Maryland Law Review

Volume 76 | Issue 4 Article 7

In Defense of the Long Privacy Statement

Mike Hintze

Recommended Citation
76 Md. L. Rev. 1044 (2017)

IN DEFENSE OF THE LONG PRIVACY STATEMENT

MIKE HINTZE*

INTRODUCTION

Size matters. In fact, when it comes to privacy statements, there is an obsession with size. Much scholarship and commentary on privacy statements bemoan the fact that consumers rarely read them and place the blame on the length of those statements. The solution? Shorten and simplify!

Proposals for standardized short-form notices, "nutrition label" notices, icons, and other attempts to replace long privacy statements abound. But none of these proposals have proven to be a satisfactory substitute for a full, detailed description of what data an organization collects and how it is used, shared, retained, and protected. These short-form approaches inevitably leave out important details, gloss over critical nuances, and simplify technical information in a way that dramatically *reduces* transparency and accountability.

This Essay discusses the multiple purposes of privacy statements,[1] including the legal obligations they are designed to fulfill. It recognizes that

---

* Partner, Hintze Law PLLC. Part-time Professor, University of Washington School of Law. Formerly, Chief Privacy Counsel, Microsoft Corporation. The views expressed in this Essay are my own and do not necessarily reflect the positions of any current or former employer or client. I would like to thank the following people for their feedback and advice: Tobias Bräutigam, Ryan Calo, Susan Freiwald, Woodrow Hartzog, Susan Lyon-Hintze, Sjoera Nas, Neil Richards, Ira Rubinstein, Emily Schlesinger, the participants in the October 2015 workshop on this Essay at the Privacy Law Scholars Conference in Amsterdam, Netherlands, and the staff of the *Maryland Law Review*.

1. This Essay uses the term "privacy statement," rather than "privacy policy" or "privacy notice." While all three terms are commonly used to describe the type of document that is the focus of this Essay, the terms "privacy policy" and "privacy notice" are less specific and can lead to confusion. For instance, the term "privacy policy" is also frequently used to refer to an organization's set of internal policies and guidelines that govern personal data. This internal policy is typically focused on principles and rules that internal personnel use to guide product design and data management practices. By contrast, the external "privacy statement" is in large part a factual document that describes in detail how that internal policy has been applied to specific products or activities. To take one example, an organization's internal policy may state it should not collect more personal data than it needs to operate its business and provide its services. The policy may further require internal teams to document and justify their data collection practices. But the privacy statement will provide the facts regarding what data types are collected and how they are used. In other words, a privacy statement reflects the organization's internal *policy*, but also provides a detailed factual *statement* of how those policies are applied in practice. Thus, using the term "privacy statement" more accurately reflects what the document is, and it avoids the confusion inherent in using the same term to describe both internal and external documents. Likewise, the

there are many audiences for privacy statements, including consumers, regulators, policymakers, academics, researchers, investors, advocates, and journalists. Further, this Essay argues that efforts to make privacy statements significantly shorter and simpler only optimize these statements for the one audience least likely to read them—consumers—rather than the audiences in the best position to police privacy statements and the practices they describe.

Whatever the audience, a detailed (long) privacy statement increases transparency by providing a single place where an interested reader can find the "full story" of an organization's privacy practices. Unlike many alternate methods of providing notice, a detailed privacy statement makes the full range of privacy information available at any time and to any person—before, during, or after the time an individual uses an organization's products or services.

Long privacy statements also create organizational accountability. The exercise of drafting a privacy statement requires organizations to conduct a detailed investigation of its own practices to fully understand and document what data is being collected and how it is processed. Although few consumers, other than a small number of highly motivated individuals, will read privacy statements, those who act on behalf of consumers—advocates, regulators, and journalists—do read them. It is mainly those advocates, regulators, and journalists who ask the hard questions when a privacy statement is unclear or incomplete and are in a position to raise public awareness and create consequences when an organization has inadequate or problematic privacy practices. And, it is that kind of accountability that leads to positive change.

To be clear, this Essay is not defending long privacy statements that are poorly drafted. Writing that is unclear, poorly organized, or needlessly complex or legalistic has no place in a privacy statement. Nor is this Essay suggesting we should write off consumers because they rarely read privacy statements, regardless of the length. If we want to achieve transparency for all audiences, long privacy statements are necessary, but often not sufficient. Additional efforts should be made to help consumers understand what is being done with their data and to give them meaningful control.[2] But, such measures almost always will be inadequate and incomplete, unless provided in conjunction with a full, detailed privacy statement.

---

term "privacy notice" can be used to refer to many types of notices. Products or services may provide specific privacy-related details to consumers in a piecemeal way in the user interface. *See infra* Part III.E (discussing contextual or just-in-time notices). Thus, users may see many privacy *notices* as they interact with a product or service. By contrast, the privacy *statement* is the comprehensive document that gathers all the essential privacy-related information in a single place.

2. Helping consumers understand often involves measures in addition to a detailed privacy statement, such as contextual privacy disclosures. See Part III.E of this Essay for a discussion of just-in-time or contextual privacy notices.

Similarly, while long privacy statements are often essential to achieving true transparency, a privacy statement should not be long simply for the sake of being long. A privacy statement for a simple app that collects one type of information and uses it for one purpose can be quite short. But, a privacy statement for an organization that offers a range of more complex, interrelated, and data-intensive services often must be quite long in order to provide all the relevant details. How long should a privacy statement be? A privacy statement should be as long as it needs to be to meet legal requirements and provide full descriptions of the pertinent data practices.

Part I of this Essay describes the many statutory, self-regulatory, contractual, and other legal and quasi-legal elements that can be required as part of a privacy statement, which necessarily result in a lengthy document. Part II describes and analyzes common criticisms of long privacy statements. Part III critiques several alternative proposals and explains why they are inadequate substitutes for a detailed privacy statement. Part IV discusses the several privacy benefits that result from organizations drafting and publishing long privacy statements—principally increased transparency and accountability. Finally, Part V describes ways in which privacy statements can be improved without sacrificing the transparency and accountability that come from a detailed privacy statement.

I. COMMONLY REQUIRED ELEMENTS OF A PRIVACY STATEMENT

Privacy statements, at a minimum, must meet the legal obligations to which the organization is subject. These obligations can arise from statutory requirements, self-regulatory programs, contractual provisions, and other sources. In most cases, an organization will be subject to many different sets of overlapping obligations. Requirements arising from different sources may be similar, but not identical. As a result, organizations need to compile and reconcile many requirements, and draft a privacy statement that meets all of them.

A. Statutory Obligations

Privacy laws around the world create privacy statement obligations. As a result, regulatory compliance will compel most organizations that collect or process personal data to have a privacy statement of some kind. Simply meeting legal obligations can increase the length of a privacy statement dramatically. The more jurisdictions in which an organization acts, the more specific privacy statement requirements will apply. These requirements can add up, leading to longer and longer privacy statements.

In the United States, there is no generally applicable federal privacy law that mandates privacy statements. But, several sectoral laws do, as do a number of state privacy laws. One of the most significant laws in this regard

is the California Online Privacy Protection Act ("CalOPPA"), which requires nearly every website and online service post a privacy statement.[3] Specifically, it requires the posting of a privacy policy by every website and online service that collects "personally identifiable information" from a consumer residing in California.[4] Although the definition of "personally identifiable information" under CalOPPA may not be as broad as some definitions of personal data,[5] any website or online service that has even a possibility of a California resident providing one of these types of data (which could be obtained through enabling registration, newsletter sign-up, or customer support contact via email) could find itself subject to these obligations.[6] And, its impact extends well beyond California, since it applies to any website, anywhere, to which a California resident can provide data.[7]

CalOPPA requires a privacy statement that includes several different elements. A compliant privacy statement must include at least:

- The "categories of personally identifiable information" collected via the website or online service;
- The types of third-parties with which the personally identifiable information may be shared;
- Information about whether an operator of the website or online service has established a process for a consumer to review or edit his or her personally identifiable information and, if so, a description of such process;
- Information regarding how individuals will be notified of a material change to the privacy statement;
- A description of how (or whether) the website or online service responds to "do-not-track" signals or similar mechanisms;

---

3. CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2008).

4. *Id.* § 22575(a).

5. *Id.* § 22577(a). "Personally identifiable information" is defined as:

> [I]ndividually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form, including any of the following: (1) A first and last name. (2) A home or other physical address, including street name and name of a city or town. (3) An e-mail address. (4) A telephone number. (5) A social security number. (6) Any other identifier that permits the physical or online contacting of a specific individual[, and] (7) Information concerning a user that the Web site or online service collects online from the user and maintains in personally identifiable form in combination with an identifier described in this subdivision.

Id. § 22577(a)(1)–(7). *Compare id.* § 22577(a), *with* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 72–102 (2012) (providing a broader concept of data subject to its privacy framework). European privacy law also defines "personal data" broadly. *See* Council Regulation 2016/679, art. 4(1), 2016 O.J. (L 119) 33 (EU).

6. CAL. BUS. & PROF. CODE § 22576.

7. *Id.* § 22577(c).

- Information about whether third parties may collect, through the website or online service, personally identifiable information about an individual's online activities over time and across different websites; and,
- The effective date of the privacy statement.[8]

At the federal level, the United States has several privacy laws that require privacy statements for certain business activities and types of data collection. For example, if a website or online service collects information from children, it is likely subject to the Children's Online Privacy Protection Act ("COPPA").[9] COPPA requires every website that is directed to children under the age of thirteen, or that knowingly collects personal information from such children, to post a privacy statement.[10] The regulations implementing COPPA[11] require that such a privacy statement include: "The name, address, telephone number, and email address of [the organization(s) that] collect[] or maintain[] personal information from children through the Web site or online service."[12] Additionally, the organization must provide a description of:

- "What information the [organization(s)] collects from children,"
- "Whether the Web site or online service enables a child to make personal information publicly available,"
- "How the operator uses such information[,] and, the operator's disclosure practices for such information;"
- A disclosure "that the parent can review or have deleted the child's personal information," and a description of how to do so; and,
- A disclosure "that the parent can refuse to permit further collection or use of the child's information," and a description of how to do so.[13]

Other U.S. federal privacy laws require additional privacy statement disclosures. For example, companies that meet the broad definition of "financial institution" under the Gramm-Leach-Bliley Act ("GLBA")[14] must provide a privacy notice to their customers.[15] These notices must be provided

8. *Id.* § 22575(b).

9. Children's Online Privacy Protection Act of 1998, Pub. L. No. 105-277, 112 Stat. 2681 (codified at 15 U.S.C. §§ 6501–6506 (2012)).

10. 15 U.S.C. §§ 6501, 6502.

11. 16 C.F.R. §§ 312.1–312.13 (2016).

12. *Id.* § 312.4(d)(1).

13. *Id.* § 312.4 (d)(2)–(3).

14. 15 U.S.C. §§ 6801–6809 (2012).

15. *Id.* § 6803.

at the time the customer relationship is established and on an annual basis thereafter, for as long as the customer relationship continues.[16] Privacy notices must include a description of:

- The types of nonpublic personal information the financial institution collects;
- The categories of such information (about both current and former customers) the financial institution discloses;
- The categories of third parties (affiliated and nonaffiliated) to which such disclosures are made (subject to certain exceptions);
- The consumer's right to opt out of certain disclosures of such "information to *nonaffiliated* third parties, including the method(s) by which the consumer may exercise that right" (subject to several exceptions);
- Any disclosures of information among *affiliates*, and a notice regarding the ability to opt out of such disclosures;
- Any information disclosed to service providers and joint marketing partners with which the financial institution has contracted from which the individual cannot opt-out;
- Any information disclosed to third parties for "everyday business purposes, such as to process transactions, maintain account(s), respond to court orders and legal investigations, or report to credit bureaus" from which the individual cannot opt-out;
- The financial institution's "policies and practices with respect to protecting the confidentiality and security of nonpublic personal information"; and,
- Any other information the financial institution wishes to provide.[17]

Another example of a U.S. privacy law that imposes specific privacy statement requirements on organizations in a particular industry sector can be found in the privacy provisions of the Health Insurance Portability and Accountability Act ("HIPAA").[18] For covered entities in the health care industry, their privacy statements must include descriptions (with examples) of the organization's uses and disclosures of protected health information.

