Cyber Security Policy and Research Institute

THE GEORGE WASHINGTON UNIVERSITY

A New Privacy Framework with Criteria Inspired by Fair Information Practice Principles

Samuel Klein and Lance J. Hoffman

Abstract

How does one evaluate and assess policies and practices and compare systems to determine their protection of an individual's privacy? Some frameworks define a set of criteria that individuals can use to compare policies, practices, and systems to determine whether or not their privacy is protected. Other frameworks take a risk-mitigation approach, measuring policies, practices, and systems in terms of the risk they pose to an individual's privacy. The framework described here uses the Fair Information Practice Principles (FIPPs) to develop a criteria-based approach to assessing and evaluating policies and practices and ultimately comparing systems. This framework computes scores that not only reflect the privacy protection of specific components within a system, but also reflect the privacy protections afforded by the system as a whole. The use of it and other frameworks to assess Facebook privacy protection is discussed.

August 28, 2015

Report GW-CSPRI-2015-02

A New Privacy Framework with Criteria Inspired by Fair Information Practice Principles

Table of Contents

1. INTRODUCTION

Privacy policies, privacy notices, privacy statements, data policies, data handling policies, conditions of use, terms of service, terms and conditions—the list goes on. Systems around the globe have adopted all sorts of policies to govern the collection, use, dissemination, and maintenance of others' personally identifiable information (PII). But how do these different policies compare? Are some more transparent than others? Do some make a better effort at minimizing the amount of data they collect or better limit how they use the collected data? Do some make no effort at all? As these systems and their policies become increasingly complex, decision-makers of all varieties (including individuals, national governments, and multinational corporations to name a few) will require tools that help them make better sense of the systems and policies they are dealing with. This paper describes a framework to help such decision-makers assess, evaluate, and compare privacy policies and practices from different systems.

The framework provides a Privacy Score that rates a system's adoption and application of the Fair Information Practice Principles (FIPPs). First, the framework identifies 93 criteria—referred to as System Practices—which a system might follow. Individuals using the framework (e.g., those whose PII is processed and handled by a system they want to evaluate), rate each System Practice for intrusion into or protection of their privacy based on a scale of 1-5. Then, the framework averages these individually inputted ratings to compute the Privacy Score for the entire system. (While the current work averages scores, other functions can be used, including ones that weigh the inputs of various users differently).

2. BACKGROUND

2.1. Existing Privacy Frameworks

Frameworks currently exist for measuring and determining the privacy protections afforded by systems. However, there is a wide variety in the focus of each framework. Some frameworks aim to mitigate risk to ensure privacy protections, while others seek to evaluate and assess written privacy policies to ensure that best practices for protecting privacy are in place and working. Furthermore, some frameworks take an objectives-based approach, seeking to identify and accomplish certain measurable goals, while other frameworks adopt a criteria-based approach, which involves creating a "checklist" of criteria against which privacy policies and practices can be compared.

2.1.1. Privacy Risk Management Framework

The Privacy Risk Management Framework is a framework focused on privacy engineering, and in particular managing and preventing privacy risk. This framework adopts an objectives-based approach to privacy engineering. A recent draft publication entitled *NISTIR 8062: Privacy Risk Management for Federal Information Systems* from the National Institute of Standards and Technology (NIST) seeks to develop a privacy risk management framework that identifies key objectives for agencies and organizations to keep in mind when designing systems

and protecting privacy.[1] These objectives—predictability, manageability, and confidentiality—seek to mitigate risk within systems that process and handle information, especially PII. By identifying standard objectives for agencies and organizations, NIST hopes to develop a repeatable and measurable framework for ensuring privacy protection.

2.1.2. Privacy Trust Framework

The Privacy Trust Framework is a framework focused on evaluating and assessing privacy policies. This framework adopts a criteria-based approach to evaluation and assessment. Patient Privacy Rights (PPR), a non-profit organization dedicated to increasing patient control over their health data, developed a criteria-based approach for evaluating and assessing privacy policies. Known as the Privacy Trust Framework, PPR developed it in conjunction with the Coalition for Patient Privacy, Microsoft, and a health-consulting firm. The framework divides 75 different criteria up among 15 different principles.[2] The 75 criteria are used to rate privacy policies and score them on their level of compliance with the 15 principles. In addition, the Privacy Trust Framework provides guidance to organizations drafting privacy policies by providing them with a foundational set of privacy principles to adopt, transform, and build on.

