Minnesota Journal of Law, Science & Technology

Volume 20 | Issue 1 Article 3

1-6-2019

Predictability for Privacy in Data Driven Government

Jordan Blanke
Mercer University

Janine Hiller
Virginia Tech

Predictability for Privacy in Data Driven Government

Jordan M. Blanke* and Janine S. Hiller†

Abstract

The Deferred Action for Childhood Arrivals program (DACA) required individuals to provide a great deal of personal information in order to participate and remain in the United States legally; could information in the same system now be used for deportations? More broadly, how should systems of data that are created legitimately by United States agencies and compiled for one reason, be used for other reasons? The increasing emphasis on "smart cities" that use data to efficiently provide and plan for service delivery will require the integration of data from multiple government and non-government sources, in ways that citizens may not expect. There are increasing calls for the federal government to open up and share the data collected for one reason for use in additional, unrelated ways, and to combine that data with data collected by commercial, private entities. Systems design for enabling citizen privacy is essential for a foundation of trust between public agencies and citizens. For example, the Census Bureau is beginning to take additional steps to protect the facially anonymous statistics that it releases, due to concerns that individuals may be identified by increasingly sophisticated technical means that link data to persons. To address privacy

---

* Ernest L. Baskin, Jr. Distinguished Professor of Computer Science and Law at the Stetson School of Business and Economics at Mercer University in Atlanta

† R.E. Sorenson Professor of Finance and Professor of Business Law at the Pamplin College of Business, Virginia Tech.

The authors thank the Privacy Law Scholars Conference, Professor Margaret Hu, Washington and Lee University, and Jocelyn Aqua, PWC, for their helpful comments.

in fast growing and evolving government information systems, the National Institute for Standards and Technology (NIST) proposes a systems approach to protect the privacy of personally identifiable information held by federal agencies. It adopts a privacy engineering and risk management approach with three privacy engineering objectives: predictability, manageability, and disassociability. Because of its fundamental importance to the effective protection of privacy, this article focuses on the first privacy engineering objective: predictability. Predictability is not an established term in the privacy literature. Therefore, this article analyzes the concept of predictability, what it may mean and how it may evolve, and then analyzes it by means of established legal concepts. Nonobviousness in patent law and the reasonable expectation standard in privacy jurisprudence provide lessons for the creation and maintenance of more trustworthy systems and the protection of citizen privacy.

INTRODUCTION

The Deferred Action for Childhood Arrivals program (DACA) required individuals to provide a great deal of personal information in order to participate and remain in the United States legally; could information in the same system now be used for deportations?[1] More broadly, how should systems of data that are created legitimately by United States agencies and compiled for one reason, be used for other reasons? Data collected by local governments in order to provide services, such as water and sewer, might be useful for predicting family growth and school populations, for example. The increasing emphasis on "smart cities" that use data to efficiently provide and plan for service delivery will require the integration of data from multiple government and non-government sources, in ways that citizens may not expect.[2] Furthermore, there are increasing calls for the federal government to open up data collected for one reason for use in additional, unrelated ways, and to combine that data with data collected by commercial, private entities.[3] Though well-defined data can beneficially inform decision making, without updated, intentional, integrated protections, citizens' privacy may be the victim. Certainly, data breaches are a concern, but those are not the only threats to privacy as "there is increasing use of government statistical data by private organizations that seek to link data collected for statistical purposes with identifiable individuals."[4] Indeed, the Census Bureau is beginning to take additional steps to protect the facially anonymous statistics that it releases, due to concerns that individuals may be

---

1. *See* Caitlin Dickson, *'DREAMers' Gave Up Their Personal Info for DACA. They Wonder, Will the U.S. Use It to Deport Them?* YAHOO NEWS (Sept. 7, 2017), https://www.yahoo.com/news/dreamers-gave-personal-data-daca-now-wonder-will-u-s-use-deport-204512167.html.

2. *See* Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581 (2014); Janine S. Hiller & Jordan M. Blanke, *Smart Cities, Big Data, and the Resilience of Privacy*, 68 HASTINGS L.J. 309 (2017).

3. *See* NATIONAL ACADEMY OF SCIENCES, ENGINEERING AND MEDICINE, INNOVATIONS IN FEDERAL STATISTICS: COMBINING DATA SOURCES WHILE PROTECTING PRIVACY 11 [hereinafter INNOVATIONS IN FEDERAL STATISTICS] (Robert M. Groves and Brian A. Harris-Kojetin, Eds., 2017) (making it clear, however, that statistical uses should not identify individuals and that privacy protections are essential); COMMISSION ON EVIDENCE BASED POLICY MAKING, THE PROMISE OF EVIDENCE BASED POLICY-MAKING (2017).

4. *See* INNOVATIONS IN FEDERAL STATISTICS, *supra* note 3, at 74.

identified by increasingly sophisticated technical means that link data to persons.[5]

To address privacy in fast growing and evolving government information systems, the National Institute for Standards and Technology (NIST) proposes a systems approach to protect the privacy of personally identifiable information held by federal agencies (the "Privacy Framework"). It adopts a privacy engineering and risk management approach, introducing two important components: privacy engineering objectives and a privacy risk model. The three privacy engineering objectives proposed in the Privacy Framework are predictability, manageability, and disassociability.

Because of its fundamental importance to the effective protection of privacy, this article focuses on the first privacy engineering objective: predictability. Systems design for enabling citizen privacy is based on a foundation of trust between public agencies and citizens, and NIST identified predictability as one of the building blocks. But when is a system predictable? And who decides when it meets that objective? Predictability is not an established term in the privacy literature. Therefore, this article analyzes the concept of predictability, what it may mean and how it may evolve, and then analyzes it by means of established legal concepts. Administrators who apply a predictability objective to systems of information can learn from lessons found in patent law and Fourth Amendment jurisprudence, and as a result create more trustworthy systems.

The article proceeds in four parts. Part I discusses the fundamental background of privacy principles and their relationship to federal policies about data systems. Part II describes the development of and relationship between the Cybersecurity Framework and the Privacy Framework. Part III focuses on understanding the building block of predictability, examining its meaning and comparing it to analogous concepts that are found in patent law nonobviousness and reasonable expectation jurisprudence. In an era of increased pressure on government agencies to make the information in their systems widely available, the Conclusion proposes that agencies should consider whether the gap between old and potentially new uses of data is too wide, whether there is hindsight bias in risk

---

5. *Id.* at 75.

assessments, and if the very analysis that they perform is diminishing the assumptions that there is some personal information that should remain private.

I. INFORMATION SYSTEM PRIVACY AND GOVERNMENT POLICY

Fair Information Privacy Practices, in one form or another, are foundational principles for privacy protection around the globe, and rules and policies are primary sources for management of information in the government. The NIST Privacy Framework, privacy objectives, and government policy, refer to and implement many of these practices.

A. FAIR INFORMATION PRIVACY PRACTICES

In 1973 the Department of Health, Education, and Welfare produced a document, *Records, Computer, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems*, that would become the basis for much of modern information privacy theory.[6] The report, which was initially called the Code of Fair Information Practices, but has become more widely known as the Fair Information Practice Principles (FIPPs), listed five principles:

- There must be no personal data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.[7]

These five principles have been the basis for most subsequent guidelines regarding informational privacy and data protection. In 1980, the Organization of Economic

6. U.S. DEP'T OF HEALTH, EDUC., & WELFARE, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS 41–42 (1973).

7. *Id.*

Cooperation and Development (OECD) produced another influential and slightly expanded enumeration of these principles in its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (the "OECD Guidelines").[8] The basic principles are: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation, and Accountability.[9]

---

8. Org. of Econ. Cooperation and Dev. [OECD], *The OECD Privacy Framework*, at 3 (2013).

9. The OECD principles are, in full:

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

a) with the consent of the data subject; or

b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. Individuals should have the right:

a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;

b) to have communicated to them, data relating to them

i. within a reasonable time;

ii. at a charge, if any, that is not excessive;

iii. in a reasonable manner; and

The OECD Guidelines were a primary source for the development of the European Data Directive of 1995[10] and the newly enacted General Data Protection Regulation[11] (which became effective in May 2018). They are also largely the basis for the current iteration of FIPPs adopted by many federal agencies and incorporated into the Office of Management Budget's very important 2016 revision.

B. FEDERAL RULES AND POLICIES

The requirements of the Office of Management and Budget's updated Circular A-130 (A-130) "apply to the information resources management activities of all agencies of the Executive Branch of the Federal Government."[12] Among the most important basic principles stated in the document are:

> Government agencies shall be open, transparent, and accountable to the public.
>
> Protecting an individual's privacy is of utmost importance. The Federal Government shall consider and protect an individual's privacy throughout the information life cycle.
>
> While security and privacy are independent and separate disciplines, they are closely related.
>
> The design of information collections shall be consistent with the intended use of the information, and the need for new information shall be balanced against the burden imposed on the public, the cost of the collection, and any privacy risks.[13]

---

iv. in a form that is readily intelligible to them;

c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and

d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above. *Id.* at 14–15.

10. Directive 95/46, on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (EC).

11. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and repealing Directive 95/46/EC, 2016 O.J. (L 119), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=EN [https://perma.cc/ENB6-HFWK].

12. OFFICE OF MGMT. AND BUDGET, CIRCULAR NO. A-130 (2016), https://iapp.org/media/pdf/resource_center/a130revised.pdf.

13. *Id.* at 3–4.

A-130 also sets a number of policy goals for agencies that need to be "specific, verifiable, and measurable, so that progress against these goals can be tracked."[14] Regarding inventories of data, agencies shall

> Maintain an inventory of the agency's information systems that create, collect, use, process, store, maintain, disseminate, disclose, or dispose of PII to allow the agency to regularly review its PII and ensure, to the extent reasonably practicable, that such PII is accurate, relevant, timely, and complete; and to allow the agency to reduce its PII to the minimum necessary for the proper performance of authorized agency functions.[15]

With regard to governance, agencies must "[r]equire that information security and privacy be fully integrated into the system development process."[16] With regard to information management and access, agencies must incorporate into their planning, budgeting, governance, and other policies, that "[f]ederal information is properly managed throughout its life cycle, including . . . creation, use, processing, storage, maintenance, dissemination, disclosure, and disposition."[17] Agencies must also ensure that "[f]ederal information and information systems are managed in a manner that identifies and mitigates privacy and security risks."[18]

An entire section of A-130 is devoted to Privacy and Information Security. In the subsection pertaining to privacy, agencies are directed to

> Establish and maintain a comprehensive privacy program that ensures compliance with applicable privacy requirements, develops and evaluates privacy policy, and manages privacy risks;
>
> Limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of agency functions;
>
> To the extent reasonably practicable, ensure that PII is accurate, relevant, timely, and complete, and reduce all PII to the minimum necessary for the proper performance of authorized agency functions;

---

14. *Id*. at 5.