16. 16 C.F.R. §§ 313.4, 313.5.

17. *Id.* § 313.6. In this Essay, the citations for the privacy rules implementing GLBA refer to the regulations promulgated by the Federal Trade Commission ("FTC"). Several agencies are responsible for implementing and enforcing GLBA. Each of the agencies has separately promulgated regulations implementing the privacy provisions of GLBA, but have done so in a coordinated way so that the rules are consistent (and in most cases, identical).

18. 42 U.S.C. §§ 1320d–1320d-9 (2012). The HIPPA Privacy Standards implementing the privacy provisions of HIPPA are codified at 45 C.F.R. §§ 164.500–164.534 (2016).

Additionally, the statement must comply with more than a dozen additional requirements—many unique to HIPAA—including very detailed requirements to include specific text at the top of the document and to describe certain rights of the individual, specific duties of the covered entity, and how to file a complaint.[19]

Around the world, privacy statement requirements are ubiquitous. In Australia, for example, the Privacy Act 1988[20] imposes specific requirements for what to include in a privacy statement. The substantive requirements are set out in the Australian Privacy Principles ("APP") contained in schedule 1 of the Act. APP 1, regarding the "open and transparent management of personal information," lists the following seven items that must be in a published privacy statement:

(a) The kinds of personal information that the entity collects and holds;
(b) How the entity collects and holds personal information;
(c) The purposes for which the entity collects, holds, uses and discloses personal information;
(d) How an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
(e) How an individual may complain about a breach of the Australian Privacy Principles, or a registered APP code (if any) that binds the entity, and how the entity will deal with such a complaint;
(f) Whether the entity is likely to disclose personal information to overseas recipients; and
(g) If the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the policy.[21]

APP 5, regarding "notification of the collection of personal information," lists several additional disclosures that must be provided to an individual when data is collected.[22] One way to achieve the APP notification is to include the required disclosures in the published privacy statement.[23] As a practical matter, a privacy statement will typically cover both the APP 1

19. 45 C.F.R. § 164.520(b)(1).
20. *Privacy Act 1988* (Cth) (Austl.).
21. *Id.* pt 1 s 1.4.
22. *Id.* pt 2 s 5.
23. *See Chapter 5: APP 5—Notification of the Collection of Personal Information*, OFFICE OF THE AUSTRALIAN INFO. COMM'R, https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information (last visited May 17, 2017).

and APP 5 requirements. As set forth in the Act, these additional disclosures include:

(a) The identity and contact details of the entity;
(b) If:
(i) the APP entity collects the personal information from someone other than the individual; or
(ii) the individual may not be aware that the APP entity has collected the personal information;
the fact that the entity so collects, or has collected, the information and the circumstances of that collection;
(c) If the collection of the personal information is required or authorised by or under an Australian law or a court/tribunal order—the fact that the collection is so required or authorised (including the name of the Australian law, or details of the court/tribunal order, that requires or authorizes the collection);
(d) The main consequences (if any) for the individual if all or some of the personal information is not collected by the APP entity;
(e) Any other APP entity, body or person, or the types of any other entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected by the entity . . . .[24]

In contrast, under Canada's Personal Information Protection and Electronic Documents Act ("PIPEDA"),[25] organizations must make available information including:

(a) The name or title, and the address, of the person who is accountable for the organization's policies and practices and to whom complaints or inquiries can be forwarded;
(b) The means of gaining access to personal information held by the organization;
(c) A description of the type of personal information held by the organization, including a general account of its use; . . .
(d) [O]ther information that explain the organization's policies, standards, or codes; and
(e) What personal information is made available to related organizations (e.g., subsidiaries).[26]

While this information could be provided to individuals in different ways, PIPEDA requires that it be accessible "without unreasonable effort,"[27]

24. *Privacy Act 1988* (Cth) pt 2 cl 5.2 (Austl.).
25. Personal Information Protection and Electronic Documents Act, S.C. 2000, c 5 (Can.).
26. *Id.* sch 1 cl 4.8.2.
27. *Id.* sch 1 cl 4.8.1.

and the common practice is to provide these details through a privacy statement.

In Europe, the 1995 Data Protection Directive requires individuals to be informed of the purposes for which personal data about them is being processed.[28] "Processing" is defined broadly, and includes any collection, use, or sharing of personal data.[29] Other specific requirements for privacy statements include "the identity of the data controller,"[30] "the recipients or categories of recipients of the data" (if any),[31] and "the existence of [a] right of access" and rectification regarding the data.[32] Some data protection authorities in individual EU member states have provided additional guidance on what to include in a privacy statement.[33]

The requirements of the recently-enacted General Data Protection Regulation ("GDPR")[34] will replace those enacted under the EU Data Protection Directive when the GDPR becomes enforceable in May 2018. Compared to the 1995 Data Protection Directive, the GDPR imposes much more extensive obligations on organizations with respect to the specific information they are required to provide to individuals. This information includes:

- "The identity and the contact details of the controller and, where applicable, of the controller's representative"[35];
- "The contact details of the data protection officer, where applicable"[36];
- Where personal data is obtained from a source other than the data subject:
    - The types of personal data obtained,[37] and

28. Council Directive 95/46, arts. 10–11, 1995 O.J. (L 281) (EU) 31, 41–42.

29. *Id.* art. 2(b), at 38 ("'[P]rocessing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction[.]").

30. *Id.* art. 10(a), at 41.

31. *Id.* art. 10(c), at 41.

32. *Id.*

33. *See, e.g.*, INFORMATION COMMISSIONER'S OFFICE, PRIVACY NOTICES, TRANSPARENCY, AND CONTROL: A CODE OF PRACTICE ON COMMUNICATING PRIVACY INFORMATION TO INDIVIDUALS (2016), https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/.

34. Council Regulation 2016/679, 2016 O.J. (L 119) (EU) 1.

35. *Id.* arts. 13(1)(a), at 40, 14(1)(a), at 41.

36. *Id.* arts. 13(1)(b), at 40, 14(1)(b), at 41. See *id.* art. 37, at 55, for the requirements for designating a data protection officer.

37. *Id.* arts. 14(1)(d), at 41, 15(1)(b), at 43.

- The source(s) "from which the personal data originate, and if applicable, whether it came from publicly accessible sources"[38];

Where the personal data is collected from the data subject, the organization, in some circumstances, must notify the subject whether collecting the data is required, including:

- Whether it is a "requirement necessary to enter into a contract"[39];
- Whether it is otherwise required by statute or contract[40];
- The "possible consequences of failure to provide such data"[41];
- The intended purposes of processing the personal data[42];
- The legal basis for the processing[43];
- Where the legal basis for processing is "the legitimate interests pursued by the controller or a third party under Article 6(1)(f)," a description of those interests[44];
- Where the legal basis for processing is "the consent of the data subject under Articles 6(1)(a) or 9(2)(a), the existence of the right to withdraw such consent at any time" (which will not affect the lawfulness of any processing that occurred before such consent is withdrawn)[45];
- Where personal data is used for automated decisionmaking, including profiling, referred to in Article 22(1) and (4), the existence of such processing, meaningful information about the logic involved, and the significance of the processing and any anticipated consequences for the data subject[46];
- "The recipients or categories of recipients of the personal data, if any"[47];
- "The period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period"[48];

38. *Id.* arts. 14(2)(f), at 42, 15(1)(g), at 43; *see also id.* Recital 61, at 12 ("Where the origin of the personal data cannot be provided to the data subject because various sources have been used, general information should be provided.").

39. *Id.* art. 13(2)(e), at 41.

40. *Id.*

41. *Id.*

42. *Id.* arts. 13(1)(c), at 40, 14(1)(c), at 41, 15(1)(a), at 43.

43. *Id.* arts. 13(1)(c), at 40, 14(1)(c), at 41; *see also id.* art. 6, at 36 (listing the legal bases for processing personal data).

44. *Id.* arts. 13(1)(d), at 41, 14(2)(b), at 42.

45. *Id.* arts. 13(2)(c), at 41, 14(2)(d), at 42.

46. *Id.* arts. 13(2)(f), at 41, 14(2)(g), at 42, 15(1)(h), at 43.

47. *Id.* arts. 13(1)(e), at 41, 14(1)(e), at 41, 15(1)(c), at 43.

48. *Id.* arts. 13(2)(a), at 41, 14(2)(a), at 42, 15(1)(d), at 43.

- The existence of the right of a data subject to:
    - Request from the controller "access to and rectification or erasure of personal data"[49]; or,
    - Object to the processing of personal data or obtain a restriction of such processing under certain circumstances[50];
- Receive data he or she has provided to the controller in a structured, commonly used and machine-readable format, and transmit that data to another controller (data portability)[51];
- "The right to lodge a complaint with a supervisory authority"[52]; and,
- Where the controller intends to transfer personal data to a third country or international organization, the fact of such transfer and either:
    - "The existence or absence of an adequacy decision by the [European] Commission," or
    - In the case of transfers based on "suitable safeguards" under Articles 46, 47, or 49(1)(b) (such as contractual provisions or binding corporate rules), a description of such safeguards and how to obtain a copy of them.[53]

There are many other jurisdictions that have privacy laws on the books that require some kind of privacy statement. While some requirements are similar across different statutes, each statute is unique. Those drafting privacy statements must take care to ensure that the text of the statement meets the requirements of every statute that could apply. Thus, simply meeting the baseline statutory legal obligations for a privacy statement can result in a very long document—particularly if the privacy statement applies

49. *Id.* arts. 13(2)(b), at 41, 14(2)(c), at 42, 15(1)(e), at 43; *see also id.* art. 15, at 43 (right of access), art. 16, at 43 (right to rectification), art. 17, at 43–44 (right to erasure).

50. *Id.* arts. 13–15, at 41–43. The right to object applies to processing based on Article 6(1)(e) ("necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller") or Article 6(1)(f) ("necessary for the purposes of the legitimate interests pursued by the controller or by a third party"), or for the purposes of marketing. *Id.* arts. 6(1)(e)–(f), at 36, art. 21(1)–(2), at 45. The right to obtain a restriction on processing applies under four narrow circumstances described in Article 18(1). *See id.* at 44. An organization may choose to specify these circumstances in its privacy statement in order to avoid implying a broader right to object or restrict processing than is provided by the GDPR.

51. *Id.* art. 12(7), at 40. See also *id.* art. 20, at 45, for the scope of the data portability obligations.

52. *Id.* arts. 13(2)(d), at 41, 14(2)(e), at 43, 15(1)(f), at 43.

53. *Id.* arts. 13(1)(f), at 41, 14(1)(f), at 42; *see also id.* art. 15(2), at 43.

to a company that operates across multiple jurisdictions or offers products or services available in multiple jurisdictions.[54]

B. Self-Regulatory and Other "Voluntary" Standards

In addition to statutory requirements, many organizations may find themselves subject to a variety of self-regulatory standards that impose additional requirements on their privacy statements. There are many different types of self-regulatory programs, from privacy seal programs to industry associations standards, to the optional EU-U.S. Privacy Shield framework governing trans-North Atlantic data transfers. And while all participation is voluntary, many organizations may feel compelled to join for a variety of reasons.[55]

A detailed set of privacy statement requirements will apply if an organization participates in the recently-negotiated EU-U.S. Privacy Shield. The EU-U.S. Privacy Shield is an agreement between the European Commission and the U.S. Department of Commerce necessitated by the provisions of European data protection law that restrict transfers of personal data to jurisdictions with laws that do not provide an adequate level of data protection, as determined by the European Commission. In a 2016 decision, the European Commission found that the "United States ensures an adequate level of protection for personal data transferred under the EU-U.S. Privacy Shield from the Union to self-certified organizations in the United States."[56] Under the EU-U.S. Privacy Shield, U.S. organizations can self-certify their adherence to the Privacy Shield Principles, enabling it to receive data transfers based on the European Commission's finding that the Principles

54. It is worth noting that legal obligations regarding privacy statements include more than just the items that must be included in a notice. Some laws attempt to mandate standards of clarity. For example, the GDPR requires that information be provided "in a concise, transparent, intelligible and easily accessible form." Council Regulation 2016/679, art. 12(1), 2016 O.J. (L 119) 39 (EU) 1. Similarly, COPPA requires that a privacy statement "must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials." 16 C.F.R. § 312.4(a) (2016). This is one of the few examples of a legal requirement regulating the length of a privacy statement, albeit indirectly, by stating that it must be concise and may *not* contain superfluous information. Additionally, several privacy laws mandate that a privacy statement be easy to find by being posted prominently or conspicuously. Under COPPA, for example, the link to the privacy statement must be "prominent and clearly labeled . . . on the home or landing page or screen of its Web site or online service, *and*, at each area of the Web site or online service where personal information is collected from children [and] . . . must be in close proximity to the requests for information in each such area." 16 C.F.R. § 312.4(d) (2016).

