Ian Goldberg & Eric Brewer, *Off-the-Record Communication, or, Why Not To Use PGP*, *in* PROCEEDINGS OF THE 2004 ACM WORKSHOP ON PRIVACY IN THE ELECTRONIC SOCIETY 77, 77 (Sabrina De Capitani di Vimercati & Paul Syverson eds., 2004), *available at* http://dl.acm.org/citation.cfm?id=1029200.

145 *See id.* at 78–79.

146 *Id.*

147 *About Adium*, ADIUM, http://www.adium.im/about.

148 CRYPTOCAT, https://crypto.cat.

149 XABBER, http://www.xabber.com.

150 *IM+: Instant Messanging for iPhone, iPod Touch, and iPad*, SHAPE, http://www.shape.ag/en/products/details.php?product=im&platform=iphone.

151 *Chatting off the Record*, GOOGLE, https://support.google.com/chat/answer/29291?hl=en.

152 *Id.*

153 *See id.*; *see also Google Privacy Policy*, *supra* note 77.

As an added benefit to users, and arguably to society at large, the concealment of content from the controller inevitably diminishes its ability to censor users' communications and curtail free speech.[154] While advancing privacy and free speech rights, the lack of control over content also inevitably means enhanced opportunity for malicious actors to engage in perverse activity, such as child pornography, hate speech, and other criminal activities. This means that the resistance that PETs offer towards surveillance and control also makes it difficult to detect criminal activity or mandate "correct" behavior through code, e.g., through censorship of undesirable materials. This means that tools other than technology-based surveillance and control must be relied upon in order to deal with such activities.[155]

It is important to note that content encryption tools by themselves do not provide protection from traffic analysis by data controllers, such as email, social network, Internet, and platform providers, who are in a position to observe encrypted communications. Such controllers can see when, how frequently, and with whom users communicate, and are able to infer social communication graphs from such data.[156] To protect against this type of information leakage—and potential surveillance—content encryption tools must be used in combination with the collaborative PETs classified in the third category below,[157] which provide communication anonymity and other properties of traffic analysis resistance.

Collaborative PETs providing anonymous communications, such as Tor,[158] enable users to access websites and online services anonymously. In this section we consider these technologies in relation to the data controller offering the online service that users access anonymously via Tor, while making abstraction of whether the anonymizing service is implemented by a single user or by a community of collaborating users. From the perspective of the data controller, the anonymous communication system can be seen as a client-side tool, since individuals can use it unilaterally without requiring the controller to modify its service.

When a user accesses a service through Tor, it is not possible for the service provider to determine the user's identity, which is masked behind a series of proxies.[159] Furthermore, it is not possible for websites to link different sessions

---

[154] Dan Moren & Lex Friedman, *Silent Email Filtering Makes iCloud an Unreliable Option*, MACWORLD (Feb. 28, 2013, 9:45 AM), http://www.macworld.com/article/2029570/silent-email-filtering-makes-icloud-an-unreliable-option.html; *see also* Jeffrey Rosen, *The Delete Squad: Google, Twitter, Facebook and the New Global Battle over the Future of Free Speech*, NEW REPUBLIC (Apr. 29, 2013), http://www.newrepublic.com/article/113045/free-speech-internet-silicon-valley-making-rules#.

[155] *See infra* notes 202–209 and accompanying text.

[156] *See* Beato, Kohlweiss & Wouters, *supra* note 141, at 221.

[157] *See infra* notes 141–177 and accompanying text.

[158] *Tor FAQ*, TOR, https://www.torproject.org/docs/faq.html.en.

[159] *Id.*

to a single user, effectively disabling any tracking capability.[160] However, service providers such as websites can block connections that come from the Tor network.[161] In fact, they may be incentivized to do so in order to maximize behavioral advertising revenues, with which Tor can interfere.

An additional approach for PETs in this category uses obfuscation, that is, the automated generation—by client-side software tools—of "fake" signals that are indistinguishable from users' actual online activities, providing users with a noisy "cover."[162] One example of an obfuscation tool is TrackMeNot,[163] a browser plugin that aims to obstruct search engines from compiling accurate user profiles based on individuals' search history.[164] To achieve this, TrackMeNot generates automated "dummy" queries, which obfuscate the user profile and elude profiling algorithms.[165] Although TrackMeNot and other search obfuscation tools have been found to be vulnerable to attacks that allow search engines to distinguish between user-generated and computer-generated queries,[166] further advances in this area may result in tools that achieve robust protection from profiling based on obfuscation.[167]

To sum, client-side PETs in this category are deployed unilaterally by a user while using a service offered by a data controller, but do not depend on active data controller implementation. They satisfy the model of an untrusted data controller, relying on *data minimization* and avoidance of *a single point of failure*. They depend on the security of the software implementation of the PET, and thus require that the code be available for *public scrutiny*.