15. *Id*. A-130 provides that "'[p]ersonally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." *Id*. at 33.

16. *Id*. at 9.

17. *Id*. at 14.

18. *Id*.

> Take steps to eliminate unnecessary collection, maintenance, and use of Social Security numbers, and explore alternatives to the use of Social Security numbers as a personal identifier;
>
> Conduct privacy impact assessments when developing, procuring, or using IT; and
>
> Maintain and post privacy policies on all agency websites, mobile applications, and other digital services, in accordance with the E-Government Act and OMB policy.[19]

With regard to Information Security, A-130 mandates that agencies implement standards and guidelines contained in NIST Interagency or Internal Reports (NISTIRs), including the Cybersecurity Framework and Privacy Framework.[20] Appendix II to A-130 addresses an agency's Responsibility for Managing Personally Identifiable Information.[21] It states that while FIPPs are not OMB requirements, "they are principles that should be applied by each agency according to the agency's particular mission and privacy program requirements."[22] OMB finds that "FIPPS retain a consistent set of core principles that are broadly relevant to agencies' information management practices."[23] The FIPPs as applicable to federal agencies are

> *Access and Amendment*. Agencies should provide individuals with appropriate access to PII and appropriate opportunity to correct or amend PII.[24]
>
> *Accountability*. Agencies should be accountable for complying with these principles and applicable privacy requirements, and should appropriately monitor, audit, and document compliance. Agencies should also clearly define the roles and responsibilities with respect to PII for all employees and contractors, and should provide

---

19. *Id*. at 16–17.

20. *Id*. at 18.

21. *Id*. at Appendix II-1. Personally identifiable information (PII) is defined as "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual" and is necessarily very broad. *Id*. Appendix II discusses that agencies have to be very careful in determining what information is PII and that in some cases, information that was not PII can become PII when combined with other information. An agency needs to evaluate the "sensitivity of each individual data element that is PII, as well as all of the data elements together" and consider that the "sensitivity level of the PII will depend on the context." *Id*. at Appendix II-2.

22. *Id*. at Appendix II-2.

23. *Id.*

24. *Id.* While "access and amendment" often appears as part of "individual participation," the OMB notes that it is including it as a stand-alone principle in A-130 "to emphasize the importance of allowing individuals to access and amend their information when appropriate." *Id*. at Appendix II-2 n.116.

appropriate training to all employees and contractors who have access to PII.[25]

Authority. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII if they have authority to do so, and should identify this authority in the appropriate notice.[26]

Minimization. Agencies should only create, collect, use, process, store, maintain, disseminate, or disclose PII that is directly relevant and necessary to accomplish a legally authorized purpose, and should only maintain PII for as long as is necessary to accomplish the purpose.[27]

Quality and Integrity. Agencies should create, collect, use, process, store, maintain, disseminate, or disclose PII with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to ensure fairness to the individual.[28]

Individual Participation. Agencies should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the creation, collection, use, processing, storage, maintenance, dissemination, or disclosure of PII. Agencies should also establish procedures to receive and address individuals' privacy-related complaints and inquiries.[29]

Purpose Specification and Use Limitation. Agencies should provide notice of the specific purpose for which PII is collected and should only use, process, store, maintain, disseminate, or disclose PII for a purpose that is explained in the notice and is compatible with the purpose for which the PII was collected, or that is otherwise legally authorized.[30]

Security. Agencies should establish administrative, technical, and physical safeguards to protect PII commensurate with the risk and magnitude of the harm that would result from its unauthorized access, use, modification, loss, destruction, dissemination, or disclosure.[31]

Transparency. Agencies should be transparent about information policies and practices with respect to PII, and should provide clear

---

25. *Id*. at Appendix II-3.

26. *Id*. at Appendix II-3. While "authority" often appears as part of "purpose specification," the OMB notes that it is including it as a stand-alone principle in A-130 "to emphasize the importance of identifying a specific authority for creating, collecting, using, processing, storing, maintaining, disseminating, or disclosing PII." *Id*. at Appendix II-2 n.117.

27. *Id*. at Appendix II-3. The OMB notes that "minimization" is referred to as "collection limitation" in some versions of the FIPPs, such as in the OECD Guidelines. *Id*. at Appendix II-3 n.118.

28. *Id*. at Appendix II-3.

29. *Id.*

30. *Id.*

31. *Id.*

> and accessible notice regarding creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII.[32]

As described in Part II, NIST relates the predictability objective to the OMB circular, and to the FIPPs of authority, accountability, use and purpose limitation, and transparency.[33]

II. THE NIST FRAMEWORKS

The Privacy Framework follows from a successful and earlier cybersecurity risk framework (the "Cybersecurity Framework").[34] The Cybersecurity Framework was required to be implemented by federal entities, but it was subsequently widely adopted by the private sector.[35] Because the Privacy Framework evolved from the Cybersecurity Framework and is an integrative part, it is relevant to briefly discuss its history and parallel to the Privacy Framework.

A. THE CYBERSECURITY FRAMEWORK

In 2013, President Obama issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity."[36] Among

---

32. *Id*. at Appendix II-2-3. The OMB notes that "transparency" is referred to as "openness" in some versions of the FIPPs, such as in the OECD Guidelines. *Id*. at Appendix II-3 n.119.

33. *See infra* Part III.

34. *See* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, DEPARTMENT OF COMMERCE LAUNCHES COLLABORATIVE PRIVACY FRAMEWORK EFFORT (Sept. 4, 2018), https://www.nist.gov/news-events/news/2018/09/department-commerce-launches-collaborative-privacy-framework-effort (stating that the success of the Cybersecurity Framework has provided guidance in developing the Privacy Framework). *See generally* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1 (2014), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf ("In enacting this policy, the Executive Order calls for the development of a voluntary risk-based Cybersecurity Framework–a set of industry standards and best practices to help organizations manage cybersecurity risks.") [*hereinafter* CYBERSECURITY FRAMEWORK].

35. *See* Armand J. Zottola, *NIST in the Private Sector*, DIG. RIGHTS REVIEW (Venable LLP Wash. D.C.), March 22, 2017, at 1, available at http://www.lexology.com/library/detail.aspx?g=2878150e-9c01-4c05-b6fd-06dbac58b4f7 (describing how the reach and influence of the Cybersecurity Framework has extended to the private sector).

36. *See* Improving Critical Infrastructure Cybersecurity, 78 Fed. Reg. 11739, 11739–40 (Feb. 12, 2013) (identifying privacy and civil liberties protections as essential in Section 5, and specifically naming the Fair Information Practices Principles as a fundamental building block).

other action items, the executive order tasked NIST with creating a Cybersecurity Framework that

> [I]nclude[s] a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks. The Cybersecurity Framework shall incorporate voluntary consensus standards and industry best practices to the fullest extent possible. The Cybersecurity Framework shall be consistent with voluntary international standards when such international standards will advance the objectives of this order, and shall meet the requirements of the National Institute of Standards and Technology Act . . . [37]

Furthermore, NIST was instructed to produce a framework that would "[p]rovide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk."[38] The Executive Order set the approach for creating secure cyber systems by focusing on the creation of a common language, employing a risk management approach, and requiring engagement across sectors, including voices from public and private entities.[39] Over the next year, NIST held public meetings and received comments from a wide variety of interest groups and stakeholders across multiple domains.[40] While it is beyond the scope of this article to review the Cybersecurity Framework in detail, it is important to understand how it addressed the issue of privacy, and furthermore, how the framework has been widely accepted by the private sector cybersecurity community.[41] The Cybersecurity Framework set the stage for work in the privacy arena,[42] and the wide acceptance of the cybersecurity approach

---

37. *Id*. at 11741.

38. *Id*.

39. *See* CYBERSECURITY FRAMEWORK, *supra* note 34, at 1 (explaining how the Executive Order was implemented through the Cybersecurity Framework).

40. *See* Janine S. Hiller & Roberta S. Russell, *Modalities for Cyber Security and Privacy Resilience: The NIST Approach*, 2015 PROC. OF THE ISCRAM, May 24–27, at 2.

41. *See* Zottola, *supra* note 35, at 1 (explaining the adoption of the Cybersecurity Framework in the private sector).

42. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 34, ¶ 3 ("We've had great success with broad adoption of the NIST Cybersecurity Framework, and we see this as providing complementary guidance for managing privacy risk.") (quotation omitted).

may help analogize how the NIST Privacy Framework might be similarly adopted and implemented.

The Cybersecurity Framework built a common terminology and described a process for identifying and protecting assets, detecting threats and vulnerabilities, responding to attacks, and recovering from breaches.[43] It provided a methodology to create an institutional profile, against which industry benchmarking could be carried out to understand the relative position of an organization and its cyber security strengths and weaknesses.[44] Throughout, the framework included specific actions and references to specific best practices, international norms, industry standards, and existing cyber security processes.[45] The resulting Cybersecurity Framework implemented a risk management approach, intended to be flexible and adaptable to a wide variety of government and private sector critical infrastructures.[46] It is important to note that in addition to the federal systems where the NIST Cybersecurity Framework can be mandatory, a great number of private sector players have also voluntarily adopted the approach.[47] While there were criticisms, the NIST

---

43. *See* CYBERSECURITY FRAMEWORK, *supra* note 34, at 1, 7 (explaining the basics of the framework as providing a common language, identifying and prioritizing risk and managing cybersecurity across an entire organization)

44. *See id.* at 4–5 ("The *Framework Core* is a set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors." This Core is then used to create a "Framework Profile" which can be used to benchmark and guide decision making).