55. Some organizations participate in programs that offer privacy seals based on a desire to demonstrate corporate responsibility or to develop (or enhance) a trusted reputation. Others join industry associations, such as the Network Advertising Initiative or the Digital Advertising Alliance because membership is nearly ubiquitous within a particular industry, and not joining would put the company at a disadvantage. Still others choose to participate in programs such as the EU-U.S. Privacy Shield because it provides a legal basis for certain cross-border data transfers.

56. Commission Implementing Decision (EU) 2016/1250, para. 13, 2016 O.J. (L 207) 1, 3.

provide an adequate level of data protection. The privacy statement of an organization participating in the Privacy Shield must include:

- A statement of its participation in the Privacy Shield,[57] and its adherence to the Privacy Shield Principles with respect to "all personal data received from the EU in reliance on the Privacy Shield"[58];
- A link to, or the web address for, the Privacy Shield List maintained by the Department of Commerce (https://www.privacyshield.gov)[59];
- "Where applicable, the entities or subsidiaries of the organization also adhering to the Principles"[60];
- A description of when exceptions to the organization's adherence to the Principles based on "statute, government regulation, or case law that creates conflicting obligations or explicit authorizations . . . will apply on a regular basis"[61];
- "The types of personal data collected"[62];
- "The purposes for which it collects and uses personal information"[63];
- "The type or identity of third parties to which it discloses personal information, and the purposes for which it does so"[64];
- "Its liability [for damages] in cases of onward transfers to third parties"[65];
- A description of "the requirement to disclose personal information in response to lawful requests by public authorities,

57. *Id.* annex II, at 49.

58. *Id.* § II.1.a.iii, at 50; *see also id.* § II.7d, at 52. This requirement is what, in effect, makes a U.S. company's adherence to the Privacy Shield Principles enforceable. If a company declares that it adheres to these principles, and then fails to do so, the FTC can initiate an action against the company under its existing authority over "unfair and deceptive" practices. *See* 15 U.S.C. § 45 (2012).

59. Commission Implementing Decision 2016/1250, annex II, § II.1.a.i, 2016 O.J. (L 207) (EU) 1, 49.

60. *Id.* § II.1.a.ii, at 49.

61. *Id.* § I.5, at 49.

62. *Id.* § II.1.a.ii, at 49.

63. *Id.* § II.1.a.iv, at 50.

64. *Id.* § II.1.a.vi, at 50.

65. *Id.* § II.1.a.xiii, at 50. The organization's liability in the case of onward transfers does not apply when "the organization proves that it is not responsible for the event giving rise to the damage." *See id.* § II.7.d, at 52. An organization will likely wish to include a description of this limitation in its privacy statement in order to avoid creating strict liability for damage resulting from onward transfers.

including to meet national security or law enforcement requirements"[66];

- "The right of individuals to access their personal data"[67];
- "The choices and means the organization offers individuals for limiting the use and disclosure of their personal data"[68];
- Information about "how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints"[69];
- "The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual, and whether it is: (1) the panel established by [Data Protection Authorities ("DPAs")], (2) an alternative dispute resolution provider based in the EU, or (3) an alternative dispute resolution provider based in the United States,"[70] and a link to the website or complaint submission form of the independent recourse mechanism that is available to investigate unresolved complaints[71];
- A statement regarding the organization "being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body"[72]; and
- A statement of "the possibility, under certain conditions, for the individual to invoke binding arbitration" for claimed violations of the Principles.[73]

These privacy statement requirements under the Privacy Shield are dramatically more extensive than those under the U.S.-EU Safe Harbor Agreement,[74] which the Privacy Shield replaced. Under the Safe Harbor agreement, an organization was required only to declare in its privacy

66. *Id.* § II.1.a.xii, at 50.

67. *Id.* § II.1.a.vii, at 50. Note that the right to access personal data is subject to certain limitations set out in Principle II.8. An organization will likely wish to carefully state those limitations in its privacy statement so as to avoid overstating the scope of the right.

68. *Id.* § II.1.a.viii., at 50.

69. *Id.* § II.1.a.v, at 50.

70. *Id.* § II.1.a.ix, at 50.

71. *Id.* § II.7.a.i, at 52; *id.* § III.6.d, at 55–56.

72. *Id.* § II.1.a.x, at 50

73. *Id.* § II.1.a.xi, at 50. The right of the individual to invoke binding arbitration applies to only to those "residual" claims that remain unresolved after pursuing the other available means of recourse under the Privacy Shield. *See id*. annex I, at 37. An organization will likely wish to thoroughly describe the limitations on the right to arbitration in order to avoid creating a broader right than exists under the Privacy Shield.

74. Commission Decision 520/2000/EC, 2000 O.J. (L 215) (EU) 1.

statement that it adheres to the Safe Harbor Principles,[75] and to include a link to, or URL of, the Safe Harbor website.[76] The increase in privacy statement requirements from those in the Safe Harbor Agreement to those in the Privacy Shield is another example of privacy statement obligations increasing over time, leading to the need for longer and longer privacy statements.

Another type of self-regulatory standard is created by privacy seal programs, such as TRUSTe[77] or EuroPriSe.[78] These programs review websites and products against a set of privacy standards, and those that are found to meet the standards are permitted to display a seal indicating they have adopted sound privacy practices. While quite different in their approaches, both the TRUSTe and EuroPriSe standards create an additional set of privacy statement requirements.

The basic TRUSTe certification standards describe fifteen specific items that must be included in the organization's privacy statement, and another eight that must be added if the organization participates in the EU-U.S. Privacy Shield. They include:

(a) A definition of the scope of the Privacy [Statement];
(b) Types of Personal Information (PI) or Third-Party PI collected, either directly through active or passive means . . . ;
(c) The identity of the Participant (e.g., company name), and, where applicable, the identity of subsidiaries collecting PI or Third-Party PI;
(d) Types of entity(ies) other than the Participant, including Service Providers, collecting PI or Third-Party PI;
(e) Purpose(s) for which PI or Third-Party PI is used;
(f) Types of Third Parties, if any, with whom collected PI or Third-Party PI is shared and for what purpose(s);
(g) A description of the method for updating privacy settings or exercising choice, including choice for interest-based advertising, as required in these Certification Standards;
(h) A description, as required in these Certification Standards, of the method to request access to, or deletion of, collected PI;

75. *See FAQ—Self Certification*, EXPORT.GOV, https://build.export.gov/main/safeharbor/eu/eg_main_018388 (last updated May 7, 2012) ("All organizations that self-certify for the Safe Harbor must also state in their relevant published privacy policy statements that they adhere to the Safe Harbor Principles.").

76. *See Helpful Hints on Self-Certifying Compliance with the U.S.-EU Safe Harbor Framework*, EXPORT.GOV, https://build.export.gov/main/safeharbor/eu/eg_main_018495 (last visited May 17, 2017).

77. TRUSTE, https://www.truste.com/ (last visited May 17, 2017).

78. EUROPEAN PRIVACY SEAL, https://www.european-privacy-seal.eu/EPS-en/Home (last visited May 17, 2017).

(i) A general description of the Participant's information retention policies, and the types of information security measures in place to protect collected PI . . . as required in these Certification Standards;
(j) Types of passive collection technologies used by the Participant or Third Parties including Service Providers and the purpose for using those technologies (e.g., cookies, web beacons, device-recognition technologies);
(k) A description of the method for contacting the Participant, including company name, email address or a link to an online form, and physical address;
(l) A description of the method for notification of any Material Changes in the Participant's privacy practices;
(m) A statement that collected PI or Third-Party PI is subject to disclosure pursuant to judicial or other governmental subpoenas, warrants, orders, or other lawful requests by public authorities; in the event that Participant files for bankruptcy; to protect the rights of the Participant; or protect the safety of the Individual or others[;]
(n) The effective date of the Privacy [Statement]; and
(o) Clear and Conspicuous access to the Validation Page, as outlined in TRUSTe's guidelines, and how to contact TRUSTe to express concerns regarding Participant's Privacy [Statement] or privacy practices.[79]

If a TRUSTe program participant chooses to join the EU-U.S. Privacy Shield, it must also include in its privacy statement information about:

(a) Its participation in EU-U.S. . . . Privacy Shield and a link to or web address for the EU-U.S. . . . Privacy Shield list;
(b) Participant's commitment to apply the Principles to all PI received from the EU in reliance on the EU-U.S. Privacy Shield . . .;
(c) The entities or subsidiaries of the Participant's organization that are also adhering to the Principles;
(d) The independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the Individual.
    (1) EU: Participant must identify whether this dispute resolution body is: (1) the panel established by European Data Protection Authorities, (2) an alternative dispute

79. TRUSTE, ENTERPRISE PRIVACY CERTIFICATION STANDARDS 1–3, https://www.truste.com/privacy-certification-standards/program-requirements/ (last updated Apr. 3, 2017).

> resolution (ADR) provider based in the EU, or (3) an ADR provider based in the United States . . . .;
> (e) Being subject to the investigatory and enforcement powers of the Federal Trade Commission, the U.S. Department of Transportation or any other U.S. authorized statutory body;
> (f) The possibility, under certain conditions, for the Individual to invoke binding arbitration;
> (g) Its liability in cases of onward transfer to Third Parties; and
> (h) Any relevant establishment based in the EU . . . that can respond to Individuals' inquiries or complaints, along with contact information for that establishment.[80]

By contrast, the criteria for the EuroPriSe privacy seal are not so proscriptive. Instead, they pose several relevant questions to ask when evaluating a privacy statement. Some of these questions suggest specific details that must be in a privacy statement, such as the identity of the data controller and contact details that consumers can use for questions or complaints.[81] Other questions have a broader impact on the required content (and therefore length) of a privacy statement. They include:

- Does the privacy [statement] provide sufficient information on relevant privacy issues resulting from the use of the web-based service (e.g. use of cookies, processing of IP addresses)?
- Does the privacy [statement] provide specific and meaningful information about the processing of personal data instead of mere blanket confirmations of legal compliance?[82]

Both of these questions suggest that a privacy statement must contain a lot of information. And they implicitly caution against too much brevity and simplicity. The privacy statement must contain sufficient detail to describe the data that is collected and how it is processed, in a way that is "specific and meaningful." For a privacy statement that must describe a number of complex technologies, several interrelated services, multiple data uses, and in the context of new or rapidly evolving businesses, doing so adequately will necessarily require some lengthy descriptions. A short, simple privacy statement is the opposite of what these criteria require.

Another set of self-regulatory requirements are specific to the online advertising industry. Most companies that provide targeted advertising services participate in the Network Advertising Initiative ("NAI")[83] and/or

---

80. *Id.* at 3–4.

81. EUROPRISE, EUROPRISE CRITERIA FOR THE CERTIFICATION OF IT PRODUCTS AND IT-BASED SERVICES 20–21 (2017).

82. *Id.* at 20.