C. *Category III: Collaborative Applications Without a Data Controller*

A third category of PETs refers to stand-alone systems that are typically operated by a set of users who work collaboratively to achieve privacy

---

[160] *Id.*

[161] *Id.*

[162] Daniel C. Howe & Helen Nissenbaum, *TrackMeNot: Resisting Surveillance in Web Search*, *in* LESSONS FROM THE IDENTITY TRAIL: ANONYMITY, PRIVACY AND IDENTITY IN A NETWORKED SOCIETY 417, 417–18, 420–21 (Ian Kerr et al. eds., 2009).

[163] *TrackMeNot*, N.Y.U. COMPUTER SCI., http://cs.nyu.edu/trackmenot; *see also* Howe & Nissenbaum, *supra* note 162, at 417–18, 420–21.

[164] Omer Tene, *What Google Knows: Privacy and Internet Search Engines*, 2008 UTAH L. REV. 1433, 1466.

[165] Howe & Nissenbaum, *supra* note 162, at 417–18, 420–21.

[166] Ero Balsa, Carmela Troncoso & Claudia Diaz, *OB-PWS: Obfuscation-Based Private Web Search*, *in* PROCEEDINGS OF THE 2012 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 491, 494–95 (2012), *available at* http://www.cosic.esat.kuleuven.be/publications/article-2083.pdf.

[167] For the legal case for obscurity, see Woodrow Hartzog & Frederic Stutzman, *The Case for Online Obscurity*, 101 CALIF. L. REV. 1, 1–4 (2013); Woodrow Hartzog & Frederic Stutzman, *Obscurity by Design*, 88 WASH. L. REV. 385, 385–88 (2013); Fred Stutzman & Woodrow Hartzog, *Boundary Regulation in Social Media*, *in* PROCEEDINGS OF THE ACM 2012 CONFERENCE ON COMPUTER SUPPORTED COOPERATIVE WORK 769, 769–70 (2011), *available at* http://dl.acm.org/citation.cfm?id=2145320.

protection. In these systems, participants concurrently act as both users and service providers. The objective of these PETs is to enable the collaborative provision of a service without a centralized party, which would ostensibly be in a position to conduct surveillance.

Collaborative solutions are particularly important to achieve privacy protection from traffic analysis.[168] Traffic analysis is the process of intercepting communications and examining patterns in traffic data in order to gain intelligence.[169] It can be performed even when the intercepted messages remain encrypted.[170] In their book on wiretapping, Diffie and Landau highlight the importance of traffic analysis with respect to surveillance, stating that "traffic analysis, not cryptanalysis, is the backbone of communications intelligence."[171] This is because traffic data is exposed by default and easy to process. Moreover, the communication patterns extracted through traffic analysis are often more indicative of behavior than actual content, and can be used to select targets to subject to more intensive surveillance.

Most of the PETs designed to resist traffic analysis aim to provide communication anonymity. The key idea is that the users of the system join in order to provide cover for each other and thereby constitute an "anonymity set."[172] Adversaries recording and analyzing traffic data in such systems cannot determine which of the users in the anonymity set is associated with a specific action or recover communication patterns between users (i.e., the communication graph). Examples of such technologies include Mixmaster, a system for anonymous email;[173] I2P for anonymous chat, email, and other applications;[174] and Freenet for anonymous publishing, content sharing and forums.[175] Additional efforts in this vein include peer-to-peer social networking services, including MyZone[176] and Safebook.[177]

But by far the most successful example of a PET in this category is the Tor network, which is used daily by more than half a million users to anonymously

---

[168] *See generally* George Danezis & Richard Clayton, *Introducing Traffic Analysis*, *in* DIGITAL PRIVACY: THEORY, TECHNOLOGIES, AND PRACTICES 95, 95–116 (Alessandro Acquisti et al. eds., 2008).

[169] Traffic data includes the timing, order, frequency, and volume of communications, as well as the location and identities of the parties engaged in a communication. DIFFIE & LANDAU, *supra* note 49, at 92.

[170] *Id.* at 39.

[171] Danezis & Clayton, *supra* note 168, at 96 (citing DIFFIE & LANDAU, *supra* note 49, at 92).

[172] "*Anonymity* is the state of being not identifiable within a set of subjects, the *anonymity* set." Pfitzmann & Köhntopp, *supra* note 80, at 2.

[173] *See* MIXMASTER, http://mixmaster.sourceforge.net.

[174] *See Anonymous Network*, I2P, http://www.i2p2.de.