45. *See id.* at 1 ("The Framework provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.").

46. *See id.* ("The Framework enables organizations – regardless of size, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.").

47. "A recent Gartner study reported that NIST's Cybersecurity Framework is already used by 30% of U.S. organizations. This number is expected to rise to 50% by 2020. According to a March 2016 survey by Dimensional Research, 70% of these organizations adopted the framework to align themselves with cybersecurity best practices, 29% were required to do so by business partners, and 28% adopted the framework because of federal contract requirements." Zottola, *supra* note 35, at 1. There are applications in health, *see* Lee Kim, *Building Holistic, Robust Security with the NIST Cybersecurity Framework*, HIMMS BLOG (Apr. 18, 2017), http://www.himss.org/news/ building-holistic-robust-security-nist-cybersecurity-framework (calling for the adoption of the NIST Cybersecurity Framework by healthcare organizations), and critical infrastructure, *see* U.S.

Cybersecurity Framework addressed cybersecurity in a systematic way that promoted enterprise decision making to assess capabilities, strengthen cyber security, and reduce vulnerabilities.[48] The NIST cybersecurity risk management framework has been a successful core document and has been used not only by public agencies but by private business as well.[49]

Cybersecurity and privacy are clearly not identical concerns, but NIST recognized their complex relationship by stating that "[i]ntegrating privacy and cybersecurity can benefit organizations by increasing customer confidence, enabling more standardized sharing of information, and simplifying operations across legal regimes."[50] Privacy

---

DEPT. OF HOMELAND SECURITY, COMPUTER EMERGENCY READINESS TEAM, CYBERSECURITY FRAMEWORK https://www.us-cert.gov/ccubedvp/cybersecurity-framework (last visited Nov. 19, 2018) (explaining critical infrastructure the Cybersecurity Framework can be used to protect); PRICEWATERHOUSECOOPERS LLP, WHY YOU SHOULD ADOPT THE NIST CYBERSECURITY FRAMEWORK 1 (2014), https://www.pwc.com/us/en/increasing-it-effectiveness/ publications/assets/adopt-the-nist.pdf ("Framework targets organizations that own or operate critical infrastructure."), and there is a proposed bill built on the framework, *see* Press Release, Congressman Ralph Abraham, Abraham Introduces the NIST Cybersecurity Framework Bill (February 28, 2017), https://abraham.house.gov/media-center/press-releases/abraham-introduces-nist-cybersecurity-framework-bill ("H.R. 1224 takes steps to prompt federal agencies to follow National Institute for Standards and Technology's (NIST) widely accepted cybersecurity protocols and technical standards.").

48. *See* CYBERSECURITY FRAMEWORK, *supra* note 34, at 13 ("An organization can use the Framework as a key part of its systematic process for identifying, assessing, and managing cybersecurity risk.").

49. *See* Zottola, *supra* note 35, at 1 ("[I]ts influence and standards are widely seen in the private sector and in many private sector commercial agreements.").

50. CYBERSECURITY FRAMEWORK, *supra* note 34, at 3. NIST recently released a document combining, for the first time, controls for both security and privacy; *see also* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY SPECIAL PUBLICATION 800-53, REVISION 5 (2017), http://csrc.nist.gov/publications/drafts/800-53/sp800-53r5-draft.pdf. It states that it "provides a catalog of security and privacy controls for federal information systems and organizations." *Id*. at ii. "NIST continues to work with the privacy community to better integrate privacy and security controls, and is particularly interested in how best to achieve such integration in this publication." *Id*. at vi. The "latest draft goes beyond both information security and the federal government to address ways all kinds of organizations can maintain security and privacy in their interconnected systems." NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST CRAFTS NEXT-

protection was embedded in the Cybersecurity Framework in the sense that privacy impacts were part of a "general set of considerations" within the cybersecurity audit, privacy legal compliance activities, and training.[51] Privacy was more specifically addressed, in part, within a parallel document called the "Roadmap," released at the same time as the Cybersecurity Framework and meant to be a practical implementation aid.[52] The Roadmap to the Cybersecurity Framework criticized the widely recognized FIPPs as being inadequate from a systems and risk management viewpoint because they lacked common definitions for privacy and privacy harms, and contained no metrics for measuring success or determining best practices.[53] The Cybersecurity Framework and Roadmap led NIST to work towards a parallel privacy systems and risk approach to tackle privacy concerns.

B. THE PRIVACY FRAMEWORK

NIST began its work on creating a privacy framework along the same lines as the Cybersecurity Framework by first bringing stakeholders together. The first workshop in April 2014 produced a debate between privacy scholars and systems developers around creating a common terminology with which multiple sides could communicate:

> A key objective of the workshop was to explore the proposition that development of privacy framework components analogous to other engineering fields would enable the creation of reusable, standards-based tools and practices for developers. These tools and practices would facilitate the design and maintenance of systems and technologies with strong privacy postures.[54]

GENERATION SAFEGUARDS FOR INFORMATION SYSTEMS AND THE INTERNET OF THINGS (Aug. 15, 2017), https://www.nist.gov/news-events/news/2017/08/nist-crafts-next-generation-safeguards-information-systems-and-internet.

51. CYBERSECURITY FRAMEWORK, *supra* note 34, at 13.

52. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST ROADMAP FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY, (Feb. 12, 2014), https://www.nist.gov/sites/default/files/roadmap-021214.pdf [*hereinafter* CYBERSECURITY ROADMAP]; *see also* CYBERSECURITY FRAMEWORK, *supra* note 34, at 11 (discussing the roadmap).

53. *See* CYBERSECURITY ROADMAP, *supra* note 52 at 8–9.

54. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, SUMMARY OF THE PRIVACY ENGINEERING WORKSHOP AT THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 1 (Apr. 10, 2014), https://www.nist.gov/sites/default/files/documents/cyberframework/privacy-workshop-summary-052114.pdf.

A NIST goal was to "enable the creation of new systems that mitigate the risk of privacy harm and address privacy risks in a measurable way within an organization's overall risk management process."[55]

In anticipation of the second workshop, in September 2014, NIST published a "NIST Privacy Engineering Objectives and Risk Model Discussion Draft (the "Discussion Draft").[56] The Discussion Draft noted that "[i]n the security field, risk management models, along with technical standards and best practices, are key components of improving security. Similarly, the safety risk management field also has well-developed models, technical standards and best practices. To date, the privacy field has lagged behind in the development of analogous components."[57] For the first time, in an attempt to close that gap, NIST proposed a set of privacy engineering objectives—predictability, manageability, and confidentiality.[58] The Discussion Draft compared these three privacy objectives to the three cybersecurity objectives of confidentiality, integrity, and availability of information.[59] Like the three cybersecurity objectives that would mitigate cyber vulnerabilities, the proposed privacy objectives were intended to allow systems operators to mitigate privacy harms.[60] NIST stated that in developing the three privacy objectives, its staff was guided by its review of "long-standing theories on the concept of privacy such as controlling for surprises and avoiding the 'creepy' factor, self-determination and individuals' interest in controlling their information and freedom from intrusion."[61]

After the second workshop, in May 2015, NIST produced the Draft "*Privacy Risk Management for Federal Information Systems*" (Draft) that combined the elements of privacy

---

55. *Id.*

56. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST PRIVACY ENGINEERING OBJECTIVES AND RISK MODEL DISCUSSION DRAFT (Sept. 15, 2014), https://www.nist.gov/sites/default/files/documents/2017/01/19/nist_privacy_engr_objectives_risk_model_discussion_draft.pdf [hereinafter Discussion Draft].

57. *Id.* at 1. An output of the first workshop was the Discussion Draft.

58. *See id.* at 2–3.

59. *See id.* (comparing cybersecurity and privacy objectives).

60. *See id.* at 3–4.

61. *Id.* at 2 (citations omitted).

engineering and risk management.[62] The Draft again emphasized that "[f]ederal agencies need methods that yield repeatable and measurable results if they are to be able to implement privacy protections in information systems in a consistent manner," and noted that while "existing tools such as the FIPPs and privacy impact assessments (PIAs) provide a foundation for taking privacy into consideration, they have not yet provided a method for federal agencies to measure privacy impacts on a consistent and repeatable basis."[63] The Draft discussed that in other areas, such as cybersecurity, "risk management has played a key role in enabling agencies to achieve their mission goals while minimizing adverse outcomes."[64]

The Draft included three privacy engineering objectives – predictability, manageability, and disassociability—"for the purpose of facilitating the development and operation of privacy-preserving information systems."[65] The objectives were designed "to enable system designers and engineers to build information systems that implement an agency's privacy goals and support the management of privacy risk."[66] Like the three cybersecurity objectives, these three objectives "provide[d] a degree of precision and measurability, so that system designers and engineers, working with policy teams, can use them to bridge the gap between high-level principles and implementation."[67] The Draft noted that federal "agencies have been reliant on principles like the FIPPs that have provided a combination of values, governance principles, and requirements, but lack the concrete conceptualizations"[68] that the three cybersecurity objectives provide. The FIPPS "do not yield an approach for consistent communication of outcome-based aspects of a system that would enable engineers to

62. NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, NIST INTERNAL REPORT 8062, DRAFT PRIVACY RISK MANAGEMENT FOR FEDERAL INFORMATION SYSTEMS (2015), http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.

63. *Id.* at 1.

64. *Id.*

65. *Id.*

66. *Id.*

67. *Id.* at 21.