83. NETWORK ADVERTISING INITIATIVE, http://www.networkadvertising.org/ (last visited May 17, 2017).

one of the regional Digital Advertising Alliance ("DAA") programs.[84] These programs require the participating advertising companies to include several specific disclosures in their privacy statements. For instance, the NAI Code of Conduct requires participating companies to include the following in their privacy statements:

> (a) The Interest-Based Advertising, and[/or] Ad Delivery and Reporting services undertaken by the member company;
> (b) The types of data collected, [including any PII collected,] or used for Interest-Based Advertising and[/or] Ad Delivery and Reporting purposes . . . ;
> (c) How such data will be used, including transfer, if any, to a third party;
> (d) The technologies used by the member company for Interest-Based Advertising, and[/or] Ad Delivery and Reporting . . . .
> (e) The approximate length of time that Interest-Based Advertising or Ad Delivery and Reporting data will be retained by the member company;
> (f) A statement that the company is a member of the NAI and adheres to the [NAI] Code; and
> (g) A link to an Opt-Out Mechanism for Interest-Based Advertising[; and]
>
> [The use of] standard interest segments for Interest-Based Advertising that are based on health-related information or interests . . . .[85]

C. Contractual Obligations

In addition to privacy law and self-regulatory obligations that may apply to an organization's privacy statement, many organizations are also subject to contractual requirements impacting the content of their privacy statements. For example, apps, websites, and online services that contain ads served by third party ad networks will be impacted by another requirement of the NAI and DAA programs under which participating companies must "pass through" certain privacy statement obligations to those that use their ad targeting and delivery services. Specifically, NAI obligates participating companies to require the websites that collect data for "Interest-Based Advertising to clearly and conspicuously post notice" that contains:

---

84. *See* DIGITAL ADVERTISING ALLIANCE, http://www.aboutads.info (last visited May 17, 2017); EUROPEAN INTERACTIVE DIGITAL ADVERTISING ALLIANCE, http://www.edaa.eu (last visited May 17, 2017); DIGITAL ADVERTISING ALLIANCE OF CANADA, http://www.youradchoices.ca (last visited May 17, 2017).

85. 2015 UPDATE TO NAI CODE OF CONDUCT, NETWORK ADVERTISING ALLIANCE 6–7 (2015), http://www.networkadvertising.org/sites/default/files/NAI_Code15encr.pdf.

(a) A statement of the fact that data may be collected for Interest-Based Advertising purposes on the website;
(b) A description of types of data that are collected for Interest-Based Advertising purposes on the website;
(c) An explanation of the purposes for which data is collected by or will be transferred to, third parties; and
(d) A conspicuous link to an Opt-Out Mechanism for Interest-Based Advertising.[86]

Likewise, apps, websites and online services that use third-party analytics services, such as Google Analytics or Flurry, have additional information that they are contractually bound to include in their privacy statements. For instance, the Google Analytics terms require that:

> You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies that are used to collect data. You must disclose the use of Google Analytics, and how it collects and processes data. This can be done by displaying a prominent link to the site "How Google uses data when you use our partners' sites or apps," (located at www.google.com/policies/privacy /partners/, or any other URL Google may provide from time to time).[87]

The Flurry Analytics Terms of Service require that you must post a privacy policy. That policy must (i) provide notice of your use of a tracking pixel, agent or any other visitor identification technology that collects, uses, shares and stores data about end users of your applications (whether by you, Flurry or your Ad Partners) and (ii) contain a link to Flurry's Privacy Policy and/or describe Flurry's opt-out for the Analytics Service to your end users in such a manner that they can easily find it and opt-out of the Analytics Service tracking.[88]

D. Other Legal Considerations

Privacy litigation can create additional legal obligations that affect what goes into a privacy statement. For example, in 2014, Google settled class action claims based on its Internet search service including a user's search query terms in the "referral header."[89] As a result of this practice, when that user arrived on a third-party website as the result of clicking on a link or ad on the Google search results page, that website would know the search terms

86. *Id.* at 7.

87. *See Google Analytics Terms of Service*, GOOGLE, http://www.google.com/analytics/terms/us.html (last visited May 17, 2017).

88. *See Flurry Analytics Terms of Service*, YAHOO! DEVELOPER NETWORK (Apr. 20, 2014), http://www.flurry.com/legal-privacy/terms-service/flurry-analytics-terms-service.

89. Gaos v. Google, No. 5:10–CV–4809, 2012 WL 1094646 (N.D. Cal. Mar. 29, 2012).

the user entered that resulted in the display of that link or ad.[90] The essence of the claims was that Google shared this information with a third party without the knowledge or consent of the user.[91] As part of the settlement, Google agreed to disclose this practice to its users.[92] As a result, in order to avoid litigation, other companies that have similar or analogous practices may feel compelled to add equivalent disclosures.[93]

Understanding, compiling, and reconciling all the applicable requirements for a privacy statement can be a difficult undertaking—especially for an organization that operates across multiple jurisdictions (or even has a website that is accessible from multiple jurisdictions), or engages in a range of practices that span multiple industry sectors or involve the collection of multiple types of personal data. Many of these requirements can result in just a couple of lines or a single paragraph of text. But, many others (such as a description of all the data types collected and how they are used) can take multiple pages for an adequate description. And if the practices or technologies involved are at all complex, then adequately describing them with sufficient detail to meet legal obligations will add much more length to a privacy statement.

II. COMMON CRITICISMS OF PRIVACY STATEMENTS

A. Privacy Statements Are Too Long

The most relevant criticism for the purposes of this Essay is that privacy statements are too long. Much of this criticism simply points out that a privacy statement is long, but lacks any analysis of why the particular length is inappropriate or problematic. For instance, a favorite tactic that critics of long privacy statements employ is to compare the length of a privacy statement to famous documents or pieces of literature. A 2010 New York Times article reported that Facebook's privacy policy was longer than the U.S. Constitution[94]—a comparison that is somewhat ironic given that most provisions of the U.S. Constitution are quite short, lacking in details, and

90. *Id.*

91. *Id.* at *1–2.

92. *In re* Google Referrer Header Privacy Litigation, 87 F. Supp. 3d 1122, 1129–30 (N.D. Cal. 2015).

93. As part of the settlement, Google agreed to add this disclosure to its privacy FAQs. But companies that choose to put their key privacy disclosures in a single document so that readers do not have to hunt across multiple documents for information, as this Essay argues is a best practice, would place such disclosures in the privacy statement. For example, in the section discussing its Bing search service, the Microsoft Privacy Statement contains a provision with the heading "Search query passed in referral URL." *See Microsoft Privacy Statement*, MICROSOFT, https://privacy.microsoft.com/en-us/privacystatement (last visited May 17, 2017).

94. Nick Bilton, *Price of Facebook Privacy? Start Clicking*, N.Y. TIMES (May 12, 2010), http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html.

subject to wildly differing interpretations. In a similar eighteenth century comparison, former Federal Trade Commission ("FTC") Chairman Jon Leibowitz claimed that the average privacy statement is longer than the U.S. Declaration of Independence—another relatively brief document—at a 2012 press conference announcing the release of the FTC's Privacy Framework Report.[95]

Other common comparisons involve claims that various privacy policies are longer than Shakespeare's Hamlet or Macbeth.[96] These comparisons appear to be based on a study released by the UK advocacy group, called Which?, that compared the lengths of different companies' terms of use with those of several works of William Shakespeare.[97] Unfortunately, the Which? report, in some cases, conflated privacy statements with much broader terms and conditions.[98]

In any event, these comparisons are much ado about nothing. They are largely meaningless theatrics that do not take into account the important roles that privacy statements play. A more serious analysis or criticism of a privacy statement's length must point to specific ways in which the statement is too long. Is the problem with the writing style, and if so, how should that be improved to make it more concise? Are there parts of the statement that are redundant or superfluous and should be removed? And, if the only way to shorten the statement is to remove information, how does providing fewer details about an organization's data collection and use practices maintain transparency and accountability?

---

95. Terri Thornton, *FTC: If It's Your Computer, You Should Own Your Data*, MEDIASHIFT (Mar. 27, 2012), http://mediashift.org/2012/03/ftc-if-its-your-computer-you-should-own-your-data087.

96. *See, e.g.*, MIT Startup Exchange (@MITSTEX), TWITTER (Mar. 28, 2015, 10:24 AM), https://twitter.com/MITSTEX/status/603929911951290368 ("More words in Apple's privacy policy than in Hamlet according to @djweitzner. One of these things should probably be simplified. #STEXcyber"); Lateline (@Lateline), TWITTER (May 5, 2015, 12:00 AM), https://twitter.com/Lateline/status/595437794924736513 ("'You wouldn't sit down & read Hamlet, you're not very likely to read the privacy policy.' Prof Fred Cate #metadata"); IAPP Daily Dashboard (@DailyDashboard), TWITTER (Mar. 6, 2014 1:19 PM) https://twitter.com/DailyDashboard/status/441639311629631488 ("Richard Thomas notes that Shakespeare's Hamlet (his longest) was shorter & much easier 2 read than Paypal's #privacy policy. #PrivacySummit."); *see also* Tom Gardner, *To Read, or Not to Read. . . the Terms and Conditions: PayPal Agreement is Longer Than Hamlet, While iTunes Beats Macbeth*, DAILYMAIL (Mar. 22, 2012, 12:00 PM), http://www.dailymail.co.uk/news/article-2118688/PayPal-agreement-longer-Hamlet-iTunes-beats-Macbeth.html.

97. *See* Rich Parris, *Online T&Cs Longer Than Shakespeare Plays—Who Reads Them?*, WHICH? (Mar. 23, 2012), http://conversation.which.co.uk/technology/length-of-website-terms-and-conditions/.

98. For example, the report begins by praising Google's (then) new combined privacy policy, but then appears to discuss the lengths of different companies' terms and conditions in a way that sometimes treats them separately from a privacy statement and sometimes adds together the words of a terms and conditions document to the words of a privacy statement. *Id.*

B. Consumers Rarely Read Privacy Statements

Related to the criticism that privacy statements are too long is the corollary implication that because they are too long, consumers rarely read them. Multiple surveys support the conclusion that consumers generally do not read privacy statements.[99] However, critics are wrong to argue that privacy statements should be shortened because "people don't read them."

In a 2008 study, for example, Aleecia McDonald and Lorrie Cranor estimated that an average Internet user in the United States would need to spend 244 hours a year to read the privacy statements for the websites they visit.[100] That is about forty minutes a day, or slightly more than half the average time these same Internet users spend online.[101] This research supported and explained the conclusion that consumers rarely read privacy statements. Specifically, the authors concluded that consumers do not read them because it is impractical for them to do so—there just are not enough hours in the day to dedicate that amount of time to reading privacy statements.[102]

While McDonald and Cranor provide a more serious contribution to the discussion of long privacy statements than the simplistic length comparisons discussed above, there is little evidence that more people would read privacy statements if they were shorter. The research does not show that people click on privacy statements and then give up when they are too long. On the contrary, it appears that most consumers never even click on the privacy link in the first place, so they often do not know whether they will be confronted with a short or a long statement.

Additionally, it is likely the case that most consumers do not feel a need to read a privacy statement for *every* website or online service they visit. For example, a typical consumer might visit more than a thousand websites in a year.[103] She might simply consume information for the vast majority of the time as she surfs around the web. While she understands that her clicks on

---

99. *See, e.g.*, Press Release, TRUSTe, Study Finds More Americans Concerned About Data Privacy Than Losing Their Income (Jan. 28, 2016), https://www.truste.com/about-truste/press-room/study-finds-more-americans-concerned-about-data-privacy-than-losing-their-income/ (noting that the TRUSTe/National Cyber Security Alliance U.S. Consumer Privacy Index reveals a third of respondents were aware of privacy policies and only sixteen percent ever read them); *see also* Aaron Smith, *Half of Online Americans Don't Know What a Privacy Policy Is*, PEW RES. CTR. (Dec. 4, 2014), http://www.pewresearch.org/fact-tank/2014/12/04/half-of-americans-dont-know-what-a-privacy-policy-is/ (citing research showing that many people believe that the mere presence of a privacy statement indicates that data collected will remain confidential).

100. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 ISJLP 541, 560 (2008).