[175] *See The Freenet Project*, FREENET, https://freenetproject.org.

[176] *See Welcome to MyZone*, MYZONE, http://www.joinmyzone.com.

[177] Leucio Antonio Cutillo, Refik Molva & Thorsten Strufe, *Safebook: A Privacy-Preserving Online Social Network Leveraging on Real-Life Trust*, 47 IEEE COMMS. MAG., Dec. 2009, at 94, 94.

browse the web, circumvent censorship, and communicate with each other.[178] To achieve strong anonymity, Tor routes user connections through a series of Tor relays (three relays by default), with each relay operated by an individual or organization, including multiple universities and the Chaos Computer Club.[179]

In contrast to the previous category, where Tor is discussed in relation to a data controller (external to the Tor system) offering an online service that is accessed anonymously by users, here the focus is on the operation of the anonymity network itself, where participants in the system may not only act as end-users but also as service providers. This perspective is not concerned with data controllers that offer a service external to the anonymity network, but rather with the entities that implement it in a collaborative fashion. In this context, Tor, as well as other anonymity systems such as I2P, may be used not only to anonymously access external services (as considered in the previous category), but also to enable the provision of privacy-enhanced services within the network itself. Examples of such services include Tor hidden servers that offer chat, email, file sharing, blogs, etc.

As with other anonymous communication networks, a key aspect of Tor is that no single relay can observe both the source and destination of a communication. If an anonymous communication system were built using a single proxy, that proxy would effectively act as a trusted party constituting a single point of failure with respect to both surveillance and censorship.[180] Consequently, single-proxy anonymity systems, such as Anonymizer[181] and HideMyAss,[182] are not only outside the scope of this Article's definition of PETs, but also viewed with distrust by technical experts.[183] This distrust seems well founded, given reports that Anonymizer is linked to companies that sell surveillance systems to governments[184] and that HideMyAss has revealed the identity of "anonymous" users to law enforcement.[185]

Instead, the trust model in networks such as Tor is distributed among multiple network relays to avoid a single point of failure. From a protocol

---

[178] *Tor FAQ*, *supra* note 158; Roger Dingledine, Nick Mathewson & Paul Syverson, *Tor: The Second-Generation Onion Router*, *in* PROCEEDINGS OF THE 13TH USENIX SECURITY SYMPOSIUM 303, 304–05 (2004).

[179] CHAOS COMPUTER CLUB, http://www.ccc.de/en. The Chaos Computer Club is Europe's largest association of hackers. *Id.*

[180] *See Tor FAQ*, *supra* note 158.

[181] *See How Anonymizer Universal Protects You*, ANONYMIZER, https://www.anonymizer.com/homeuser/universal/index.php#howitworks.

[182] HIDEMYASS, hidemyass.com.

[183] Qubit, *HideMyAss.com . . . Doesn't*, TECHPOWERUP (Sept. 26, 2011), http://www.techpowerup.com/152679/hidemyass-com-doesnt.html.

[184] *See* Ms. Smith, *Anonymizer Tied to Company Selling TrapWire Surveillance to Governments*, NETWORK WORLD (Aug. 14, 2012, 4:53 PM), http://www.networkworld.com/community/blog/anonymizer-tied-company-selling-trapwire-surveillance-governments.

[185] *See* Qubit, *supra* note 183.

perspective,[186] in order to deanonymize a user, all of the proxies that relay that user's communication must collude. From a traffic analysis perspective, anonymity in Tor can be compromised if *both* the first and last relays collude.[187] This weaker protection (or stronger trust model) is due to the difficulty of anonymizing web traffic: the first and last relays can identify that they are routing the same connection—even if from a protocol perspective they cannot match circuit identifiers—by comparing and correlating the start and end time of a connection and the number of packets transmitted within it.[188] Recent research in anonymous communications proposes refining Tor's trust model by allowing users to take into account in their relay selection the trust that they place in different relay operators.[189]

An important requirement for achieving effective protection is that the relays must be located in different geographic locations around the globe. This is necessary to ensure diversity of jurisdictions and of ISPs in order to prevent end-to-end tracing of connections.[190] If a single ISP or network operator who controls an Autonomous System[191] could observe a connection coming both in and out of the Tor network, that entity would be able to link the end points of the connection by correlating traffic characteristics such as start and end connection timing or number of packets.[192] For this reason, the routing policy of Tor does not allow choice of more than one relay within a given IP subnet.[193] This also means, however, that Tor cannot guarantee anonymity towards entities that have the power to monitor Internet communications on a *global scale*, as the case may be for powerful signals intelligence organizations, such as the NSA and GCHQ.[194] The leaked NSA reports indicate, however, that even these organizations have so far not been able to fully exploit the information at

---

[186] The Tor protocol is based on "onion routing." The onion routing protocol was proposed by David M. Goldschlag, Michael G. Reed and Paul F. Syverson. *See* David M. Goldschlag et al., *Hiding Routing Information*, *in* INFORMATION HIDING: PROCEEDINGS OF THE FIRST INTERNATIONAL WORKSHOP 137, 137–39 (Ross Anderson ed., 1996).