68. *Id.* at 17.

assess their systems for appropriate capabilities and system design options."[69]

The Draft emphasized that protecting privacy included not only preventing harms to privacy from unauthorized access, but also the "problematic data actions" that occurred during normal system behavior.[70] It included an Appendix that listed and defined problematic data actions such as appropriation, distortion, induced disclosure, insecurity, surveillance, unanticipated revelation, and unwarranted restriction.[71]

In January 2017, NIST published a revised version of the risk management approach (Privacy Framework).[72] The Privacy Framework reiterates the vitality of a privacy engineering and risk management approach, and discusses the additional importance of managing privacy risk as required by the Office of Management and Budget's updated Circular A-130.[73] Under A-130, there is "a new emphasis on managing privacy risk beyond solely compliance with privacy laws, regulations and policies."[74]

The revised draft describes the Privacy Framework and privacy protection as a multidisciplinary task that is constantly pushed by technology, stating that "Technological improvements can provide tremendous individual and societal benefits, but they also can have adverse effects on privacy at both the individual and societal levels. The ideal system would optimize benefits to the individual and society while minimizing the adverse effects."[75] Furthermore, "systems engineering and risk management processes could be used to integrate multidisciplinary approaches that can be incorporated into effective privacy solutions."[76]

---

69. *Id.* at 18.
70. *Id.* at 22.
71. *See id.* at 54 (Appendix E).
72. *See* NAT'L INST. OF STANDARDS & TECH., U.S. DEP'T OF COMMERCE, AN INTRODUCTION TO PRIVACY ENGINEERING AND RISK MANAGEMENT IN FEDERAL SYSTEMS (2017), http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf [hereinafter PRIVACY FRAMEWORK].
73. *See id.* at 3.
74. *Id.*
75. *Id.* at 6.
76. *Id.*

Fundamentally, the Privacy Framework begins from the premise that security and privacy are often intertwined.[77] It discusses how beneficial uses of new technology can inadvertently produce "an unintended consequence or byproduct of the system,"[78] and that while many privacy problems[79] arise from the *unauthorized* use of a system, other problems can arise from the *authorized* processing of information. Examples of problems from *unauthorized* access to PII are fairly well-known. They include "embarrassment or other emotional distress" from the disclosure of information, "economic loss from identity theft, or physical or psychological harm from 'stalking.'"[80] Examples of "[p]roblems from *authorized* processing may be less visible" or understood.[81] These include a discriminatory or stigmatizing effect on those receiving public benefits just from the collection information, frustration from knowledge of inaccurate information or the inability to correct it, and the loss of trust in a system that results in one's avoidance of a product or service that might otherwise be beneficial.[82] Such concerns about privacy and loss of trust in systems "could even contribute to systemic failures in our democratic institutions, such as voting."[83] For these reasons, it is "vital that engineers understand the issue and have the conceptual tools to build systems that minimize problems for individuals when processing their information."[84]

While acknowledging that there is no widely accepted definition of "privacy engineering," the framework adopts a definition as "a specialty discipline of systems engineering

---

77. *See id.* at 7–9.

78. *Id.* at 8.

79. The Privacy Framework adopts the term "privacy problem" to encompass what may otherwise be called privacy harm, privacy violation, privacy intrusion, or privacy invasion. *See id.* at 9–10. "This report uses 'privacy problems' with the goal of enabling system engineers and privacy specialists to more dispassionately discuss the potential adverse consequences arising from the manner in which the system is processing PII." *Id.* at 9.

80. *Id.*

81. *Id.* (emphasis added).

82. *See id.* (detailing the discrimination, frustration, and loss of trust that can result from authorized processing)

83. *Id.* at 9–10 (citing Ira S. Rubinstein, *Voter Privacy in the Age of Big Data*, 2014 WIS. L. REV. 861, 905–06 (2014) which discusses how large-scale data analytics can create privacy concerns in the electoral process outside of the ballot box).

84. *Id.* at 10.

focused on achieving freedom from conditions that can create problems for individuals with unacceptable consequences that arise from the system as it processes PII."[85] The framework discusses that while the FIPPs may have longstanding foundational meaning to those familiar with privacy principles, they provide little guidance for systems designers and implementers because they "contribute little to the development of a repeatable and measurable process that can be understood and communicated inside and outside the organization."[86] The FIPPs "are value statements rather than recipes,"[87] while in contrast a privacy engineering process is an "outcome-based focus provid[ing] the frame of reference that can facilitate translation of privacy principles into system privacy requirements."[88] While privacy officers still need to provide expertise in identifying problems, "system engineers, by gaining an understanding of a clear privacy outcome, would be better positioned to become collaborative partners in the process of building more trustworthy systems."[89] The framework concludes this section of the report by warning that, like any system that contains an element of risk, there should be "no expectation that all privacy risk can be eliminated from a system when it is processing PII."[90]

The report discusses one of the challenges that it had at the very first workshop—"the communications gap between policy and legal teams and the engineering and information technology (IT) teams . . . ."[91] Privacy engineering can help provide an outcome-oriented approach to translating privacy principles to privacy requirements.[92] The framework asserts that these objectives "are not intended to be new statements of policy," but rather, like the Cybersecurity Framework objectives, part of the "core characteristics of the systems."[93] The privacy engineering objectives—predictability,

85. *Id.* at 10–11.
86. *Id.*
87. *Id.* (quoting JULIE MCEWEN ET AL., MITRE CORP., MITRE RESPONSE TO OSTP/NITRD 'NATIONAL PRIVACY RESEARCH STRATEGY' RFI 8 (2014))
88. *Id.* at 12.
89. *Id.*
90. *Id.*
91. *Id.* at 16.
92. *See Id.*
93. *Id.*

manageability and disassociability—"are intended . . . to encourage the implementation of measurable controls for managing privacy risk" and "to help bridge the gap between high-level privacy principles and their implementation within systems."[94]

As early as the 2015 Draft, NIST stated that "[p]rivacy engineering objectives can play an important role in bridging the gap between an agency's goals for privacy and their manifestation in information systems."[95] The 2017 Privacy Framework echoed this sentiment, and stated that the objectives would "provide a degree of precision" leading to "measurable goals for managing privacy risk."[96] By focusing on outcomes, privacy principles can then be translated "into system privacy requirements."[97] The vision is that by understanding the necessary privacy system outcomes, system engineers can be "collaborative partners"[98] with privacy officers.

III. PRIVACY ENGINEERING OBJECTIVES

Three goals for standard setting seems to be de rigueur; the three cybersecurity objectives—confidentiality, integrity, and availability—are widely known information systems goals, and NIST proposes three privacy goals as well.[99] Identification of privacy goals, as described in Part II, was not clear cut, and drafters were not convinced that the comparable, widely known FIPPs could suffice as core objectives or be understood as goals by a privacy engineer.[100] The communication gap that NIST described as a challenge continues, as the three privacy objectives of predictability, manageability, and disassociability, are not generally well known. Part III discusses what these terms mean and how they relate to the FIPPS; Part IV then delves more deeply into the very important meaning of predictability.

---

94. *Id*.
95. *See* NAT'L INST. OF STANDARDS & TECH., *supra* note 62, at 1.
96. PRIVACY FRAMEWORK, *supra* note 72, at 16.
97. *Id*. at 12.
98. *Id*.
99. *See supra* Part II.
100. *See supra* Part II.

A. PREDICTABILITY

The first privacy engineering objective in the Privacy Framework—and the focus of Part IV—is predictability. It is defined as the "enabling of reliable assumptions by individuals, owners, and operators about PII and its processing by an information system."[101] According to the framework, a "reliable sense of what is occurring with PII in a system is core to building trust and accountability, and is a primary part of the underlying rationale for the transparency and accountability FIPPs."[102] It is important because "[b]y framing predictability in terms of *reliable assumptions*, agencies can begin to measure more concretely the capabilities in a system that supports these principles."[103] The framework provides an example of how what has generally been regarded as a privacy principle can become a measurable event.[104] In most circumstances, if notice is provided to a user, the only event observed or recorded is whether the user was provided with notice.[105] In contrast, it is suggested that an assessment could be made as to whether the user "read and understood the notice, or even whether they responded as anticipated."[106]

---

101. PRIVACY FRAMEWORK, *supra* note 72, at 17.

102. *Id.* at 18. Professors Neil Richards and Woodrow Hartzog argue that trust is an "essential ingredient for our digital lives." Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 433 (2016). "Without trust, people share less information, bad information, or no information at all. They become anxious, bewildered, and suspicious . . . . If people don't trust a company, they are more likely to switch to a competitor or resist or fail to become fully invested in the commercial relationship." *Id.* at 435. They argue that "modern privacy law is incomplete because from its inception it has failed to account for the importance of trust." *Id.* "One of the bedrock notions of privacy law is that companies should be transparent about their data collection, use, and disclosure practices so that individuals will be on notice of any potentially worrisome practices and can tailor their disclosures accordingly." *Id.* at 462. "Trust need not be exclusively a matter of government policy. Companies can also voluntarily adopt trust-enhancing internal policies, safeguards, and organizational schemes . . . . Companies can delete data when it is no longer needed and collect no more information than is necessary for the information relationship." *Id.* at 465. These views are obviously quite consistent with the NIST objective of predictability.

103. PRIVACY FRAMEWORK, *supra* note 72, at 18 (emphasis added).

104. *Id.*

105. *Id.*

106. *Id.*

Predictability is also "about designing systems so that *stakeholders are not surprised* by the handling of PII."[107] In this regard, predictability "can support a range of organizational interpretations of transparency—from a value statement about the importance of open processes to a requirements-based program that provides for the publication of how PII is managed."[108] Basic assessment tools, like user surveys, can be used to evaluate whether expectations are consistent with actual practice. Such surveys can also be used to assess whether a system's actual disclosure of information, for example, is in line with assumptions that users have regarding what information about them will be disclosed.