2.1.3. Generally Accepted Practice Principles

The Generally Accepted Practice Principles are a framework focused on managing and preventing privacy risk. This framework adopts a criteria-based approach to risk-mitigation. The American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants designed the Generally Accepted Privacy Principles (GAPP).[3] This framework seeks to assist accountants create a program for managing and preventing privacy risk. Although GAPP is primarily a risk-mitigation framework, it also aims to help design and implement privacy policies as well as measure performance. However, while this framework is focused on risk-mitigation like NIST's Privacy Risk Management Framework, it is different in that it adopts a criteria-based approach. In particular, the GAPP framework includes 10 principles (similar to the Privacy Trust Framework's 15), with each principle subdivided into more specific criteria (again, similar to the Privacy Trust Framework). The principles and criteria included in this framework were drafted with international privacy regulatory requirements and best practices in mind (such as the European Union's Directive on Data Privacy and the US's Gramm-Leach-

[1] "NISTIR 8062 (Draft): Privacy Risk Management for Federal Information Systems," *National Institute of Standards and Technology*, (May 2015). Accessed 16 June 2015, http://csrc.nist.gov/publications/drafts/nistir-8062/nistir_8062_draft.pdf.

[2] "Privacy Trust Framework," *Patient Privacy Rights*, (2010). Accessed 18 August 2015, http://patientprivacyrights.org/wp-content/uploads/2013/02/PPR_Trust-Framework.pdf.

[3] "Generally Accepted Practice Principles," *AICPA and CICA*, (August 2009). Accessed 16 June 2015, http://www.aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/DownloadableDocuments/GAPP-Principles.pdf.

Bliley Act, the Health Insurance Portability and Accountability Act, and the Children's Online Privacy Protection Act).

2.1.4. Privacy By Design

Privacy by Design is a framework focused on privacy engineering. This framework adopts a criteria-based approach to privacy engineering. Privacy engineering is defined as "engineering privacy directly into the design of new technologies, business practices and networked infrastructure, in order to achieve the doubly-enabled pairing of functionality and privacy."[4] Designed by Ann Cavoukian in the 1990s, the Privacy by Design Framework features seven principles created to direct system designers, application developers, network providers, and others involved in engineering to think about privacy throughout the entire product development process. This framework's focus on engineering privacy provides a strong contrast to evaluation and assessment frameworks that are more focused on compliance with regulations. The concept of Privacy By Design was included in a recent Federal Trade Commission report on protecting consumer privacy, which advocated for companies "to promote consumer privacy … at every stage of the development of their products and services."[5]

2.2. Issues with Current Frameworks

The Privacy Risk Management Framework seeks to make risk assessments based on the likelihood that certain problematic system operations will occur and the impact that these problematic operations will have on individuals. However, the proposed assessments leave little room for including feedback from the actual individuals who may be impacted by such problematic operations. Such feedback would be useful in revealing how severe an impact might be on those individuals. This paper seeks to address this shortfall by using a criteria-based framework that reveals the concerns of individuals. By allowing individuals to rate the various operations of a system according to their level of privacy protection, the framework can help agencies better gauge which problematic operations might have the biggest impact. An agency might predict that a certain problematic operation would have a significant impact on individuals, but the proposed framework could reveal that individuals are actually more concerned with a different problematic operation. (For more information on how this paper's proposed framework applies to the Privacy Risk Management Framework, see Appendix A, "Comments Submitted by the Authors to NIST on its draft of NISTIR 8062." The comments are also available at http://www.cspri.seas.gwu. edu/crowdsourcing-privacy-risk-assessment/)

---

[4] Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles," *Information and Privacy Commissioner of Ontario* (August 2009). Accessed August 27, 2015, https://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf.

[5] "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policy Makers," *Federal Trade Commission*, (March 2012). Accessed August 27, 2015, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

The Privacy Trust Framework, with its focus on health data, becomes very constrained in its ability to evaluate privacy policies and systems outside of the medical industry. This is evident in recent research conducted by Jennifer Shore and Jill Steinman at Harvard University. When Shore and Steinman used the Privacy Trust Framework criteria to evaluate Facebook's privacy policies, they had to exclude over 50 percent of the criteria because it was too specific (they used 33 out of 75 total criteria). In fact, they also pointed out that the criteria failed to capture "all aspects of data handling and sharing."[6] Appendix B lists the 33 criteria used by Shore and Steinman. This paper seeks to address this shortfall by using the FIPPs to guide the identification of other evaluation criteria in addition to the ones already defined by the Privacy Trust Framework. Since the FIPPs are a widely recognized set of principles already used to design privacy policies and systems across industries, they also provide a great starting point for designing criteria to evaluate such policies and systems.