[187] *See* Dingledine, Mathewson & Syverson, *supra* note 178, at 314–15; *Tor FAQ*, *supra* note 158.

[188] *See* Dingledine, Mathewson & Syverson, *supra* note 178, at 314–15.

[189] Aaron M. Johnson et al., *Trust-Based Anonymous Communication: Adversary Models and Routing Algorithms*, *in* PROCEEDINGS OF THE 18TH ACM CONFERENCE ON COMPUTER & COMMUNICATIONS SECURITY 175, 175 (2011).

[190] *See* Dingledine, Mathewson & Syverson, *supra* note 178, at 314–15.

[191] An Autonomous System (AS) is a collection of connected Internet Protocol (IP) routing prefixes under the control of one or more network operators that presents a common, clearly defined routing policy to the Internet. *See* Paul Krzyzanowski, *Understanding Autonomous Systems: Routing and Peering* (Apr. 5, 2013), http://www.cs.rutgers.edu/~pxk/352.notes/autonomous_systems.html.

[192] Dingledine, Mathewson & Syverson, *supra* note 178, at 314–15.

[193] *See* Roger Dingledine & Nick Mathewson, *Tor Path Specification*, GITWEB, https://gitweb.torproject.org/torspec.git?a=blob_plain;hb=HEAD;f=path-spec.txt.

[194] *See* Ewen MacAskill et al., *GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications*, GUARDIAN, June 21, 2013, http://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.

their disposal (from multiple sources, including corrupted Tor nodes and fiber optic cables) to de-anonymize a large fraction of Tor users.[195]

Tor aims to protect not only its users but also its relay operators, who are often volunteers. Relay operators may be (legally) compelled to reveal cryptographic keys or decrypt a (past) communication of interest to law enforcement. To avoid such situations, the Tor protocols establish ephemeral session keys with forward security properties,[196] meaning that relays are unable to decrypt a communication after it has terminated.

The need for forward security is best illustrated by the case of *anon.penet.fi*, an early pseudonymous email system that operated in Finland in the 1990s.[197] *Anon.penet.fi* had a simple design with a single proxy that kept a table of correspondence matching pseudonyms and email addresses.[198] In 1996, a plaintiff claimed that a user of *anon.penet.fi* had sent a message to a newsgroup infringing its copyright.[199] A court ordered the administrator of *anon.penet.fi* to unveil the identity of the user concerned.[200] The administrator, whose reputation had already been damaged by reports that the service was used to disseminate child pornography, decided to shut down *anon.penet.fi*, fearing it could no longer guarantee users' anonymity.[201]

Finally, Tor also provides a platform for offering *hidden services*—whose location or IP address cannot be determined—which can be accessed anonymously by other users.[202] In some cases, hidden services facilitate important public policy goals such as freedom of speech by Iranian bloggers, whose blogs would otherwise be blocked by state-sponsored denial of service attacks. Other examples of hidden services include anonymous blogs, decentralized instant messaging applications such as TorChat,[203] and services for safely sharing information with journalists, such as the *New Yorker*'s Strongbox.[204] Disturbingly, hidden services are also known to facilitate

---

[195] *See* Fung et al., *supra* note 84; *see also* Ball, Schneier & Greenwald, *supra* note 3.

[196] Forward security is a property of the key-agreement protocol that ensures that a session key derived from a set of long-term public and private keys will not be compromised if one of the long-term private keys is compromised in the future. *See* Shengbao Wang et al., *Perfect Forward Secure Identity-Based Authenticated Key Agreement Protocol in the Escrow Mode*, CRYPTOLOGY EPRINT ARCHIVE, http://eprint.iacr.org/2007/313.pdf.

[197] *See generally* Sabine Helmers, *A Brief History of Anon.penet.fi—The Legendary Anonymous Remailer*, COMPUTER-MEDIATED COMM. MAG., Sept. 1, 1997, www.december.com/cmc/mag/1997/sep/toc.html.

[198] *See* George Danezis, Claudia Diaz & Paul Syverson, *Anonymous Communication*, *in* HANDBOOK OF FINANCIAL CRYPTOGRAPHY AND SECURITY 341, 347 (Burton Rosenberg ed., 2011).