Predictability also supports purpose specification and use limitation.[109] If there is a focus on "maintaining reliable assumptions about processing of PII, predictability could encourage system operators to assess and address the impact of any changes in that processing."[110] If operators are diligent in keeping the users interested and involved in the discussion of their expectations, predictability can facilitate the "maintenance of stable, trusted relationships between systems and individuals . . . ."[111]

B. MANAGEABILITY

The second privacy engineering objective in the Privacy Framework is manageability, which is defined as "providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure."[112] "Manageability is an important system property enabling several of the FIPPs: access and amendment; accountability; minimization; quality and integrity; and individual participation."[113] Systems must be able to administer information at a sufficiently granular level to be able to identify and correct inaccurate information, to dispose of obsolete information, to collect or disclose only necessary

---

107. *Id*. (emphasis added).
108. *Id*. at 18–19.
109. *Id.* at 19.
110. *Id*.
111. *Id*.
112. *Id*. at 17.
113. *Id*. at 19.

information, and to assure that user's privacy preferences are accurately implemented and maintained.[114]

The framework emphasizes that manageability is not a policy statement about whether users should have the right to control their information, but rather a systems requirement that information can be controlled at a level sufficient to perform a variety of required operations on the data. Authority to make those changes is a separate issue.[115]

C. DISASSOCIABILITY

The third privacy engineering objective introduced in the Privacy Framework is disassociability, defined as "enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system."[116] This objective maps primarily across the FIPPs objective of minimization, but also of authority.[117] Disassociability is directed at making sure a system "actively protects or 'blinds' an individual's identity or associated activities from exposure."[118] It "advances the capabilities of a privacy-preserving system by engaging system designers and engineers in a deliberate consideration of points of exposure that are not essential for the operation of the system."[119]

"[A]chieving this objective should reflect the ability of the system to complete [a] transaction without associating information with individuals."[120] For example, while the completion of a health care-related transaction may require associating information with an individual, the association of that information "should not be deemed an operational requirement just because it would be difficult to disassociate the information" from that individual.[121] Agencies must assess the risk involved with associating information with an individual and understand that the recognition of such risk is a separate issue than being able to make that association as an

---

114. *See id.*
115. *Id.*
116. *Id.* at 17.
117. *See id.* at 20.
118. *Id.*
119. *Id.*
120. *Id.*
121. *Id.*

operational requirement.[122] In other words, the agency may choose to accept the risk because it is too difficult or costly to implement stronger, more privacy-preserving controls.[123] It is in this arena that technological advances in cryptography, anonymity, de-identification and others may prove to be extremely useful in mitigating privacy risks.[124]

In summary, the Privacy Framework maps the FIPPs principles of accountability, authority, purpose specification and use limitation, and transparency across the predictability objective; access and amendment, accountability, minimization, quality and integrity, and individual participation across the manageability objective; and accountability and minimization across the disassociability objective. Manageability and disassociability can be accomplished by different technical means by system operators, and stakeholders can debate whether the means are strong or effective enough. These aspects are largely measurable. However, the predictability objective, with its decisions pertaining to data purpose and broader use, is arguably the most important of these interrelated privacy objectives. The definition of predictability is less clear and less satisfying.[125] The definition of predictability presumes that processing of data will evolve and change, that system operators can identify what assumptions stakeholders make about how the data will be used in the future, and can determine and avoid surprising citizens. Maintaining trust is much about preserving predictability,[126] and thus it is essential to analyze this cog that holds the privacy framework together.

IV. THE MEANING AND APPLICATION OF PREDICTABILITY

Predictability is a cornerstone of any rule of law,[127] but particularly in a common law system. The common law is effective when it provides predictability. Individuals and

122. *See id.*
123. *See id.*
124. *See id.*
125. *See id.* at 17.
126. *See supra* note 102 and accompanying text.
127. *See, e.g.*, Antonin Scalia, *The Rule of Law as a Law of Rules*, 56 U. CHI. L. REV. 1175, 1179 (1989) ("[U]ncertainty has been regarded as incompatible with the Rule of Law.").

business can make plans because they have confidence in the predictability of legal outcomes. Much of the rationale for the doctrine of stare decisis is related to the importance of the stability and predictability of the law.[128] In that regard, it is certainly no surprise that one of NIST's privacy engineering objectives is predictability. In order for there to be confidence in a system, its users and those whom it affects should be able to build expectations upon predictability.

NIST is not a policy-setting agency; one of its goals is to promote standardization in technical systems.[129] Because privacy is not a technical system however, any technical standard will necessarily have legal and social implications. The Privacy Framework system goal of predictability needs to be considered from these viewpoints, to analyze whether it is the appropriate systems goal for protecting privacy. The NIST framework does not develop the definition of predictability, yet it is identified as one of the "north stars" for systems design and maintenance to protect privacy. There are no third-party standards for predictability for reference. Ultimately what this section grapples with is: "What does it mean for a system to be predictable so that privacy is protected?"

The following sections analyze the meaning of predictability by using comparisons from the law that are most connected to the concept of predictability as conceived by NIST: (1) preventing surprise; and (2) avoiding creepiness.[130] The analogies we believe are closest to these concepts are patent law's nonobviousness requirement and the Fourth Amendment's reasonable expectation of privacy. To be clear, we are not arguing that there is a direct relationship between these legal concepts and the application of the Privacy Framework to agencies' data actions, but that the comparisons are fruitful and can suggest actions for applying the objective in order to most effectively protect privacy in federal information systems.

---

128. *See, e.g.*, Jeremy Waldron, *Stare Decisis and the Rule of Law: A Layered Approach*, 111 MICH. L. REV. 1, 9–10 (2012) ("Everyone thinks that considerations of [predictability] are of great importance in justifying stare decisis.").

129. *About NIST*, NAT'L INST. STANDARDS & TECH., https://www.nist.gov/about-nist (last updated June 14, 2017).

130. *See* Discussion Draft, *supra* note 56, at 2.

A. PATENT LAW AND NONOBVIOUSNESS

The term "predictability" is found fairly prominently in the legal literature as it applies to determining patent obviousness. There may initially seem to be little relevance between patent law and defining privacy goals for data systems, but interestingly there is a useful parallel, a construct that may help analyze the protection of privacy in a world of swiftly evolving technology.

Patent law requires inventions to be non-obvious in order to obtain intellectual property protection.[131] The same requirement applies to improvements; when an inventor improves upon an existing, patent-protected technology or product, the improvement itself must be non-obvious in order to obtain a patent.[132] The legal determination of whether the improvement is obvious, and therefore not patentable, invokes the question of whether the improvement upon, or a different use of, an existing invention is *predictable*.[133] Obviousness is a legal question, but it is based on a factual determination.[134] The 1966 Supreme Court decision in *Graham v. John Deere*[135] adopted three factual questions relevant to determining

---

131. 35 U.S.C. § 103 (2012) provides that:

A patent for a claimed invention may not be obtained, notwithstanding that the claimed invention is not identically disclosed as set forth in section 102, if the differences between the claimed invention and the prior art are such that the claimed invention as a whole would have been obvious before the effective filing date of the claimed invention to a person having ordinary skill in the art to which the claimed invention pertains. Patentability shall not be negated by the manner in which the invention was made.

We do not extend the analogy too far between patent obviousness and privacy engineering because of differing policies underlying the analysis. In patent law predictability is to be avoided because "[g]ranting patent protection to advances that would occur in the ordinary course without real innovation retards progress and may, in the case of patents combining previously known elements, deprive prior inventions of their value or utility." KSR International Co. v. Teleflex Inc., 550 U.S. 398, 419 (2007). In privacy engineering, predictability is desired in order to support the reliable assumptions, or reasonable expectations, of privacy. General analogy can be helpful to examine the meaning of predictability, but at a more fine-grained level the analogy breaks down due to opposite policy preferences for or against predictability.

132. *See* U.S. PATENT & TRADEMARK OFFICE, MANUAL OF PATENT EXAMINING PROCEDURE § 2141 (9th ed., Jan. 2018) (citing *KSR*, 550 U.S. at 417) [hereinafter MPEP].

133. *Id.*

134. *Id.*

135. 383 U.S. 1 (1966).

obviousness for an improvement: (1) the state of the prior art; (2) the difference between the prior art and the invention; and (3) the ordinary skill of a practitioner in the relevant field.[136] The USPTO explains;

> In short, the focus when making a determination of obviousness should be on what a person of ordinary skill in the pertinent art would have known at the time of the invention, and on what such a person would have reasonably expected to have been able to do in view of that knowledge. This is so regardless of whether the source of that knowledge and ability was documentary prior art, general knowledge in the art, or common sense.[137]

Analogizing patent nonobviousness and predictability inquiries to privacy and predictability for systems engineering, the patent applicant wants the gap to be large and unpredictable so that they may obtain a patent, whereas the systems engineer does not want the gap to surprise stakeholders. Stated another way, predictability is bad for the patent applicant but good for the privacy engineer. The conditions for and analysis of what makes a patent improvement obvious or an information system data processing surprising, are mutually informative, as the information system being assessed is analogous to the improvement upon the existing patent. Applying the *Graham* gap test to the predictability of systems, an engineer first needs to understand the prior art of privacy.

1. Prior Art and Privacy

The state of the art of privacy is analogous to the prior art related to existing patents and common knowledge in the field. As data collection and processing increases, from digital footprints,[138] to increasing sensorization of the environment,[139]

---

136. MPEP *supra* note 132. The USPTO examiner will evaluate the gap based on these facts and will consider additional factors such as "commercial success, long-felt but unsolved needs, failure of others, and unexpected results," to make a determination.

137. *Id.*

138. *See* Mary Madden et al., *Digital Footprints*, PEW RES. CTR. (Dec. 16, 2007), http://www.pewinternet.org/2007/12/16/digital-footprints/.

139. *See* Peter Clarke, *Yole Predicts the 'Sensorization' of Modern Life*, EE TIMES (June 12, 2015), https://www.eetimes.com/document.asp?doc_id=1326858.

to systems of data systems, and predictive analytic systems,[140] this first step makes it essential to have a longitudinal understanding of the privacy environment and how the system processes information in variance from current law and norms. This will be a difficult task, as there is no database similar to the USPTO database that can be searched to determine if there is a history of any similar collection or use of the information in a system, although the USPTO search for prior art is broader than such a theoretical database. The first step would be, however, to interrogate past agency or entity processing of data in a similar manner to begin to understand the prior art, and the stakeholders' reliable assumptions. The discrepancy, however, is that unlike the grant of a patent, past system practices have not been vetted, and the internal investigation of prior systems and their effect will not include external systems that would affect a stakeholder's reliable assumption of how the data will be processed more generally.

Patent examiners are instructed to consider the prior art in both the field in which the invention is situated and the "prior art that is in a field of endeavor other than that of the [patent] applicant . . . or solves a problem which is different from that which the applicant was trying to solve."[141] As difficult as a patent examination is to execute, the privacy engineer's job will be much more complex and difficult. An additional part of the analogy is that just as the patent examination must consider different fields of practice, the privacy engineer should consider different contexts when viewing the prior art. This is the stage at which NIST's reference to the necessity of interactions between the privacy engineer and the privacy officer, and inclusion of laws, regulations, and norms, is essential to establish privacy prior art.