101. *Id.*

102. *Id.* at 563.

103. *Id.* at 557–58. McDonald and Cranor estimated that U.S. internet users visited 1,462 unique websites annually and used this number as the basis for their calculations. *Id.*

those websites may be tracked and recorded against a cookie ID, she does not feel the need to deeply understand those sites' privacy practices. There are a few sites, however, where she does research on some more sensitive topics, or where she makes purchases and stores a credit card number, or where she has uploaded her address book to enable her to send invitations to a party. It would be reasonable for her to conclude that it is important to read and understand the privacy statements only on that much smaller subset of sites she visits. Further, if she does not use every feature or service available on those sites or is only concerned about certain issues (like sharing), she will only need to read a portion of the privacy statements even for that handful of sites.

Thus, the conclusion that most consumers rarely, if ever, read privacy statements (and could not realistically read them all, even if they wanted to) does not answer the question of whether this is a problem that needs to be solved. And, even if this conclusion does point to a problem, it does not follow that shortening and simplifying privacy statements would be the solution.

C. Privacy Statements Are Unrealistic in Today's World

Some critics of privacy statements have suggested that they are simply unrealistic in today's complex world.[104] They claim that data collection, use, and sharing is too ubiquitous and too complex to be adequately described in a notice. These critics also point out that many means of data collection—from cameras to various types of sensors—lack a user interface through which notice can be provided. But these criticisms do not provide a sufficient reason to give up on privacy statements.

First, these criticisms tend to be more a critique of notice in the context of the traditional notion of "notice and consent,"[105] for example, as reflected in the OECD Privacy Principles of "purpose specification" and "use limitation."[106] A discussion of the merits of the "notice and consent" model of privacy regulation is beyond the scope of this Essay. But even accepting the validity of those critiques, it does not follow that privacy statements serve no purpose.

Even if there are challenges with privacy statements supporting the "purpose specification" and "use limitation" principles, they still play a

---

104. *See, e.g.*, FRED H. CATE, PETER CULLEN & VIKTOR MAYER-SCHONBERGER, DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY: REVISING THE 1980 OECD GUIDELINES (2013).

105. *Id.*; *see also*, Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF 'INFORMATION ECONOMY' 343 (Jane K. Winn ed., 2006).

106. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (1980), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

critical role in supporting the "openness" and "accountability" principles of the OECD Privacy Principles. In other words, if we decouple the long privacy statement from the concept of consent, it still plays an essential role in transparency or openness, and in creating organizational accountability.[107]

Second, although describing complex technologies and business models can be difficult, that does not mean that drafting a privacy statement cannot or should not be done. On the contrary, the more complex the data collection, use, and sharing, the greater the need for a well-written privacy statement to explain those complex data practices. To explain these complexities effectively, such statements often need to be longer than they had been in the past.

III. PROBLEMS WITH ALTERNATE PROPOSALS

There have been many approaches and proposals for short notices—from simplified text and "nutrition label" approaches, to standardized icons and machine-readable privacy disclosures. Some of these approaches are designed to supplement a long privacy statement and others designed to replace a long statement. Those designed to supplement a full, detailed privacy statement have had various levels of effectiveness and success, and some can be quite valuable if used well.

Those designed to replace long privacy statements, on the other hand, suffer from several problems. They eliminate too much detail. They lose important nuances. They simplify to the point that they convey little meaningful information about an organization's data collection and use practices. There is little evidence that they improve consumer understanding or affect consumer behavior.[108] And in some cases, the simplifications and generalizations can even mislead readers.[109] In sum, shortened and simplified approaches to privacy disclosures deprive the consumers and other readers of important detail and meaningful information that is essential to judge an organization's privacy practices. As a result, these approaches nearly always reduce transparency and undermine organizational accountability.

---

107. See Parts IV.A & B of this Essay for a discussion of these benefits.

108. *See, e.g.*, Omri Ben-Shahar & Adam S. Chilton, *Simplification of Privacy Disclosures: An Experimental Test* 1, 28 (University of Chicago Coase-Sandor Institute for Law & Economics Working Paper No., 737, 2015), http://ssrn.com/abstract=2711474 (describing results of experiments in which different simplified approaches to privacy statements had no significant impact on users' comprehension or choices).

109. For example, in order to shorten and simplify a privacy statement, an organization might describe a general practice of not sharing data with third parties, but decline to include a detailed list of exceptions. Even if couched by words like "generally" or "typically," a reader might come away with an impression that is different than the reality. Only by describing all the specific details of its practices can a company provide an accurate picture to the reader.

A. Shortening and Simplifying the Privacy Statement Text

Pressure to shorten and simplify privacy statements have resulted in some organizations going too far. Google provides one well-known example. In 2012, Google published a new privacy statement that consolidated more than sixty separate privacy statements.[110] In designing its new statement, it appeared to embrace the "shorter and simpler is better" mantra that had become so common. However, Google immediately faced a backlash against its new privacy statement.[111] The criticism mainly focused on two primary themes. The first was that this new statement meant Google would now be widely combining data across services.[112] The second was there was not enough detail.[113]

A discussion of the pros and cons of combining data across services is beyond the scope of this Essay, but it is worth noting that Google's prior approach of having different privacy statements for different services could be seen as implying that the data collected within each service, and subject to its own separate privacy statement, is maintained and used only within the confines of that service. At the very least, the approach of maintaining separate privacy statements created ambiguity and uncertainty about the extent to which Google could or did combine data across different services. The new statement, however, by describing data collected from many services in a single, common privacy statement had the benefit of making the fact of such data combination more transparent. And, since transparency should be the goal of every privacy statement, Google's new statement was an improvement in that regard.

The second main criticism of Google's 2012 privacy statement was that it lacked sufficient detail, including service-specific details, to allow users to understand Google's data practices and to make informed decisions about the use of its services. The primary source of this criticism was from the Article 29 Working Party, which reviewed the new privacy statement and issued several recommendations to Google. Among the recommendations were that "Google should disclose and detail how it processes personal data in each service and differentiate the purposes for each service and each category of

---

110. *See Updating Our Privacy Polices and Terms of Service*, GOOGLE OFFICIAL BLOG (Jan. 24, 2012), http://googleblog.blogspot.com/2012/01/updating-our-privacy-policies-and-terms.html.

111. *See, e.g.*, *Privacy Lawsuit Against Google for Policy Change Moves Forward*, ELECTRONIC PRIVACY INFO. CENT. (July 22, 2014), https://epic.org/2014/07/privacy-lawsuit-against-google.html (describing a class action lawsuit resulting from Google's privacy statement consolidation, and noting concerns and complaints raised by advocacy groups, state attorneys general, members of Congress, EU officials, and others).

112. *Id.*

113. *See, e.g.*, Letter from Article 29 Data Protection Working Party, to Larry Page, CEO, Google (Oct. 16, 2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2012/20121016_letter_to_google_en.pdf.

data,"[114] and that it should "[p]rovide additional and precise information about data that have a significant impact on users (location, credit card data, unique device identifiers, telephony, biometrics)."[115] Following the Article 29 Working Party recommendations, several national data protection authorities initiated investigations and enforcement actions against Google. For instance, the Dutch DPA concluded that "Google does not properly inform users which personal data the company collects and combines, and for what purposes."[116] Likewise, the Commission National de L'Informatique et des Libertés ("CNIL") imposed a 150,000€ penalty and other sanctions against Google after concluding:

> [Google] does not sufficiently inform its users of the conditions in which their personal data are processed, nor of the purposes of this processing. They may therefore neither understand the purposes for which their data are collected, which are not specific as the law requires, nor the ambit of the data collected through the different services concerned.[117]

In combining its many privacy statements into one, Google did much more than just eliminate redundancies and clarify its practices regarding data combinations. It went further in its efforts to simplify and shorten its text: details that had previously been disclosed in its separate privacy statements were deleted. The disclosures that remained were very high-level and general, so that they could cover a wide range of services. But, as a result, Google's privacy statement did not adequately inform the reader what specifically happens when a user interacts with a particular Google service. To provide greater transparency and accountability, the statement needed to have more information and more specific details. In short, it needed to be longer.

B. Standardized Short-Form or "Nutrition Label" Privacy Notice Forms

Several efforts have been made to adopt standardized short-form notices or "nutrition label" privacy notices. These proposals identify a small number of privacy topics that can be addressed with very brief text, or can be reduced to a yes/no answer. This key information is then presented in a standardized format such as a table or a format similar to the uniform nutrition labels found

114. *Id*.

115. *Id.*

116. Press Release, Dutch DPA, Dutch DPA: Privacy Policy Google in Breach of Data Protection Law (Nov. 28, 2013), https://cbpweb.nl/en/news/dutch-dpa-privacy-policy-google-breach-data-protection-law.

117. Press Release, Commission National de L'Informatique et des Libertés, The CNIL's Sanctions Committee Issues a 150,000 € Monetary Penalty to Google Inc. (Jan. 8, 2014).

on packaged food. However, these efforts typically leave no room for nuance, and they result in the notice leaving out important details. Most aspects of privacy are not easily reducible to a binary yes/no response, and are not quantifiable in the way, for example, calories or grams of carbohydrates are on a food nutrition label. For example, if a privacy "nutrition label" asks whether or not a company shares personal data with third parties, then every company that is being honest will have to say yes, since, for example, any company could be compelled by law enforcement to turn over data. If the criteria are more specific, such as whether the company shares data with third parties for an unnecessary and unrelated purpose, such criteria become subject to differing interpretations and less clear. The following two subsections discuss specific examples of attempts to ameliorate the perceived problems with the long privacy statement with short-form notices.

1. NTIA Short Form Notice Code of Conduct

One recent effort to develop a short-form notice is that of the multi-stakeholder process convened by National Telecommunications and Information Administration ("NTIA"), which sought to create a Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices.[118] The draft Code established a model form that set out specific data types that an app may collect,[119] and specific categories of third parties with which data may be shared.[120] The app then must simply check yes or

---

118. *See Privacy Multistakeholder Process: Mobile Application Transparency*, NAT'L TELECOMMS. & INFO. ADMIN. (Nov. 12, 2013), http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency. The latest draft of the Code is available at NAT'L TELECOMMS. & INFO. ADMIN., SHORT FORM NOTICE CODE OF CONDUCT TO PROMOTE TRANSPARENCY IN MOBILE APP PRACTICES (2013) [hereinafter NTIA CODE], http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf.

119. The data types include:

> (1) Biometrics (information about your body, including fingerprints, facial recognition, signatures and/or voice print), (2) Browser History (a list of websites visited), (3) Phone or Text Log (a list of the calls or texts made or received), (4) Contacts (including list of contacts, social networking connections or their phone numbers, postal, email and text addresses), (5) Financial Info (includes credit, bank and consumer-specific financial information such as transaction data), (6) Health, Medical or Therapy Info (including health claims and other information used to measure health or wellness), (7) Location (precise past or current location of where a user has gone), and (8) User Files (files stored on the device) . . . .

NTIA CODE, *supra* note 118, at 2–3.

120. The categories of third parties include:

> (1) Ad Networks (Companies that display ads to you through apps), (2) Carriers (companies that provide mobile connections), (3) Consumer Data Resellers (companies that sell consumer information to other companies for multiple purposes including offering products and services that may interest you), (4) Data Analytics Providers (companies that collect and analyze your data), (5) Government Entities (any sharing

no for each data type and each type of third party data sharing. A problem with this form is that it does not allow for any description of why the data is collected. For example, is location data collected if and only if the individual uses a mapping feature of the app, or is it a flashlight app that just continuously harvests location in the background? Under the NTIA form, such limited and necessary data collection would appear the same as the ubiquitous and unnecessary data collection.

A bigger problem with the NTIA model is that because it specifies the disclosure of only specific, enumerated data types, it provides incomplete coverage of possible data collection and use. As a result, it is not hard to imagine apps that would result in wildly misleading notices if they followed the NTIA model. For instance, there could be a seemingly benign app—say, a flashlight app—that does not collect any of the specific data types listed on the NTIA model form, but it runs in the background and logs every keystroke typed into the device and sends that keystroke data back to the app developer. What would the NTIA notice look like? If it strictly adhered to the NTIA form, it would look like it collects no data.