[199] *See id.* at 348.

[200] *Id.*

[201] *See id.*

[202] *See Tor: Overview*, TOR, https://www.torproject.org/about/overview.html.en.

[203] *TorChat*, GITHUB, https://github.com/prof7bit/TorChat.

[204] *See Strongbox*, NEW YORKER, http://www.newyorker.com/strongbox.

malevolent activity. The Silk Road[205] was a large online black market operated as a Tor hidden server. An estimated 70% of the ten thousand products for sale by Silk Road vendors were illegal drugs.[206] Law enforcement officials often complained that the security of Tor made it impossible to crack down on such illegal activities, and called for the introduction of backdoors in Tor to make law enforcement work possible. After operating for more than two and a half years, the Silk Road was taken down by the FBI on October 2, 2013. Reports on the FBI investigation indicate that it was traditional detective work that led to the successful arrest of the Silk Road operator, rather than an attack on the Tor network.[207] Another recent high-profile example is that of Freedom Hosting, a web hosting service also implemented as a Tor hidden server that the FBI characterized as the "largest facilitator of child porn on the planet."[208] The FBI took down the service and arrested its operator in August 2013. According to news reports, the FBI conducted a targeted attack that exploited a vulnerability in the Freedom Hosting server, without compromising the Tor network.[209] These two cases emphasize that human intelligence (HUMINT), detective work, and targeted operations can lead to law enforcement successes, even if anti-surveillance technologies are in use. At the same time, these methods do not facilitate low-cost mass surveillance.

With respect to its transparency practices, Tor makes both its protocols and open source software available for public review. This is necessary to build trust and ensure that there are no backdoors built into the system, which could compromise the anonymity of Tor users. Indeed, Tor is likely the PET subject to the most detailed scrutiny of privacy researchers, with dozens of research papers published over the past decade analyzing its security, reporting vulnerabilities, and proposing design improvements.[210] Such engagement by a community of experts is crucial to ensure that the system is continuously updated and improved.

The leaked NSA documents outline the various strategies that the NSA employed to try to de-anonymize Tor users.[211] None of these strategies have

---

[205] *All Things Considered: Silk Road: Not Your Father's Amazon.com* (NPR Radio Broadcast June 12, 2011).

[206] *See, e.g.*, James Ball, *Silk Road: The Online Drug Marketplace That Officials Seem Powerless To Stop*, GUARDIAN, Mar. 22, 2013, http://www.theguardian.com/world/2013/mar/22/silk-road-online-drug-marketplace.

[207] Nate Anderson & Cyrus Farivar, *How the Feds Took Down the Dread Pirate Roberts*, ARS TECHNICA (Oct. 3, 2013, 12:00 AM), http://arstechnica.com/tech-policy/2013/10/how-the-feds-took-down-the-dread-pirate-roberts.

[208] Sean Gallagher, *Alleged Tor Hidden Service Operator Busted for Child Porn Distribution*, ARS TECHNICA (Aug. 4, 2013, 4:00 PM), http://arstechnica.com/tech-policy/2013/08/alleged-tor-hidden-service-operator-busted-for-child-porn-distribution.

[209] Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013, 4:17 PM), http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi.

[210] *See, e.g.*, Danezis, Diaz & Syverson, *supra* note 198, at 367–69.

[211] Fung et al., *supra* note 84.

come as a surprise to the privacy research community, as the attacks had already been independently discovered and published by academic researchers and were thus publicly known. In fact, in several instances the attacks and vulnerabilities known to the academic research community appear to be more sophisticated than those actually considered by the NSA. The Tor Project notes in its blog,

> Despite the understandable concern provoked among users by these disclosures, Tor developers themselves were encouraged by the often relatively basic or out-of-date nature of the attacks described. In response to one journalist's request for comment, Roger Dingledine wrote that "we still have a lot of work to do to make Tor both safe and usable, but we don't have any new work based on these slides."[212]

D. *Policy Implications*

Information privacy law applies obligations mainly to data controllers. Hence, the policy implications of the foregoing debate depend on the relevant category of PETs, which corresponds to the degree of engagement by a data controller.

With respect to the first category, consisting of PETs that require adoption by a data controller, policymakers should *incentivize* and in appropriate cases *require* implementation of PETs into the design of infrastructures, products, and services. This should be viewed as appropriate application of the principle of "Privacy by Design."[213] In cases where PETs can enhance individuals' privacy without sacrificing any of the functionalities and stated, i.e., primary, goals of the data controller, they should be mandated.[214] This is particularly the case in the context of infrastructures that are effectively mandatory for individuals, i.e., where the service provider enjoys monopoly power either *de jure*—as in the case of utilities, highways, and voting systems—or *de facto*—as in the case of the mobile infrastructure.