2. Ordinary Skill and Stakeholders

Whether an invention is obvious—or predictable—is measured through the eyes of one who has ordinary skill in the

140. *See* Dennis Hirsh, *Introduction* to *Predictive Analytics Law and Policy: A New Filed Emerges*, 14 I/S: J. L. & POL'Y FOR INFO SOC'Y 1, 1–3 (2017).

141. MPEP, *supra* note 132.

area.[142] In *KSR International Co. v. Teleflex Inc.* ("KSR"),[143] the Supreme Court stated that:

> When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a *predictable* variation, § 103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.[144]

In this context, the definition of who has ordinary skill in assumptions about processing of PII matters greatly, as this defines the eyes through which privacy implications of the system will be viewed; the stakeholder is analogous to the person of ordinary skill in patent law. The USPTO Examination Guidelines explain that,

> The person of ordinary skill in the art is a hypothetical person who is presumed to have known the relevant art at the time of the invention. Factors that may be considered in determining the level of ordinary skill in the art may include: (1) "type of problems encountered in the art;" (2) "prior art solutions to those problems;" (3) "rapidity with which innovations are made;" (4) "sophistication of the technology; and" (5) "educational level of active workers in the field."[145]

The factors relevant to ordinary skill in patent law may also be helpful for analyzing the nature of a reliable assumption; the hypothetical person should understand: the sophistication of the individuals whose PII is being used can change the assumptions of what a system will do, rapidly changing use of PII may make it difficult to make accurate assumptions, and unusual uses of PII or quickly changing uses of PII due to technical advances. Again, the privacy officer could be the best situated to reflect upon both sides of the equation.

3. The Gap Between Old and New

In sum, the patent applicant must show that "the improvement is more than the predictable use of prior art elements according to their established functions."[146] Assessing

142. 35 U.S.C. § 103 (2012).
143. 550 U.S. 398 (2007).
144. *Id.* at 417 (emphasis added).
145. MPEP *supra* note 132.
146. *KSR*, 550 U.S. at 417.

the gap between the prior art and the invention through the view of the skilled person in the area is the final step to determine predictability and nonobviousness. A gap analysis was firmly established as precedent, the core component to decide whether an invention was predictable. In 2007, the Supreme Court in KSR added nuance to the determination by rejecting a formulistic approach to determining obviousness.[147] The Court held that in addition to considering the gap between the inventions and the state of prior art, that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."[148] In cases of inventions that combine the functions of two previously known technologies to create a third, "it can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does."[149] In other words, "a court must ask whether the improvement is more than the predictable use of prior art elements according to their established functions."[150] In addition, secondary considerations should be included in the analysis and subsequent guidance from the USPTO lists these factors:

> (A) Combining prior art elements according to known methods to yield predictable results;
>
> (B) Simple substitution of one known element for another to obtain predictable results;
>
> (C) Use of known technique to improve similar devices (methods, or products) in the same way;
>
> (D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;
>
> (E) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success.[151]

---

147. It is beyond the scope of this article, but the KSR decision has been subject to criticism and the claim that it moves the test for obviousness on a scale previously tending towards objectivity instead towards subjectivity. *See* Gene Quinn, *KSR the 5th Anniversary: One Supremely Obvious Mess*, IP WATCHDOG (Apr. 29, 2012), https://www.ipwatchdog.com/2012/04/29/ksr-the-5th-anniversary-one-supremely-obvious-mess/id=24456/.

148. *KSR*, 550 U.S. at 416.

149. *Id.* at 418.

150. *Id.* at 417.

151. MPEP, *supra* note 132. F and G are not included in the list as they are incorporated into the general analysis discussed above. "(F) Known work in one field of endeavor may prompt variations of it for use in either the same

These elements might be mapped to the flexible uses of PII in information systems and predictability as described by the NIST goal. The question becomes whether the use of PII in a secondary way could arguably be analyzed with regard to a predictable outcome similar to the guidelines for patent predictability. Such mapping could produce the following allowable actions:

(A) PII that has been used predictably in two different ways can be combined if there are predictable results;

(B) Simple substitution of one use for PII for another use for PII to obtain predictable results;

(C) Use of PII in a known way is predictable if used in another system (methods, or products) in the same way;

(D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;

(E) If it is "Obvious to combine" PII – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success.

Professor Christopher Cotropia points out two variations in the predictability analysis within KSR's definition[152] and names these Type I and Type II predictability. Type I predictability is the analysis established before KSR, focusing on the gap between an existing patented technology and the improvement on that technology being reviewed for nonobviousness and patentability.[153] Cotropia summarizes Type 1 predictability analysis as "whether bridging this gap would have been obvious to one skilled in the art or not."[154] Type II predictability, on the other hand, does not focus on the difference between the inventions but rather focuses on the "predictability as to results,"[155] which seems to closely map to

---

field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art; (G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention." *Id.*

152. *See generally* Christopher A. Cotropia, *Predictability and Nonobviousness in Patent Law After KSR*, 20 MICH. TELECOM. & TECH. L. REV. 391 (2014).

153. *Id*. at 397.

154. *Id*.

155. *Id*. at 405.

the NIST goal for privacy engineering. Cotropia criticizes Type II predictability because of its "inability to provide insight to the size of the gap."[156] In sum, Type I predictability asks whether the invention's creation was predictable, whereas Type II asks whether the "invention produces predictable results."[157] This is a significant difference, as it "shifts the substantive questions . . . [to focus on] the invention and how it operates."[158]

There is a striking comparison between the patent analysis of predictability and the use of PII in information systems under FIPPs and the NIST concept of predictability. Similar to Type I analysis, FIPPs data use requirements revolve around a determination of whether the data are being used for purposes that are the same as disclosed, agreed upon, and purposed for; a small or nonexistent gap would result in predictability.[159] The use of the patent examination framework of considering prior art and the ordinarily skilled person could be helpful in this analysis. The NIST approach, however, arguably uses a Type II form of predictability that focuses on the resulting functions of the system and whether the use of PII results in surprise.[160]

A fundamental criticism of Type II predictability is that it results in hindsight bias, or what is commonly known as "Monday Morning Quarterbacking."[161] People tend to analyze past events differently once they know the results. It is much easier to believe an "event is more predictable after it becomes known than it was before it became known"[162] The result is that "because the perspective of the skilled artisan is changed from being prospective to being retrospective," this "increases the likelihood of errors"[163] in determining predictability. In a particularly relevant comment for privacy, Cotropia describes the impact as the "risks of journeying down a development path

156. *Id*. at 407.
157. *Id*. at 412.
158. *Id*. at 424.
159. *See supra* Part I.A.
160. *See supra* Part II.
161. *See, e.g.*, Therese A. Louie, Mahesh N. Rajan & Robert E. Sibley, *Tackling the Monday Morning Quarterbacking: Applications of Hindsight Bias in Decision-Making Settings*, 25 SOC. COGNITION 32 (2007)
162. Neal J. Roese & Kathleen D. Vohs, *Hindsight Bias*, 7 PERSP. ON PSYCHOL. SCI. 411, 411 (2012).
163. Cotropia, *supra* note 152, at 424.

that an ordinary skilled artisan would not have taken."[164] The NIST approach to privacy engineering risks the same hindsight bias by using a Type II predictability analysis that looks back at the way that the system supports reliable assumptions about how PII will be used in that same system. Without at least including a joint Type I analysis that looks at the gap between different uses of the information (prior art) under the standard of the ordinarily skilled artisan, the flexibility that NIST incorporates in its vision may be a self-fulfilling and hollow exercise.

Furthermore, the standard of the ordinarily skilled artisan is deeply connected with the legally prominent concept of the reasonable person, based on the on the benchmark of the ordinarily prudent person. Privacy rights under the Fourth Amendment have for a long time been viewed through the lens of reasonable expectations, which also incorporates this approach.[165] The next section explores these concepts as related to predictability and what it means to have reasonable assumptions about the use of data in an information system.

B. REASONABLE EXPECTATIONS AND PREDICTABILITY

The NIST privacy objectives are applied to data that are in an agency's system of records. They are not meant to be applied to decide whether an agency can collect that data without a warrant and whether the data collection might violate the Fourth Amendment.[166] It should be noted that to that extent, the concept of reasonable expectations, which is part of any discussion about the meaning of privacy in the Fourth Amendment context, is not applicable. But, the definition of predictability, using the term reliable assumptions, is perilously similar to the reasonable expectation term of Fourth Amendment jurisprudence. As the previous discussion of patent nonobviousness and predictability revealed, reasonable

---

164. *Id.*

165. *See infra* Part IV.B.1.

166. *See* Harold Laidlaw, *Shouting Down the Well: Human Observation As a Necessary Condition of Privacy Breach, and Why Warrants Should Attach to Data Access, Not Data Gathering*, 70 N.Y.U. ANN. SURV. AM. L. 323, 353 (2015) ("The administrative information exception is intended to be uncontroversial. Essentially it serves the interest of avoiding formalistic restrictions on the access of data that may be passively gathered but which has historically been considered categorically available to state actors.").

expectations are part of the analysis. For this comparative reason, the next section discusses the history of reasonable expectations, and its challenges for relevance in an era of technological change. How to reliably predict potentially changing assumptions is where the comparison to the reasonable expectation of privacy can be instructive. "[T]he reasonable person's task in the law . . . is the sound resolution of whatever rational conflict the law may throw at him."[167] This also serves the purpose of keeping the determination as a question of fact, rather than a question of law.[168] "[T]he generalisations made in the name of the reasonable person are not legal generalisations. They do not enter the law. They are used by the law to avoid the need for a legal generalisation to be made."[169] This becomes relevant to the notion of predictability as an objective concept that is quantifiable and factual.

1. The Reasonable Expectation of Privacy

Ever since its creation more than fifty years ago in *Katz v. United States*,[170] the "reasonable expectation of privacy" test has served as the barometer for privacy protection under the Fourth Amendment. However, due in large part to evolving surveillance techniques and ubiquitous digital collection of information, this standard may fail. As Professor Daniel Solove stated, "the reasonable expectation of privacy test cannot be resuscitated . . . [and it] is not merely in need of repair—it is doomed."[171] The question is whether the notion of predictability suffers from the same inherent weaknesses, or whether lessons from reasonable expectation jurisprudence can provide a map for avoiding the pitfalls.