2. Gramm-Leach-Bliley Act Model Privacy Form

As noted above, the GLBA requires financial institutions to provide initial and annual privacy notices to their customers.[121] When financial institutions started providing the privacy statements required by the Act in 2001, there was much criticism of the newly drafted statements, in large part because they were often perceived as unnecessarily long and complex.[122] In 2009, the agencies tasked with implementing and enforcing GLBA jointly adopted a model privacy form that was designed to simplify and standardize privacy notices, and that would serve as a safe harbor for financial institutions that rely on it to meet their privacy notice obligations.[123]

Model notices under GLBA give very little information about what data is collected and how it is used by the financial institutions. They are focused

---

> with the government except where required by law or expressly permitted in an emergency), (6) Operating Systems and Platforms (software companies that power your device, app stores, and companies that provide common tools and information for apps about app consumers), (7) Other Apps (other apps of companies that the consumer may not have a relationship with), and (8) Social Networks (companies that connect individuals around common interests and facilitate sharing).

Id. at 3.

121. *See supra* Part II.

122. *See, e.g.*, David Arkush & David C. Vladeck, *Petition for Rulemaking* (July 26, 2001), https://epic.org/privacy/consumer/glbpetition.pdf (petitioning the FTC and other financial regulators, containing signatures from more than a dozen consumer advocacy groups, and complaining that privacy notices sent to consumers under GLBA are long, dense, and confusing).

123. Final Model Privacy Form Under the Gramm-Leach-Bliley Act, 74 Fed. Reg. 62890–62994 (Dec. 1, 2009).

on giving a very high-level description of *some* of the categories of entities with which personal data may be shared and describing how to exercise a limited right to opt-out of *some* of that data sharing. Given the brevity of these notices, the notices from many different financial institutions look almost identical.[124] They provide little or no meaningful insight—either for consumers or other readers—into the unique data collection, or internal use or retention practices, of each financial institution, and provide only limited insight into the data sharing practices.[125]

C. Privacy Icons

Like other attempts to abbreviate privacy disclosures, privacy icons are inherently limited in their ability to convey useful information. What matters in the area of privacy is often dependent on nuance, gradations, and context. Icons can convey little or none of that meaning. Icons that attempt to convey meaning are inherently binary—either the company does something or it does not. There may be a handful of details for which such an approach can be useful, but icons cannot convey the full range of practices and policies that readers of a privacy statement typically care about. They may convey the "what" but not the "why." The context, detail, and explanation that icons lack are often critical for individuals to have a useful understanding of a particular privacy practice.

Icons are included in the EU General Data Protection Regulation ("GDPR") in a somewhat half-hearted way:

> The information to be provided to data subjects pursuant to Articles 13 and 14 may be provided in combination with standardized icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.[126]

---

124. One goal of the model notice was to make different financial institutions' privacy notices easier to compare. *Id.* at 62892, 62893 ("Because the privacy rule allows institutions flexibility in designing their privacy notices, notices have been formatted in various ways and as a result have been difficult to compare, even among financial institutions with identical practices.").

125. This shortcoming is largely due to the limitations of GLBA itself. The statute is almost entirely focused on third-party data sharing and providing a limited right to opt-out of such sharing. *See* 15 U.S.C. § 6802(b) (2012). It requires little or no transparency about an organization's internal use of the data it collects. *But see* Lorrie Faith Cranor et al., Are They Actually Different? Comparing Thousands of Financial Institutions' Privacy Practices 13 (2013) (unpublished manuscript), http://www.blaseur.com/papers/financial-final.pdf (suggesting that automated comparisons of thousands of financial institutions' privacy statements that follow the GLBA model can reveal differences among those organizations' practices).

126. Council Regulation 2016/679, art. 12(7), 2016 O.J. (L 119) 40 (EU). Article 12(8) gives the Commission the authority to develop the standardized icons. *Id.* art. 12(8).

Thus, the adoption of icons appears to be voluntary, likely dooming them from the start. An earlier GDPR draft from the Committee on Civil Liberties, Justice and Home Affairs of the European Parliament ("LIBE Committee") was more proscriptive and included a requirement to adopt a standard form privacy statement that contained standard icons,[127] and an annex listed standard icons with particular meanings, including icons representing:

- "No personal data are collected beyond the minimum necessary for each specific purpose of the processing";
- "No personal data are retained beyond the minimum necessary for each specific purpose of the processing";
- "No personal data are processed for purposes other than the purposes for which they were collected";
- "No personal data are disseminated to commercial third parties";
- "No personal data are sold or rented out";
- "No personal data are retained in unencrypted form."[128]

Such icons would have been difficult to implement and of questionable value—due to the general problems with icons described above. Additionally, with regard to these proposed icons, there were far too many ambiguities built into them. For instance, with respect to the first two icons that set out a "minimum necessary" standard for data collection and retention, such a standard raises the perennial debate in privacy is how much data is "necessary" to achieve a defined purpose. Does a necessity standard mean that the organization can only collect the minimum amount of data that enables it to accomplish the purpose? Or, does it allow the collection of more data if that additional data allows that purpose to be achieved with greater efficiency and efficacy? If the latter, how much is enough? Similar debates play out with regard to how long it is necessary to retain data. The proposed icon indicating that no personal data are processed other than for the purposes for which they were collected would merely reinforce the incentive to define the purposes very broadly from the beginning. An icon focused on data being "sold or rented out" will lead to other forms of commercial transactions involving data—or to simply giving away the data for free. By contrast, requiring a company to describe what it does in each of these areas in plain language reduces the opportunities for such mischief and increases transparency.

---

127. *See* European Commission, *Inofficial Consolidated Version After LIBE Committee Vote Provided by the Rapporteur 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*, art. 13a (Oct. 22, 2013), http://www.janalbrecht.eu/fileadmin/material/Dokumente/DPR-Regulation-inofficial-consolidated-LIBE.pdf.

128. *Id.* Annex 1.

Other privacy icons have been proposed in the past, but none have gained any significant traction.[129] Nevertheless, icons *can* play a helpful role in certain narrow contexts with a limited and specific purpose. The one example of a privacy icon that has gained some traction is the AdChoices icon for online behavioral advertising.[130] The AdChoices icon is different from other privacy icon proposals in that its primary purpose is not to convey information about an organization's privacy practices—other than that the advertisement with which it appears might be delivered by a third party that engages in online behavioral advertising. Rather, the main value of the icon is that it provides a standard, recognizable, and contextual link to find more information, typically including links to the relevant privacy statement or statements, and an ability to exercise choice.

It is possible that other approaches to icons may be successful in the future, but only if narrowly focused and supplemented by more detailed information, such as information provided in a long privacy statement.

D. Machine-Readable Privacy Disclosures

The GDPR language creating a voluntary approach to the use of privacy icons includes the requirement that if such icons are used, they must be machine-readable.[131] This and other proposals for machine-readable privacy disclosures require a technical standard setting out a defined schema that can be coded into a website or an application and can be read and interpreted by a web browser or other software running on a user's device. But like icons, machine-readable privacy disclosures suffer from many of the same shortcomings, including an inability to convey context and nuance that can be described in a detailed privacy statement designed for human readers. But unlike privacy icons, there is a long history with respect to machine-readable privacy disclosures, which includes an international standard that gained some limited traction but has since faded into obsolescence.

---

129. *See, e.g.*, *Privacy Icons v. 0.2*, MOZILLA WIKI, https://wiki.mozilla.org/Privacy_Icons_v0.2 (last updated Sept. 28, 2011, 5:40 PM) (icons proposed by Mozilla); *Privacy Icons*, MOZILLA WIKI, https://wiki.mozilla.org/Privacy_Icons (last updated June 27, 2011, 8:33 PM) (same); *Privacy Policies are Too Complicated: We've Simplified Them*, DISCONNECT, https://disconnect.me/icons (last visited May 17, 2017).

130. The AdChoices icon was developed by the Digital Advertising Alliance ("DAA") and is part of its self-regulatory program. *See* AM. ASSOC. OF ADVERTISING AGENCIES ET AL., SELF-REGULATORY PRINCIPLES FOR ONLINE BEHAVIORAL ADVERTISING 5, 9, 18 (2009), http://digitaladvertisingalliance.org/sites/digital.daaoperations.org/files/DAA_files/seven-principles-07-01-09.pdf. For consumer information about the icon, see *YourAd Choices Gives You Control*, DIGITAL ADVERTISING ALLIANCE, http://youradchoices.com/ (last visited May 17, 2017).

131. Council Regulation 2016/679, art. 12(7), 2016 O.J. (L 119) (EU) 40.

The Platform for Privacy Preferences Project ("P3P") was developed by the World Wide Web Consortium ("W3C") in the late 1990s.[132] It was designed to be a machine-readable reflection of a company's privacy statement, so that user agents (whether a web browser or other specialized software) could inform users of a website's practices and automate decision-making in line with the user's preferences. A number of websites adopted P3P statements early on, particularly after mid-2000 when Microsoft announced support for P3P in its upcoming Windows XP operating system.[133] But P3P received criticism from the beginning from advocates,[134] regulators,[135] and industry.[136] And while many websites continued limited implementations of P3P for a number of years in order to maintain compatibility with widely used web browsers that supported P3P, it became clear over time that such implementations were increasingly meaningless,[137] and P3P quietly faded away.[138]

There are likely multiple factors why P3P failed, but one common criticism is that it was both too complex and too limited. One need only browse the P3P 1.0 specification to see the enormous number of elements

---

132. See *Platform for Privacy Preferences (P3P) Project*, W3C (Oct. 3, 2007), http://www.w3.org/P3P/, for detailed specifications, background, and other resources on P3P.

133. *See* Press Release, Microsoft, Microsoft Announces Privacy Enhancements for Windows, Internet Explorer (June 21, 2000), http://news.microsoft.com/2000/06/21/microsoft-announces-privacy-enhancements-for-windows-internet-explorer/#sm.00000uau43haf5e5rvrxl4adp515m; *How to Manage Cookies in Internet Explorer 6*, MICROSOFT, https://support.microsoft.com/en-us/kb/283185 (last visited May 17, 2017) (explaining the resulting implementation in Internet Explorer 6 regarding its treatment of based on a website's P3P compact policy (or absence thereof)).

134. *See, e.g.*, ELECTRONIC PRIVACY INFO. CTR., PRETTY POOR PRIVACY: AN ASSESSMENT OF P3P AND INTERNET PRIVACY (2000), https://epic.org/reports/prettypoorprivacy.html.

135. *See, e.g.*, *Working Party on the Protection of Individuals with regard to the Processing of Personal Data, Opinion 1/98: Platform for Privacy Preferences (P3P) and the Open Profiling Standard (OPS)* (June 16, 1998), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/1998/wp11_en.pdf.

136. *See, e.g.*, Kenneth Lee & Gabriel Speyer, *Platform for Privacy Preferences Project (P3P) & Citibank*, W3C (Oct. 22, 1998), http://www.w3.org/P3P/Lee_Speyer.html.

137. For instance, sites began publishing "fake" P3P policies in order to fool browsers that supported P3P. *See, e.g.*, *Google Bypassing User Privacy Settings*, IEBLOG (Feb. 20, 2012), https://blogs.msdn.microsoft.com/ie/2012/02/20/google-bypassing-user-privacy-settings/ (criticizing Google for publishing a P3P compact policy that contained the English words: "This is not a P3P policy!").

138. In 2015, fifteen years after first announcing support for P3P, Microsoft ended that support with the release of Windows 10:

> The *Platform for Privacy Preferences 1.0 (P3P 1.0)* is obsolete in Windows 10 (Microsoft Edge and all modes of Internet Explorer 11 for Windows 10). Support for P3P 1.0 has been removed in Windows 10 and will have minimal ongoing servicing for previous versions of Windows. Recommended practice is to avoid deploying P3P privacy policies on your site.