To be sure, some Big Data evangelists would argue that *more data* is always better, if only for reasons to be determined at a later date; in which case *any* data minimization could be viewed as sacrificing potential future benefit. Yet, surely such a view is more religious than it is scientific. As Julie Cohen

---

[212] *Tor Weekly News—October 9th, 2013*, TOR BLOG, (Oct. 9, 2013), https://blog.torproject.org/blog/tor-weekly-news-—-october-9th-2013.

[213] *See* Gürses, Troncoso & Diaz, *supra* note 36, at 2–8. Promotion, or indeed even recognition of PETs is conspicuously missing from the policy debate, even in Europe, where the Article 29 Working Party, which has issued dozens of opinions on the application of data protection law, has so far failed to attempt a full survey or exposition of PETs. *See* Caspar Bowden, From PETs to Privacy Engineering (Apr. 24, 2013) (presentation at the Privacy Platform in Brussels) (presentation on file with author).

[214] *See* Jonathan Mayer & Arvind Narayanan, *Privacy Substitutes*, 66 STAN. L. REV. ONLINE 89 (2013), http://www.stanfordlawreview.org/sites/default/files/online/topics/66_SLR_89_MayerNarayanan.pdf.

puts it: "[S]ome of the claims on behalf of Big Data, those framed in terms of a 'singularity' waiting in our soon-to-be-realized future, sound quasi-religious, conjuring up the image of throngs of dyed-in-the-wool rationalists awaiting digital rapture."[215]

Suffice it to say that the jury is still out with respect to the efficiency and efficacy of a "collect it now, decide what to do with it later" approach, as opposed to more conventional data collection practices. It remains to be proven that unbarred collection is an effective strategy, much less a cost-effective one, accounting not only for big data rewards, but also for attendant privacy risks. Indeed, there is no inherent reason that big data practices cannot benefit from employing the same principles that inform PETs, namely data minimization, avoiding a single point of failure, and opening the algorithms to public scrutiny.

In fact, researchers can, or are, already looking into the application of these design principles in big data scenarios. This includes, for example, studying the marginal benefit of collection and processing of certain attributes for personalization relative to the risks accrued, where similar personalization can be offered with much less data collection. Further, researchers are already exploring ways of opening big data algorithms to scrutiny, especially with respect to re-identification of individuals, discrimination, and fairness.[216] These research efforts may eventually mitigate some of the risks associated with big data to help develop accountable and more democratically organized models of data collection and processing.

The role of government and regulation in promoting PET innovation is particularly important where businesses would have to incur costs in order to introduce privacy-friendly services. As discussed above, current technological architectures often permit "surveillance by default, privacy by effort,"[217] and businesses see little benefit in implementing costly mechanisms that are not duly understood and acknowledged by consumers. For businesses to listen, consumers need to not only know and understand the benefits of PETs, but also to threaten to revolt or leave the system en masse if privacy protective mechanisms are not provided.[218]

PETs seek to "restore" the previous balance common in the "analogue world" of private by default, public—and therefore available for surveillance—by sometimes insurmountable effort. Similarly, regulatory intervention is warranted where intrusive systems create additional revenue streams and

---

[215] Julie E. Cohen, *What Privacy Is For*, 126 HARV. L. REV. 1904, 1922 (2013).

[216] *Id.* at 1932.

[217] danah boyd, Making Sense of Privacy and Publicity, Keynote Address at SXSW, Austin, Tex. (Mar. 13, 2010) ("Historically, a conversation that you might have in the hallway is private by default, public through effort . . . . Conversely, when you engage online in equally public settings such as on someone's Facebook Wall, the conversation is public by default, private through effort.").

[218] *See* Cuijpers & Koops, *supra* note 118, at 270. For a discussion of political dissent in Israel against the creation of a national biometric scheme, see *Who We Are*, NO2BIO.ORG, http://no2bio.org/about.

business opportunities, further disincentivizing privacy innovation. This is particularly the case in monopolistic or oligopolistic markets, where the relevant players do not compete on privacy, or at all. At the same time, it takes two to tango: governments themselves benefit from businesses' data collection zeal. In fact, where businesses fail to maximize their collection potential, governments are known to *compel* them to collect and retain consumers' information.[219]

In order to draw the information privacy framework closer to first principles and constitutional doctrine, PETs should be deployed far more extensively than they are today. Should government be interested in promoting PETs, it would have multiple ways to "nudge" business, including through requirements in bids for government contracts, provision of privacy compliance safe harbors, and integration into data protection regulation. Similarly, public sector institutions could be required to adopt PETs, at least in areas monopolized by the government.