Although the Generally Accepted Practice Principles provide an exhaustive list of criteria that can be used mitigate privacy risk, the framework is mainly intended for managers and system designers who are looking to create effective privacy policies and protections. In contrast, this paper offers a privacy framework that is accessible to more people, in particular the users of systems that process and handle their PII. Creating a framework that enables end-users to evaluate and assess policies, practices, and systems can provide managers and system designers with further input into their policies and systems. That is, rather that solely focusing on the GAPP framework to dictate the creation and management of privacy programs, organizations can also rely on the results produced by the framework proposed in this paper, as these results will reveal the concerns and take into account the considerations of end-users.

2.3. Summary of Frameworks

Table 1 provides an overview and brief comparison of the frameworks discussed in this section. It also introduces (in the shaded row) the new framework proposed in this paper: the FIPP-Inspired System Practices framework. The "focus" column refers to the main intent of the framework: to evaluate and assess, to engineer privacy, or to mitigate risk. The "methodology" column categorizes the different approaches the frameworks take: a criteria-based approach that relies on lists of principles used to rate and score or an objectives-based approach that aims to repeatedly accomplish predefined goals. The "based on" column explains where the criteria used in criteria-based approaches come from or where the objectives used in objective-based approaches come from. Finally, the "target audience" column summarizes who is intended to use the framework.

[6] Jennifer Shore and Jill Steinman, "Did You Really Agree to That? The Evolution of Facebook's Privacy Policy," *Technology Science*: 2015081102, accessed August 18, 2015, http://techscience.org/a/2015081102.

Table 1 Summary of Current Frameworks

Framework	Focus	Methodology	Based On	Target Audience
Privacy Risk Management Framework	Privacy Engineering; Risk Mitigation	Objectives-based	Objectives developed by NIST Workshop	Federal Agencies
Privacy Trust Framework	Evaluation / Assessment	Criteria-based	Principles established by bipartisan Coalition for Patient Privacy	Health Industry
Generally Accepted Practice Principles	Evaluation / Assessment; Risk Mitigation	Criteria-based	National and International Laws and Regulations	Managers; Legal Counsel; System Designers
Privacy by Design	Privacy Engineering	Criteria-based	Principles established by Ann Cavoukian	Device Manufacturers, System Designers, Application Developers, Network Providers
FIPP-inspired System Practices	**Evaluation / Assessment**	**Criteria-based**	**FIPPs**	**General; Users of Systems**

This paper proposes a new criteria-based, evaluation and assessment framework for ensuring privacy protection (bottom row of Table 1, above). This framework's design was based on the FIPPs[7] and is intended for a general audience. The FIPPs stem from the legislative work that produced the Privacy Act of 1974.[8] Although privacy legislation in the United States often takes a sector-specific approach, with individual laws governing health care, financial, and consumer data, the FIPPs provide an overarching framework to ensure similar and consistent privacy policies are adopted. In addition, they aren't only relevant to legislation; they also work to guide private and non-for-profit organizations develop and implement equally consistent privacy policies.

3. OPERATIONALIZING THE FAIR INFORMATION PRACTICE PRINCIPLES: A FIPP-INSPIRED FRAMEWORK

3.1. Definition: System Practices

The FIPPs act as inspiration for identifying the 93 System Practices used in the framework. To quantify a system's impact on an individual, a system is broken down into what this paper refers to as System Practices. A System Practice is any practice or principle that a

[7] "Appendix A – Fair Information Practice Principles (FIPPs)," *National Strategy for Trusted Identities in Cyberspace*, (April 2011). Accessed 6 July 2015, http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

[8] Privacy Act of 1974, 5 U.S.C. § 552a (1974).

system abides by when processing personally identifiable information. The framework divides and organizes System Practices into categories based on the FIPPs. More specifically, there are a total of 93 System Practices divided up among eight, distinct FIPPs. Some FIPPs include more System Practices than others.

3.2. Methodology for Identifying System Practices

System Practices were identified based on the language used to define each FIPP. For example, the language defining the Transparency FIPP focused on *notifying* individuals. Using this keyword, the question: "*what is notifying a function of?*" was asked to identify measurement variables. This led to the identification of "Methods of Notification" and "Frequency of Notification" as two variables that could be used to measure *notifying*. ("*Notifying is a function of the methods used to notify and the frequency with which notification is given.*").