P3P is No Longer Supported, MICROSOFT, https://msdn.microsoft.com/en-us/library/Mt146424%28v=VS.85%29.aspx (last visited May 17, 2017).

and variations within those elements and get a sense of the complexity.[139] Taking that complex schema and mapping it to a human-readable privacy statement and real world practices was often akin to trying to fit many square pegs into many round holes. Lawyers advised that a P3P policy must be accurate, just as a human-readable privacy statement must be, and the two must remain consistent with each other.

But despite the detail and complexity, the standard was also too limited. Like privacy icons, the binary nature of the elements made it difficult or impossible to provide the context that is so essential to conveying meaning. And in many cases, the individual elements were far too blunt. To take just one example, in the P3P syntax, when identifiable data is shared with a third party, the P3P policy must contain the "<RECIPIENT>" element.[140] And within that element, it must contain one or more tags to indicate what type of entity would be a recipient of the data. One of those tags is "<unrelated>" indicating "unrelated third parties: Legal entities whose data usage practices are not known the original service provider."[141] However, because any entity could be compelled to turn over data to an unrelated third party due to a court order in a criminal investigation or civil litigation, in order to avoid being misleading, every entity should have the "<unrelated>" tag in its P3P policy. But, having every entity use that tag renders it meaningless and allows those entities that freely share data to look exactly the same as those that carefully guard it and only turn it over when compelled.

Despite the failure of P3P, calls for machine-readable disclosures continue.[142] Given the track record, any new proposals are likely to face strong skepticism. Like privacy icons, any successful use will have to be narrowly targeted to specific aspects of privacy practices, and the full, detailed (human-readable) privacy statement still needs to play a central role in creating true transparency and accountability.

---

139. *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification*, W3C (Apr. 16, 2002), http://www.w3.org/TR/P3P/.

140. *Id.* (section 3.3.5).

141. *Id.*

142. *See, e.g.*, *supra* note 133 and accompanying text (discussing the proposal in the GDPR draft); *see also* Ryan Joe, *Exiting FTC Commissioner Julie Brill: "Advertisers and Ad Networks Need to Provide More Usable Tools for Consumers"*, ADEXCHANGER (Mar. 23, 2016, 3:23 PM), https://adexchanger.com/privacy/exiting-ftc-commissioner-julie-brill-advertisers-and-ad-networks-need-to-provide-more-usable-tools-for-consumers/ ("Forty percent of information flowing with respect to the Internet of Things is machine-to-machine communication, not machine-to-human. We need to engage that communication by having privacy policies that are machine-readable.").

E. Just-in-Time or Contextual Notices

So-called "just-in-time" notices are those that appear in a person's experience at the time and in a context that they are most relevant and understandable. For example, when a consumer downloads an app that requires location information to operate, a notice providing information to the user (and typically asking for consent) would appear when the user uses the app for the first time.[143] Just-in-time notices can be extremely valuable as a supplement to a full privacy notice. But it would be a mistake to think of them as a satisfactory alternative.

Unlike just-in-time notices, a full, detailed privacy statement provides the "full story." Providing information about data collection in a piecemeal manner may, in effect, "hide the ball" with respect to how much data may be collected and aggregated over time. A detailed privacy statement provides the opportunity to look forward and see how the organization will gather and use data over time. And, it gives the opportunity to look back to gain an understanding of the cumulative effect of how the user has engaged with the organization and its services.

Further, if privacy information were provided only through just-in-time notices, there would be no single place to find relevant information at any time and regardless of context. Often, it is not easy, or even possible, to go back and recreate the context in which a just-in-time notice is provided. But enabling users to go back and find privacy information in a convenient place is important because people's views and circumstances change over time. And, these changes can lead to changed privacy sensitivities and needs. If notice is provided only in context when the data is first collected or a choice about use or sharing is first presented, it may be difficult for a user to reconsider those choices or take other actions to protect their privacy when a heightened need for privacy arises. For example, someone who decides to flee an abusive spouse may wish to review how the apps she uses collect and expose location information, or how her social networking services reveal contacts and relationships. She may now wish to make other choices about which services she uses or how she sets her privacy options. The full privacy statement provides a convenient and easily accessible way to find that information.

---

143. Experiential or "visceral" notice, which, instead of relying on textual descriptions of data practices, leverages other aspects of the individuals' experience to inform, can also be thought of in this category. *See* M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 NOTRE DAME L. REV. 1027, 1027 (2012).

IV. THE ADDITIONAL BENEFITS OF "LONG" PRIVACY STATEMENTS

The previous Section discussed some of the benefits of long, detailed privacy statements. Detailed privacy statements provide sufficient information to help readers understand an organization's practices and make informed decisions, they offer the "full story" of an organization's privacy practices in a single location and, unlike piecemeal privacy disclosures provided in particular contexts, a full privacy statement is typically accessible at any time. Full, detailed privacy statements have several other benefits as well.

A. External Accountability

As discussed above, consumers are not the only audience for privacy statements. In fact, the evidence suggests that consumers rarely read them, and shortening privacy statements is unlikely to significantly increase the number of consumers that click on the links or read them. However, regulators, policymakers, academics, researchers, investors, advocates, and journalists *do* read privacy statements. These audiences can be highly motivated to read through a privacy statement, regardless of its length.

Some of these audiences, primarily regulators, have the authority to police privacy statements and the practices they describe in order to protect the interests of consumers (including those who do not read privacy statements).[144] Others are in a position to raise public awareness about organizations' practices. Journalists write articles educating readers about privacy issues and, frequently, "shaming" companies for bad privacy practices (or for having badly drafted privacy statements).[145] Advocates, similarly, employ various tactics to raise consumers' awareness and pressure organizations into adopting more privacy-protective policies and practices.[146]

---

144. For example, in the United States, the bulk of government enforcement activity in the area of privacy has been based in the FTC's authority under Section 5 of the FTC Act to investigate and prosecute "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C § 45(a)(1) (2012). A typical case of FTC privacy enforcement involves a failure by a company to adhere to the representations made in its privacy statement, thereby engaging in a "deceptive" practice. *See* Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 599, 628–29 (2014).

145. *See, e.g.*, Tony Bradley, *Don't Fall for the Facebook Privacy Notice Hoax*, PCWORLD (Nov. 26, 2012, 9:04 AM), http://www.pcworld.com/article/2016911/don-t-fall-for-the-facebook-privacy-notice-hoax.html; Steve Stecklow, *On the Web, Children Face Intensive Tracking*, WALL ST. J. (Sept. 17, 2010), https://www.wsj.com/articles/SB10001424052748703904304575497903523187146.

146. For example, the Electronic Frontier Foundation ("EFF") periodically publishes comparisons of companies' privacy and data protection practices, relying in large part on the representations made in the companies' privacy statements. *See, e.g.*, *Who Has Your Back?*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/who-has-your-back-2016 (last visited May 17, 2017) (report released annually).

This kind of notice-based accountability is not unique to the area of privacy. A well-known and successful example can be found with regard to financial disclosures for public companies required by the Securities and Exchange Commission ("SEC").[147] These mandated, public disclosures are long and detailed. Consumers, and indeed most individual investors, rarely read them.[148] But those who are tasked with making investment choices on behalf of individual investors and/or protecting consumers do read them and do hold companies accountable for the information disclosed in these documents.[149]

B. Internal Discipline and Compliance

The shorter and simpler a privacy statement, the more it must rely on generalities and high-level statements of principles. Those drafting such statements need not dig deep and fully understand all the specific details of what data is collected, how it is used, with whom it is shared, or how long it is retained.

In contrast, drafting a detailed, long privacy statement requires a rigorous investigation into the facts. The organization must understand the types of data collected, the mechanism by which it is collected, how it is stored and accessed within the organization, the purposes for which it is used, how long it is retained, how it is protected, with whom it is shared and for what purposes, what privacy controls are available and how they function, and more.[150] The exercise of drafting a long privacy statement can reveal

---

147. In fact, the SEC has issued guidance stating that public companies should provide detailed disclosures of material cybersecurity risks and cybersecurity incidents, including those affecting customer information. SEC. & EXCH. COMM'N, DIV. OF CORP. FIN., *Corporate Finance Disclosure Guidance: Topic No. 2, Cybersecurity* (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm. For some companies, like Facebook, privacy risks beyond cybersecurity are material enough that they disclose such privacy risks to investors in their financial disclosures. *See e.g.*, FACEBOOK, ANNUAL REPORT 12 (2015), https://s21.q4cdn.com/399680738/files/doc_financials/annual_reports/2015-Annual-Report.pdf.

148. As with privacy statements, there are periodic calls to make the disclosures more clear and readable. See, for example, the efforts at improving disclosure effectiveness described at *Disclosure Effectiveness*, SEC. & EXCH. COMM'N, https://www.sec.gov/spotlight/disclosure-effectiveness.shtml (last visited May 17, 2017).

149. *See, e.g.*, Letter from William H. Thompson, Sec. & Exchange Comm'n, to Shelly Reynolds, Vice President and Worldwide Controller, Amazon (Mar. 12, 2012), https://www.sec.gov/Archives/edgar/data/1018724/000000000012012577/filename1.pdf; Letter from Maryse Mill-Apenteng, Special Counsel, Sec. & Exchange Comm'n, to Larry Page, CEO, Google (May 2, 2012), https://www.sec.gov/Archives/edgar/data/1288776/000000000012022687/filename1.pdf; *see also* Jan Taylor Morris et al., *A New Era of Accountability?*, STRATEGIC FIN., May 2012, at 42.

150. Particularly for larger and more complex organizations, creating the requisite level of understanding likely requires internal mechanisms to conduct privacy reviews and document the details of privacy-impacting features and practices. Shortcomings in such processes will make drafting the privacy statement a much more difficult task.

internal gaps in processes, training, and compliance. And it can force greater understanding and documentation of data processing practices across the organization.[151]

The act of drafting a description of an organization's practices that is intended to be posted publicly also creates an opportunity to reevaluate those practices. Drafting serves as a "reality check" that requires the organization to think about how these practices will be viewed by readers of the privacy statement. It forces the organization to look at its policies and practices through a different lens, leading to a self-reflective analysis that might not otherwise occur. If the analysis suggests that the policies and practices may be viewed as too aggressive or invasive by readers of the privacy statement, the organization is much more likely to rethink and modify its policies and practices.

Similarly, compiling a privacy statement creates an opportunity to re-evaluate practices or decisions that may have been made in a vacuum. For example, there may have been several data collection decisions made independently by different parts of an organization. Each of them, independently, seemed fairly innocuous and low-risk. But collectively, the decisions present a greater privacy risk. That collective risk may not be fully realized until the organization goes through the exercise of describing them all in a single document. Thus, drafting a detailed privacy statement can lead to discoveries and realizations that might not otherwise occur.

But, again, few of these benefits will be realized from the exercise of drafting a high-level privacy statement that is mainly limited to principles and generalities.

C. Focusing on Notice Is Realistic and Achievable

Regulatory and legislative efforts to improve privacy practices and protect consumers from privacy harms often face an uphill battle. Privacy rules restricting the collection and use of data typically face fierce opposition from the private sector (and often from some government agencies that rely on the availability of data). Rules restricting the publication of data often face opposition from advocates of free speech and the free availability of information.[152] Prescriptive notice requirements will inevitably elicit some

151. *See* Peter P. Swire, *The Surprising Virtues of the New Financial Privacy Law*, 86 MINN. L. REV. 1263, 1314–17 (2002) (discussing the benefits of the notice obligations under the GLBA, including greater internal investments in privacy protections and enhanced accountability).