The second category includes PETs that are utilized by a user to access a service offered by a data controller. Here, policymakers should *discourage*, or in appropriate cases, *prevent the blocking of or tampering with PETs* by the controller. One argument data controllers raise to defend self-imposed restrictions on PETs is that they are bad for business. Yet, various regulatory tools such as competition law—in highly concentrated markets[220]—or the doctrine of unfairness (under the FTC's Section 5 authority in the United States[221] or standard form contract law in the EU[222]) may help fend off such claims. As long as the data minimization principle is not written off, consumers should have a right to restrict the extent of data they share with service providers to the minimum amount necessary for conducting a transaction.

To take one example, search engines have strong incentives to block TrackMeNot.[223] The use of dummy queries not only makes them consume ("waste"[224]) resources; but it also "pollutes" their databases of profiles with "noise," devaluing their quality and consequently diminishing the effectiveness at targeted advertising, which is an important element of their business

---

[219] *See, e.g.*, Council Directive 2006/24/EC of 15 March 2006 on the Retention of Data Generated or Processed in Connection with the Provision of Publicly Available Electronic Communications Services or of Public Communications Networks and Amending Directive 2002/58/EC, 2006 O.J. (L 105) 54, 57.

[220] The markets for Internet service providers and online social networking services are two conspicuous, and highly relevant, examples.

[221] Daniel J. Solove & Woodrow Hartzog, The FTC and the New Common Law of Privacy 29, 35 (Aug. 15, 2013) (unpublished manuscript) (on file with author).

[222] *See* Annick De Boeck & Mark Van Hoecke, *The Interpretation of Standard Clauses in European Contract Law*, *in* STANDARD CONTRACT TERMS IN EUROPE: A BASIS FOR AND A CHALLENGE TO EUROPEAN CONTRACT LAW 201, 225–26 (Hugh Collins ed., 2008).

[223] *See* Howe & Nissenbaum, *supra* note 162 and accompanying text.

[224] Different stakeholders may however have different views as to what constitutes "waste." Privacy-conscious users may consider consuming network resources (e.g., bandwidth) to protect their privacy as justified both morally and economically.

model.[225] In response to these criticisms, Nissenbaum argues that PETs such as TrackMeNot are legitimate as a "weapon of the weak," given the asymmetries of power and knowledge between controllers and users.[226] Users have few options to protect themselves from profiling other than using PETs such as TrackMeNot or Tor as legal protections are weak and opt-out mechanisms complex and unreliable.

Controllers can forbid in their terms of service the use of PETs that provide content encryption, anonymous access, or data obfuscation. Nissenbaum argues, though, that the law should authorize users to violate unfair terms of service, which are unilaterally imposed contracts of adhesion.[227] Thus, the use of such PETs may be viewed as a form of civil disobedience that expresses discontent with respect to existing profiling and surveillance practices.

With respect to the third category of PETs, consisting of collaborative applications without a central data controller, policymakers should protect the ability of individuals to work together to fend off surveillance. At the very least, such PETs should not be made illegal.[228]

Data controllers can stifle the use of such PETs through restrictions in their terms of service, changes to APIs, traffic management, and more. They often justify such disruptions based on a common view of PET users being inherently suspicious of untoward activity, i.e., individuals who have "something to hide."[229] Yet this is just another facet of the "nothing to hide" argument, which has been dispelled time and again in privacy literature.[230] Not only terrorists and pedophiles have "something to hide."[231] So do human rights activists, dissidents and—more generally—privacy-aware individuals who are increasingly concerned about being monitored, profiled, and singled out for unique treatment by algorithmic machines.[232] With privacy protected as a fundamental human right in Europe and recognized as a building block of a free society in the United States, the depiction of privacy-aware individuals as potential criminals is perverse. To be sure, some wrongdoers will seek to take

---

[225] *See, e.g.*, Finn Brunton & Helen Nissenbaum, *Political and Ethical Perspectives on Data Obfuscation*, *in* PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN: THE PHILOSOPHY OF LAW MEETS THE PHILOSOPHY OF TECHNOLOGY 171, 185–188 (Mireille Hildebrandt & Katja de Vries eds., 2013).

[226] *See* Nissenbaum, *supra* note 138.

[227] *See id.*

[228] *But see* Ian Steadman, *Japanese Police Ask ISPs To Start Blocking Tor*, ARS TECHNICA (Apr. 21, 2013, 3:00 PM), http://arstechnica.com/tech-policy/2013/04/japanese-police-ask-isps-to-start-blocking-tor.

[229] *See* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394–96 (1978).

[230] *See* DANIEL SOLOVE, NOTHING TO HIDE: THE FALSE TRADEOFF BETWEEN PRIVACY AND SECURITY 21–32 (2011).