In *Katz v. United States*, in order to collect evidence about illegal gambling, the FBI surreptitiously recorded a telephone conversation by attaching a tape recorder on the outside and

---

167. John Gardner, *The Many Faces of the Reasonable Person*, 131 L.Q. REV. 563, 565 (2015).

168. *See id.* at 569 (clarifying that the reasonable person standard is often explained as "a question of fact, not a question of law").

169. *Id.*

170. Katz v. United States, 389 U.S. 347 (1967).

171. Daniel J. Solove, *Fourth Amendment Pragmatism*, 51 B.C. L. REV. 1511, 1521 (2010).

top of two public telephone booths.[172] The defendant made the call from inside one of the two booths after walking in and closing the door behind him.[173] The Supreme Court held that this was an illegal search under the Fourth Amendment because the FBI had violated Katz' privacy.[174] The legacy of the *Katz* case came not from the majority opinion, but rather from Justice Harlan's concurring opinion,[175] which was subsequently adopted by the majority of the Court a year later in *Terry v. Ohio*.[176] The operative language from Harlan's concurrence is:

> My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' Thus a man's home is, for most purposes, a place where he expects privacy, but objects, activities, or statements that he exposes to the 'plain view' of outsiders are not 'protected' because no intention to keep them to himself has been exhibited. On the other hand, conversations in the open would not be protected against being overheard, for the expectation of privacy under the circumstances would be unreasonable.[177]

It is regrettable that over the last fifty years so much emphasis has been placed on trying to make sense of the differences between the supposed two prongs of the *Katz* test, when, arguably, none was intended by the Court.[178] In 2015, Professor Orin Kerr wrote *Katz Has Only One Step: The*

---

172. *Katz*, 389 U.S. at 348.

173. *Id.* at 352.

174. *Id.* at 353.

175. *Id.* at 360–62 (Harlan, J., concurring).

176. *See* 392 U.S. 1, 9 (1968) (citing Katz v. United States, 389 U.S. 347 (1967) (Harlan, J., concurring)).

177. 389 U.S. 347, 361 (Harlan, J., concurring).

178. In two excellent companion articles, Peter Winn and Harvey Schneider discuss the history of the *Katz* case in great detail. Peter Winn, *Katz and the Origins of the "Reasonable Expectation of Privacy" Test*, 40 MCGEORGE L. REV. 1 (2009); Harvey A. Schneider, *Katz v. United States: The Untold Story*, 40 MCGEORGE L. REV. 13 (2009). Schneider was the then twenty-nine-year-old lawyer who argued for Katz before the Supreme Court. Schneider described in detail how he argued to the Court that what he was proposing was an objective test – not a subjective one. He wrote: "We propose a test using a way that's not too dissimilar from the tort 'reasonable man' test . . . we would ask that the test be applied as to whether or not a third person objectively looking at the entire scene could reasonably interpret, and could reasonably say, that the communicator intended his communication to be confidential." *Id*. at 20.

Irrelevance of Subjective Expectations,[179] arguing two significant points. First, the results of an empirical study based upon 540 cases that employed the Katz test showed that, in the vast majority of cases, courts applied only the objective test, and not the subjective test.[180]

Secondly, Kerr makes a convincing argument that Harlan likely never intended that there be a separate, truly *subjective* inquiry, even though subsequent cases and articles have awkwardly attempted or pretended to do so ever since. Kerr focuses on Harlan's statement that the test was "an understanding of the rule that has emerged from prior decisions"[181] and that Harlan "did not intend to create a new test from whole cloth."[182] In order to be consistent with Harlan's assertion that he was not creating a new test, one can read the second sentence as referring to the then-existing line of cases involving a "voluntary exposure of protected spaces" and the third sentence as referring to the then-existing "protected-area cases."[183] This would explain why Harlan referred to this line of cases as "subjective" in nature, and would be consistent with his assertion that the "rule has emerged from prior decisions."[184]

Although it may not have been within the contemplation of the NIST drafters, to meet the predictability objective a system operator will necessarily need to choose *how* to assess individual assumptions about the use of information; this invokes a similar decision and struggle about whether to use a subjective or objective standard, or both. The determination will be affected, one way or another, by changes in technology and by an evolution in assumptions about how systems of data will be used and ultimately how they will impact personal life. Reliable assumptions will be difficult to assess because they can change with the times, circumstances, and social values, so

---

179. Orin S. Kerr, *Katz Has Only One Step: The Irrelevance of Subjective Expectations*, 82 U. Chi. L. Rev. 113 (2015).

180. "The results of the study suggest that the subjective prong of *Katz* is irrelevant. A majority of cases applying *Katz* did not mention subjective expectations. Only 12 percent of *Katz* cases purported to apply the subjective test. Only 2 percent of *Katz* cases claimed to hinge their analysis on the subjective test." *Id*. at 122.

181. *Katz*, 389 U.S. at 361 (Harlan concurring).

182. Kerr, *supra* note 179, at 124.

183. Kerr, *supra* note 179, at 126.

184. *Id*.

comparing them to the history and jurisprudence of the reasonable man standard seems a perfect analogy for the fast-moving subject of data analytics. The analogy provides a warning, as Professor Daniel Solove states that, "the reasonable expectation of privacy test has led to a contentious jurisprudence that is riddled with inconsistency,"[185] and that application of this approach to privacy has "failed to live up to aspirations."[186] In the years following *Katz*, the Supreme Court "adopted a conception of privacy that countless commentators have found to be overly narrow, incoherent, short-sighted, deleterious to liberty, and totally out of touch with society."[187] "As Justice Scalia once stated, 'In my view, the only thing the past three decades have established about the *Katz* test . . . is that, unsurprisingly, [reasonable expectations of privacy] bear an uncanny resemblance to those expectation of privacy that this Court considers reasonable.'"[188]

A brief review of cases following *Katz* shows how the application of the reasonable expectation standard has significantly hampered the law pertaining to privacy protection. In *United States v. Miller*, the Supreme Court held that an individual does not have an expectation of privacy in financial records once he or she has shared them with a bank.[189] In *Smith v. Maryland*, the Court similarly held that there was no expectation of privacy in the list of phone numbers one has dialed once that list has been shared with the phone company.[190] This so-called "third party doctrine" has proven to be a major impediment in protecting informational privacy as it is rare that information today is not shared somehow or someway with someone.[191] These and following decisions[192] have been criticized as being ill-suited for today's

185. Solove, *supra* note 171, at 1511.

186. *Id*. at 1519.

187. *Id*.

188. *Id*. at 1521 (quoting from *Minnesota v. Carter*, 525 U.S. 83, at 97 (Scalia, J., concurring)).

189. *See* United States v. Miller, 425 U.S. 435, at 442 (1976).

190. *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

191. *See* Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087, 1151–52 (2002).

192. In *California v. Ciraolo*, 476 U.S. 207 (1986), the Supreme Court found a defendant to have no reasonable expectation of privacy in his fenced backyard from a private plane flying at an altitude of 1,000 feet because defendant's "expectation that his yard was protected from such surveillance

data-driven world and as over-emphasizing the *secrecy* aspect of privacy: "Life in the modern Information Age often involves exchanging information with third parties, such as phone companies, Internet service providers, cable companies, merchants, and so on. Thus, clinging to the notion of privacy as total secrecy would mean the practical extinction of privacy in today's world."[193] Solove asks: "Would the Supreme Court really hold that people lack an expectation of privacy in their medical information because they convey that information to their physicians? This result would strike many as absurd."[194] It is fair to question whether the reasonable expectation standard has deviated too far from the reasonable person standard, becoming unrealistic and ineffective, by setting bright line distinctions such as the third party test.[195] The reliable assumptions objective could avoid this problem by avoiding a rules oriented approach and remaining true to a standard, such as the reasonable person standard, that considers the circumstances and context.

---

was unreasonable, because '[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed.'" *Id.* 213–14. In *California v. Greenwood*, 486 U.S. 35 (1988), the Supreme Court held that the defendant did not have a reasonable expectation of privacy in the garbage he left at his curb for pickup by the sanitation department. The Court stated that the warrantless search and seizure of the garbage would violate the Fourth Amendment only if the defendant "manifested a subjective expectation of privacy in [his] garbage that society accepts as objectively reasonable . . . [and] that an expectation of privacy does not give rise to Fourth Amendment protection . . . unless society is prepared to accept that expectation as objectively reasonable." *Id.* 39–40.

193. *See* Solove, *supra* note 191, at 1152. In *U.S. v. Jones*, 565 U.S. 400 (2012), the Supreme Court decided that a 4-week attachment of a GPS device to the underbelly of a car violated the Fourth Amendment. Justice Sotomayor, in a concurring opinion, questioned whether the third-party doctrine is still appropriate: "it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. *Id.* at 417 (Sotomayor, J., concurring). She stated that this "approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." *Id.*

194. Solove, *supra* note 171, at 1532.

195. The Supreme Court recently refused to extend the third party doctrine to the cell-site location information that is routinely generated and used by mobile telephones, in *Carpenter v. U. S.*, 138 S. Ct. 2206 (2018). There were five separate opinions in the case with multiple criticisms of the *Katz* test and multiple calls for positive legislation regarding data privacy. *See generally* Jordan M. Blanke, *Carpenter v. United States Begs for Action*, 2018 U. ILL. L. REV. ONLINE 260.