152. For example, the 2014 ruling by the Court of Justice of the European Union in Google Spain SL established the so-called "right to be forgotten." Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, Celex No. 612CJ0131 (May 13, 2014). The court ruled that search engines, in some circumstances, have an obligation to remove links to information that appear in response to a search on a person's name—even if the information in question is published lawfully. *Id.* The ruling highlighted tensions between privacy rights and the freedoms of expression

complaints, but rules focused on notice and transparency are unlikely to face as much opposition as other types of privacy requirements—particularly if they are focused on what must be in a privacy statement, as opposed to more prominent notice obligations that can interfere with product design and user experiences.[153]

Further, there are existing enforcement mechanisms. Many regulators around the world have the tools and the authority to enforce the promises and representations made by an organization in its privacy statements, and to address a privacy statements' shortcomings. For example, in the United States, the FTC has enforcement authority under Section 5 of the FTC Act to act against "unfair and deceptive" practices.[154] The FTC bases the bulk of its privacy actions on an organization's deceptive representations about its privacy practices.[155]

V. IMPROVING PRIVACY STATEMENTS WITHOUT SACRIFICING TRANSPARENCY AND ACCOUNTABILITY

Defending long privacy statements is not the same as defending badly drafted privacy statements. Too many privacy statements lack clarity. Too many use overly legalistic or technical jargon. Too many are organized poorly, difficult to navigate, redundant, and full of unnecessary (or even misleading) puffery and spin.

---

and access to information; it was criticized by those who place a high value on those competing rights. *See, e.g.*, Charles Arthur, *Explaining the 'Right to Be Forgotten'—The Newest Cultural Shibboleth*, GUARDIAN (May 14, 2014, 1:42 PM), https://www.theguardian.com/technology/2014/may/14/explainer-right-to-be-forgotten-the-newest-cultural-shibboleth; Craig Timberg & Sarah Halzack, *Right to be Forgotten vs. Free Speech*, WASH. POST (May 14, 2014), https://www.washingtonpost.com/business/technology/right-to-be-forgotten-vs-free-speech/2014/05/14/53c9154c-db9d-11e3-bda1-9b46b2066796_story.html; Eduardo Bertoni, *The Right to Be Forgotten: An Insult to Latin American History*, HUFF. POST, http://www.huffingtonpost.com/eduardo-bertoni/the-right-to-be-forgotten_b_5870664.html (last updated Nov. 24, 2014).

153. In Europe, the E-Privacy Directive includes a requirement to obtain consent for the placement of cookies. Council Directive 2009/136/EC, art. 5(3), 2009 O.J. (L 337) 30. This requirement has resulted in many web sites displaying prominent and disruptive "cookie banners" that provide notice of the use of cookies and seek the consent of users to place cookies on their devices. In response to the widespread view that the cookie banners are annoying and disruptive, a proposal to replace the E-Privacy Directive has taken a different approach to try to reduce the prevalence of such notices. *Cookie Banner Frustration to Be Tackled by EU*, BBC (Jan. 11, 2017), http://www.bbc.com/news/business-38583001.

154. 15 U.S.C. § 45(a)(1) (2012).

155. *See* Solove & Hartzog, *supra* note 144. There is a danger in putting too much reliance on deceptiveness claims, however. Organizations will be reluctant to be more transparent in a privacy statement if their statements can be held against them when they make an error. A balanced approach would have the FTC, in addition to relying on its "deceptiveness" authority, also rely on its "unfairness" authority in cases where organizations fail to disclose material details about their data collection, use, and sharing practices.

If a privacy statement needs to be long in order to fully describe the organization's relevant data practices, that does not mean it has to be unreadable. Rather than a single-minded focus on length, those interested in improving privacy statements should focus on other aspects that will both lead to greater clarity in the text and help ensure that the statement is not any longer than it needs to be. Drafting strategies that can help achieve those objectives include the following:

Clear, straightforward language. The use of technical or legal jargon reduces the clarity of a privacy statement for the average reader. Language designed to obscure or "sugar coat" a fact that some readers might view negatively undermines openness and transparency.[156] Those drafting privacy statements should focus on using plain language to describe data practices in the clearest way possible.[157] There are excellent resources and guidance available on plain language writing—many aimed at increasing the clarity of government documents, but which can be utilized for privacy statement drafting as well.[158]

Meaningful details rather than generalities. Overreliance on generalities is one of the biggest pitfalls of making the privacy statement too short and eliminating specific details. To be transparent, a privacy statement must say clearly what data is collected and when. Privacy statements should avoid the word "may" or other similar terms when possible. For example, if a service collects location data in only some circumstances, the privacy statement should not say "we may collect location data." That leaves readers guessing as to whether and under what circumstances location data is actually collected. In other words, it conveys nothing useful. It could even cross the

156. One common example of such language is the over-use of the word "anonymous." Data is often called "anonymous" in an attempt to downplay legitimate privacy concerns. In cases where some form of weaker and reversible de-identification has been used, characterizing the data as anonymous is deceptive.

157. For a comparison of several companies' privacy statements using criteria for plain language writing, see Katy Steinmetz, *These Companies Have the Best (And Worst) Privacy Policies*, TIME (Aug. 6, 2015), http://time.com/3986016/google-facebook-twitter-privacy-policies/. The Center for Plain Language report referenced in the Time article can be found at CENTER FOR PLAIN LANGUAGE, PRIVACY-POLICY ANALYSIS, http://centerforplainlanguage.org/wp-content/uploads/2015/09/TIME-privacy-policy-analysis-report.pdf (last visited May 17, 2017).

158. See, for example, a U.S. federal government site focused on fostering plain language writing in U.S. government documents and publications, PLAINLANGUAGE.GOV, http://www.plainlanguage.gov/ (last visited May 17, 2017). For texts of plain language laws that have been adopted in various U.S. states, see *Various Plain English Statutes*, LANUGAGEANDLAW.ORG, http://www.languageandlaw.org/TEXTS/STATS/PLAINENG.HTM (last visited May 17, 2017). Also, the Center for Plain Language provides resources for the use of plain language and serves as a watchdog for unclear writing by the government and private sector. CENTER FOR PLAIN LANGUAGE, http://centerforplainlanguage.org (last visited May 17, 2017).

line into being deceptive.[159] Instead, the privacy statement should say "when you do *X*, we will collect location data." In a small number of cases, generalities are unavoidable, but drafters of privacy statements should make a determined effort to eliminate as many as possible.

Few or no redundancies. Many organizations maintain different privacy statements for different products or services. When customers use several of these services, they will be faced with several separate privacy statements and will inevitably encounter a great deal of redundant text across those statements. Especially where different services are often used together, the services involve common elements, or the data collected though the services is combined, having a single privacy statement that covers all those services will almost always reduce redundancies and increase transparency. Redundancies also occur within a single privacy statement, which should be eliminated through careful drafting and an intuitive organization of the document.

Format and structure that aids in navigation. A well-structured privacy statement helps the reader find the relevant information quickly and easily. A well-structured privacy statement makes it unnecessary to read the entire statement in order to locate the information that is relevant to a particular reader or to find the answer to a particular question.[160] Using clear headings will help the reader find the relevant information quickly. If the privacy statement is long, the use of a table of contents or similar navigation aid will also increase usability.

Likewise, adopting a layered format makes privacy statements easier to understand and navigate, in spite of the fact that they often must be long in order to covey all the relevant information. Layered privacy statements can provide quick summaries and a roadmap for finding more detail in the full statement. A typical layered privacy statement will have a short "top layer" that provides a short summary (often designed to fit on one page or one screen) of a privacy statement's key points and provides a roadmap for navigating the full statement. Layered privacy statements have been used

159. For example, saying the organization "may" do something when it, in fact, will do that thing is misleading.

160. Many critiques of long privacy statements are implicitly based on the premise that individuals should or will read every word of the statement to be able to make informed decisions and protect their privacy interests. That premise is wrong. And the conclusions that flow from that incorrect premise are therefore flawed.

successfully for the last fifteen years[161] and are regularly encouraged by privacy regulators and others.[162]

Links to supplemental information. Some supplementary information beyond the privacy statement can offer different ways of presenting information that can increase understanding. For example, Google pioneered the use of videos to provide tutorials and additional privacy information.[163] Other supplemental information can provide deeper or more technical details for specific topics and/or particular audiences. For instance, Microsoft has released technical white papers on certain topics, such as additional details on the data collected as part of Windows 10 telemetry.[164] An increasing number of companies publish "transparency reports" with detailed statistics and information about requests for customer data from law enforcement and other government agencies.[165]

The publication of these types of supplemental information takes the layering approach one step further by providing an even deeper level with more granular and detailed information. The privacy statement is still the starting point, but it can link to other information that is better presented in different formats. However, this strategy should be used judiciously and thoughtfully. Readers should not have to hunt across multiple documents to find the information they need or to piece together the "full story." This supplemental information should be truly supplemental, explaining in deeper detail or in a different way something that is already disclosed in the privacy

161. An early model for layered privacy statements was developed starting in 2001 by the Center for Information Policy Leadership (CIPL). CTR. FOR INFO. POL'Y LEADERSHIP, MULTI-LAYERED NOTICES EXPLAINED (2005), http://mddb.apec.org/documents/2005/ECSG/DPM1/05_ecsg_dpm 1_003.pdf; *see also* CTR. FOR INFO. POL'Y LEADERSHIP, TEN STEPS TO DEVELOP A MULTILAYERED PRIVACY NOTICE (2006), https://www.huntonprivacyblog.com/wp-content/files/2012/07/Centre-10-Steps-to-Multilayered-Privacy-Notice.pdf.

162. For example, the Article 29 Working Party's recommendations to Google on its 2012 privacy statement included a recommendation that Google adopt a layered privacy statement. *See supra* Part III.A.

163. Google's first privacy video, *Google Search Privacy: Plain and Simple*, was released on August 8, 2007. Google, *Google Search Privacy: Plain and Simple*, YOUTUBE (Aug. 8, 2007), https://www.youtube.com/watch?v=kLgJYBRzUXY. Since then, Google has published additional privacy videos, and other companies have followed suit. For a recent example, see AVG Technologies, *AVG's Privacy Policy*, YOUTUBE (Sept. 14, 2015), https://www.youtube.com/watch?t=15&v=JTwMWKBtCwA.

164. *See* Brian Lich, *Configure Windows Telemetry in Your Organization*, MICROSOFT, https://technet.microsoft.com/en-us/itpro/windows/manage/configure-windows-telemetry-in-your-organization (last updated Jan. 13, 2017).

165. *See, e.g.*, *Government Requests Report*, FACEBOOK, https://www.facebook.com/about/government_requests (last visited May 17, 2017) (providing transparency reports from Facebook); *Google Transparency Report*, GOOGLE, http://www.google.com/transparencyreport/ (last visited May 17, 2017); *Twitter Transparency Report*, TWITTER, https://transparency.twitter.com/ (last visited May 17, 2017); *Our Commitment to Transparency*, MICROSOFT, https://www.microsoft.com/en-us/about/corporate-responsibility/reports-hub (last visited May 17, 2017); *Transparency Report: Overview*, YAHOO!, https://transparency.yahoo.com/ (last visited May 17, 2017).

statements. It should not be the place to hide inconvenient or unflattering facts.

VI. CONCLUSION

When it comes to the length of a privacy statement, there is no formula to determine the right number of pages or words. Every organization, every consumer service, every technology, every data collection method, and every business model is different. And depending on these factors, it can take wildly different amounts of text to adequately describe them. Yes, that means that some privacy statements can be quite long—perhaps even as long as some great works of literature.

But the length of the privacy statement is not really the point. The much more important consideration is whether the privacy statement has been drafted in a way that maximizes transparency and accountability. In seeking to maximize those important objectives, those drafting privacy statements must consider the multiple audiences for a privacy statement. The average consumer may not read it. But certain highly motivated consumers will. For them, having detailed information presented in a clear and straightforward way can be critical. Other audiences can serve as proxies for the average consumer who will not read it. Journalists, advocates, regulators and others can raise public awareness and create incentives for organizations to adopt good privacy practices.

There is an important balance to be struck. A privacy statement drafted with the singular aim of making it short and simple will provide little useful information and will not result in increased transparency. On the other hand, a privacy statement that is longer than it needs to be will make it more difficult to find the important details.

Privacy statements today certainly have room to improve. There are too many examples of privacy statements that are difficult or impossible to comprehend. But, the solution is not to simply shorten and simplify. The better path is to focus on clear and straightforward writing and on presenting the privacy statement in a format and structure that makes finding information easy.