[231] For a recent discussion of this topic, see danah boyd, *If You're OK with Surveillance Because You Have "Nothing To Hide," Think Again*, SLATE (June 11, 2013, 11:14 AM), http://www.slate.com/blogs/future_tense/2013/06/11/prism_scandal_the_problem_with_nothing_to_hide_and_surveillance.html.

[232] Tene & Polonetsky, *supra* note 29.

advantage of privacy protections, but we do not bring mass transit systems to a halt simply because they sometimes transport criminals or contraband. Similarly, it would be disproportionate to discredit PETs for the transgressions of a few.

Moreover, it is untenable to require PET developers to build surveillance-ready backdoors into the technology's design. Such backdoors would defeat the very purpose of PETs, which is to protect individuals from surveillance. Worse yet, they would undermine the security and trust in information communications technology and open the door not only to law enforcement agencies but also to unintended government, business or individual intruders.[233] In a similar vein, application of data retention requirements to anonymous systems such as Tor would render such systems useless. Here too, strong stakeholders will argue that toughening PETs is a boon to terrorists and criminals. Such arguments, however, have already been raised—and ultimately discarded—in the context of the "crypto wars" of the 1990s.[234]

VI. CONCLUSION

Constitutional privacy protections treat centralized power with distrust and require effective checks, balances, and safeguards against government surveillance. Over the past two decades, as individuals' daily lives have become increasingly mediated by technologies, government institutions have enhanced their surveillance powers through tightening collaboration with private sector entities, to create a "surveillant assemblage." Findings about the extent of government and private sector surveillance have recently reached the zenith with the constant drumbeat of revelations about the NSA and GCHQ.

Information privacy law, a legal framework arising in the 1970s to protect individuals' data privacy, provides little protection against such surveillance risks. This relatively new legal framework bridges two distinct trust paradigms: one assuming that data controllers are *trusted entities*, the other assuming that, in a similar vein to the constitutional framework, data controllers should be treated with suspicion and distrust. Over the past few years, the legal framework has shifted from focusing on data minimization, a cornerstone of the untrusted controller model, to imposing information stewardship obligations on data controllers who are increasingly viewed as custodians of individuals' rights. These obligations, typically grouped under the title "accountability," are based on a notion of the data controller as a trusted party.

In stark contrast, the technological community researching PETs proceeds from a diametrically opposed perception of a data controller, that of an adversary. Under this approach, information disclosed to a data controller is compromised and can no longer be viewed as private, given that a data controller itself may subject individuals to persistent surveillance.

---

[233] *Supra* notes 49–50 and accompanying text.

[234] PHILIP R. ZIMMERMANN, THE OFFICIAL PGP USER'S GUIDE 5–7 (1995).

This Article argues that the emergence and growth of the surveillant assemblage, particularly in light of recent revelations, heightens the importance of the untrusted controller paradigm for information privacy law. The law should not assume that data controllers are trustworthy; rather, it should promote—or at the very least not prevent—the deployment of PETs, defined as technological privacy solutions that combine three principles: elimination of the single point of failure inherent with any centralized trusted party; data minimization; and subjecting protocols and software to community based public scrutiny.

To better tailor this policy recommendation to real world scenarios, this Article proposes a categorization of PETs based on the role of the data controller, who is the focal point for application of information privacy law. The first category would include PETs that require active implementation by a data controller. Here, policymakers should incentivize and, in appropriate cases, require implementation of PETs into the design of infrastructures, products, and services. This should be the case particularly in monopolistic or oligopolistic markets or services provided by the public sector, where there is little competition on the basis of privacy.

The second category consists of client-side software deployed by a user to access a service offered by a data controller. Here, policymakers should discourage, or in appropriate cases prevent the blocking of or tampering with PETs by the controller. This should be the case even where businesses argue that PETs interfere with their business models or lay costly resources to waste. PETs should be viewed as a "weapon of the weak," providing individuals with minimal capabilities necessary to assert their legal and constitutional protections.

The third category consists of PETs that are collaborative applications without a data controller, such as the Tor network. At the very least, such PETs should not be made illegal. Optimally, service providers should be required to interact with PETs' users without blocking or delegitimizing their privacy choices through restricted APIs or unilaterally imposed contractual terms. In addition, PET developers should not be compelled to build surveillance-ready backdoors into the technology's design or to comply with data retention requirements, as such obligations would render the PETs unusable.

The information privacy framework can use PETs to refocus on the core concerns that have led to its introduction into legislation across the globe, after decades of ominous government data abuses leveraged to persecute citizens, minorities, and political dissidents.