In *Florida v. Riley*,[196] the Supreme Court again foreclosed a variety of potential privacy arguments by making, in retrospect, a very broad holding. While it recognized that the defendant clearly had a *subjective* expectation of privacy in his backyard greenhouse, it held that there was no *objective* expectation of privacy.[197] The plurality held that the defendant "could not reasonably have expected that his greenhouse was protected from public or official observation"[198] as long as the plane was flying in navigable airspace, as "[a]ny member of the public could legally have been flying over [his] property in a helicopter at the altitude of 400 feet and could have observed [his] greenhouse."[199] Justice O'Connor stated in her concurring opinion that the defendant's "expectation of privacy was unreasonable not because the airplane was operating where it had a 'right to be,' but because public air travel at 1,000 feet is a sufficiently routine part of modern life that it is unreasonable for persons on the ground to expect that their curtilage will not be observed from that altitude."[200] This is an extremely broad statement. The three-justice dissent criticized the plurality's decision and Justice O'Connor's observation because under that interpretation, one's "expectation of privacy is defeated if a *single member* of the public could conceivably position herself to see into the area in question without doing anything illegal."[201]

Another line of Supreme Court cases that was decided solely on the basis of the objective standard of the *Katz* test, also resulted in diminishing expectations of privacy. In *O'Connor v. Ortega*,[202] the Court addressed whether a public employee had a reasonable expectation of privacy in his desk drawers and personal file cabinets in his office.[203] The Court stated that the "operational realities of the workplace . . . may make some employees' expectations of privacy unreasonable

196. Florida v. Riley, 488 U.S. 445 (1989).

197. *Id.* at 450. The *Greenwood* and *Riley* holdings are also criticized by Solove as further examples of too narrowly interpreting privacy as secrecy. Solove, *supra* note 171 at 1520–21.

198. *See* Florida v. Riley, *supra* note 196, at 450.

199. *Id.* at 451.

200. *Id.* at 452, 453 (O'Connor, J., concurring).

201. *Id.* at 456, 457 (Brennan, J., dissenting) (emphasis added).

202. 480 U.S. 709 (1987).

203. *See* O'Connor v. Ortega, 480 U.S. 709, 711–12 (1987).

when an intrusion is by a supervisor rather than a law enforcement official."[204] The Court stated that the expectations of both public and private employees in "their offices, desks, and file cabinets . . . may be reduced by virtue of actual office practices and procedures, or by legitimate regulation."[205] This holding, along with those in similar cases, has pretty much solidified the objective societal value (applying the second prong of the *Katz* test) that there is virtually no expectation of privacy in the workplace.

The reasonable expectation of privacy jurisprudence identifies several pitfalls that plague the application of an objective standard. Any agency or company that seeks to apply predictability under the Privacy Framework as a concrete objective can learn from and attempt to avoid these pitfalls. Although predictability is described as a measurable goal, the expectation of privacy cases teach that while applying an objective standard is not simple, efforts to draw strict boundaries can create illogical results. The first issue is that of the dynamic nature of systems change; both technology developments and the adaptation of assumptions are part of that environment. An analysis of how the application of a reasonable expectation standard was not able to keep up with the technology holds lessons for the application of reliable assumptions.

2. Reliable Assumptions and Pitfalls

NIST applies the objective of predictability, defined as reliable assumptions, to the context of all stakeholders: citizens, users, and system administrators alike.[206] This discussion is limited to how the goal of predictability can be understood from the perspective of citizens' reliable assumptions.[207] In a prescient 2002 article, Shaun Spencer described the inevitable erosion inherent in the expectation-

204. *Id.* at 717.

205. *Id.*. at 717. *See infra* notes 177-184 and accompanying text.

206. *See Discussion Draft*, *supra* note 56, 18–19. The Draft does not clearly define a stakeholder. The text discusses agencies and system owners and operators, but the footnotes refer to studies of enabling consumer trust by protecting consumer privacy. We assume that consumers—citizens—are stakeholders, and that their reliable assumptions, and preventing surprise, are key to the privacy framework. The text also refers to assumptions of individuals about how their information will be used. P. 19

207. *Id.*

driven conception of privacy.[208] He accurately predicted how, in an increasingly information-rich environment, there would be incremental encroachments on privacy that would consistently drive down expectations.[209] For example, employees' expectations of privacy slowly shrank each time employers so declared limitations – first in telephone conversations, then in e-mail communications, then in anything stored on one's computer – to the point where there is virtually no expectation of privacy in the workplace today.[210] Similarly, the third party doctrine diminished the expectation of privacy in any kind of information delivered to another person.[211] Spencer described how individuals tend to internalize these successive encroachments and how, over time, the expectation keeps getting smaller and smaller.[212] The cases discussed in the previous section illustrate Spencer's point that, without a significant change in jurisprudence,[213] the reasonable expectation of privacy standard is on a downward spiral. The objective of reliable assumptions will suffer from the same spiral, and affect the fundamental nature of privacy assumptions, unless those applying the Privacy Framework avoid this pitfall.

---

208. *See generally* Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L.R. 843 (2002).

209. *Id.* at 857–58. In the absence of statutory protection for privacy, the standards rely almost exclusively on social norms. When there is legislation, often spurred by some event or some case, that legislation often serves to create or boost society's expectation of privacy. For example, in the aftermath of the disclosure that a reporter in Washington, D.C. was able to obtain a copy of Supreme Court nominee Robert Bork's video rental history, a concerned group of Congressmen very quickly passed legislation to protect those – and their – records. The effect was to elevate the societal expectation of privacy in such records. Similarly, in the aftermath of the unpopular *Olmstead* decision (*Olmstead v. United States*, 277 U.S. 438 (1928)), Congress amended the law to protect interception of telephone communications, thus creating a new expectation of privacy in such communications.

210. *Id.* at 860–62.

211. *Id.* at 860.

212. *Id.* at 863–66.

213. At the time this paper is written, Carpenter v. U.S. is pending a decision before the United States Supreme Court, a case in which discussions of differing views on the nature of expectations of privacy predominated. *See* Jeffrey Rosen, *A Liberal-Conservative Alliance on the Supreme Court Against Digital Surveillance,* THE ATLANTIC (Nov. 30, 2017) https://www.theatlantic.com/politics/archive/2017/11/bipartisanship-supreme-court/547124/.

The second pitfall to be avoided in applying the predictability objective is that it will be difficult to measure reliable assumptions. When Solove describes the inexorable erosion of privacy expectations due to technology he identifies the role that courts play in "bootstrapping" the movement of expectations, and warns that "the government could condition the populace into expecting less privacy."[214] The application of a predictability standard to systems of information will suffer from the same weaknesses unless lessons can be learned from a comparison.

There is a striking similarity between the dilemma of technology and reasonable expectation jurisprudence and data use and reliable assumptions under the goal of predictability. The court that applies the reasonable expectation of privacy to decide if the use of surveillance violates privacy rights, is analogous to the system operator and the determination of risks to privacy and whether the system use of data is predictable. In order to avoid a similar erosion of privacy, *how* the risk management approach to privacy[215] is implemented is key. There are at least three lessons about reliable assumptions to be learned from this analysis.

First, determination of assumptions is a multi-stakeholder process, but citizen vulnerabilities and potential data harms are the most difficult to assess and the most important for maintaining trust. Applying an objective view of predictability, including the circumstances and the context of the information system, but applying it in a systematic way, is important to establish reliability. Second, privacy engineering will be a catalyst for lowering the bar for assumptions of privacy, a bootstrapping exercise, unless care is taken to create a systems approach that lies outside of internal technical biases and third party pressures for access. Third, although data is collected in ever increasing amounts and in more fine-grained ways, similar to the march of surveillance technology, this fact alone should not be used as a basis for designing a system that incorporates the excesses. Numbness should not be equated with predictability.

---

214. Solove, *supra* note 171, 1523–24.

215. A discussion of the implementation of a privacy risk management assessment is beyond the scope of this article, however, under the risk analysis, the definition of vulnerabilities and problematic data actions will be required.

In sum, implementation of the NIST Privacy Framework, in a sustainable and robust way, is likely not a desktop exercise. Engagement with stakeholders, evidence gathering, and protection from creeping liberalization of data sharing should be well recognized weaknesses that are watched and monitored. Otherwise, the trust that comes from reliable assumptions about the predictable way that information systems will be used will turn into cynicism about ways in which citizens are monitored or monetized in an administrative state or industry.

CONCLUSION

Professor Julie Cohen correctly predicted that traditional values regarding "property,"[216] "choice,"[217] "knowledge,"[218] and "speech"[219] would make it very difficult to accommodate informational privacy rights. She argued that there was a need to incorporate protections that hold the data processing industry accountable.[220] NIST privacy engineering may not be a perfect fit, but it is a step in that direction. Cohen argues that "we must use both technology and law" to address privacy threats.[221] The Privacy Framework addresses Cohen's admonition that "privacy consideration has not been uppermost in the [system] design process, but what is chosen can be changed."[222] The underlying philosophy of NIST's approach is found in the privacy objectives, and the first objective, predictability, is at the crux of its success in protecting privacy in information systems. Lessons from comparisons to both the history and jurisprudence of patent nonobviousness, and the reasonable expectation of privacy, can increase the ultimate effectiveness of the Privacy Framework.

In order for predictable systems to create trust and protect privacy, administrators should become adept at monitoring the gaps between old and new uses, and should avoid the hindsight bias of the kind that can plague review of patents for

---

216. *See* Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1377–91 (2000).
217. *Id.* at 1391–402.
218. *Id.* at 1402–08.
219. *Id.* at 1408–23.
220. *Id.*
221. *Id.*
222. *Id.* at 1436.

nonobviousness. The emphasis, instead, should be placed on the prospective use of information, rather than on a retrospective analysis. To maintain reliable assumptions about how information will be used in a system, administrators should learn from the reasonable expectation of privacy jurisprudence that data use creep, like technology creep, can severely diminish privacy protection by small steps, that the Privacy Framework can contribute to the erosion of privacy by bootstrapping, by promoting assumptions that are defined in that very process; and lastly, that determining and maintaining predictable systems requires external interaction with stakeholders and longitudinal validation.

Predictability of a system to protect privacy is a laudable goal, and one day may become as ingrained and successful as the goals in the Cybersecurity Framework. Predictability may help to support the Fair Information Privacy Practices by assessing and implementing purpose and use parameters, but much work is left to be done to define the concept so that it avoids the pitfalls of similar thorny areas. This is an era of increased pressure on government agencies to make the information in their systems widely available. While there may be benefits earned from increased data availability, there can nonetheless be a systemic loss of trust if personal information is later identified or used for different purposes. To avoid predictability being a hollow objective, agencies and voluntary adopters of the Privacy Framework should institute risk management approaches that consider whether the gap between old and potentially new uses is too wide, whether there is hindsight bias in their assessments, and if the very risk analysis that they perform is diminishing the assumptions that there is some personal information that should remain private. The Census Bureau is an example of an agency that recognizes the threats to trust that can result from information system leakage, and it could benefit from the insights into the Privacy Framework under this analysis.