A high level of granularity was sought to ensure a comprehensive evaluation of the system. With regards to the Transparency FIPP, rather than just evaluating "Methods" and "Frequency" in general, they were further subdivided to provide more specific evaluation criteria. To accomplish this, similar questions were again asked: "*what is Methods a function of?*" and "*what is Frequency a function of?*" This led to the identification of different methods of notification (notification in privacy policies, in popups, or in rmails) as well as different frequencies of notification (based on time, usage of data, or type of data). This high level of granularity ensures that System Practices related to Transparency are evaluated based on a wide range of specific criteria, rather than just a few general ones.

3.3. Identified System Practices (Organized by FIPPs)

This section provides an overview of the individual System Practices identified for each FIPP. Each subsection includes an explanation as to how the System Practices were identified as well as a table listing all of the identified System Practices.

3.3.1. Transparency (T).

Six System Practices were identified under the Transparency FIPP, which emphasizes a system's duty to notify its users about collection, use, dissemination and maintenance of data. As such, the System Practices identified primarily seek to evaluate a system's notification processes, including the methods used to notify and the frequency with which notification is given. Time-dependent frequency accounts for the different times when notification might be given: only once before data is first processed, some times before it is processed, or every time before it is processed. Usage-dependent frequency accounts for the different usages of data that might trigger a notification: when data is collected, used, or shared. Data type-dependent frequency accounts for the different types of data that might trigger a notification: publically available data, personal data, or highly sensitive data.

Table 2 System Practices Categorized Under Transparency

T-1	Methods of Notification > Privacy Policy
T-2	Methods of Notification > Popup
T-3	Methods of Notification > Email
T-4	Frequency of Notification > Time Dependent
T-5	Frequency of Notification > Usage Dependent
T-6	Frequency of Notification > Data Type Dependent

3.3.2. Individual Participation (IP).

Twenty-one System Practices were identified under the Individual Participation FIPP, which emphasizes a system's duty to involve the individual in the processing of his or her data. As such, the System Practices identified primarily seek to evaluate a system's consent, access, and redress processes available to the individual. This includes evaluating the different types of consent, access, and redress available to the individual, how often these processes are available, and how easy the processes are to use.

Table 3 System Practices Categorized Under Individual Participation

IP-1	Consent > Frequency of Consent > Time Dependent
IP-2	Consent > Frequency of Consent > Usage Dependent
IP-3	Consent > Frequency of Consent > Data Type Dependent
IP-4	Consent > Options > Opt-in
IP-5	Consent > Options > Opt-out
IP-6	Consent > Difficulty > Timely
IP-7	Consent > Difficulty > Inexpensive
IP-8	Access > Frequency of Access > Time Dependent
IP-9	Access > Frequency of Access > Data Type Dependent
IP-10	Access > Actions Permitted > View
IP-11	Access > Actions Permitted > Download
IP-12	Access > Difficulty > Timely
IP-13	Access > Difficulty > Inexpensive
IP-14	Access > Difficulty > Instructions Provided
IP-15	Redress > Actions Permitted > Dispute
IP-16	Redress > Actions Permitted > Correct
IP-17	Redress > Actions Permitted > Update
IP-18	Redress > Actions Permitted > Delete
IP-19	Redress > Difficulty > Timely
IP-20	Redress > Difficulty > Inexpensive
IP-21	Redress > Difficulty > Instructions provided

3.3.3. Purpose Specification (PS).

Twelve System Practices were identified under the Purpose Specification FIPP, which emphasizes a system's duty to articulate the authority that permits the system to collect data as

well as the purpose for which the data will be used. As such, the System Practices identified primarily seek to evaluate the authority granter of a system, the articulation methods used to grant authority, and the types of purposes data may be used for.

Table 4 System Practices Categorized Under Purpose Specification

PS-1	Authority Granter > None
PS-2	Authority Granter > Data Subject
PS-3	Authority Granter > Law
PS-4	Types of Purpose > Provide Services
PS-5	Types of Purpose > Market/advertise
PS-6	Types of Purpose > Profile/analytics
PS-7	Articulation Method for Authority / Purpose > Privacy Policy
PS-8	Articulation Method for Authority / Purpose > Popup
PS-9	Articulation Method for Authority / Purpose > Email
PS-10	Frequency of Articulation > Time Dependent
PS-11	Frequency of Articulation > Usage Dependent
PS-12	Frequency of Articulation > Data Type Dependent

3.3.4. Data Minimization (DM).

Twenty-one System Practices were identified under the Data Minimization FIPP, which emphasizes a system's duty to collect only that data which is relevant and necessary to accomplish the system's stated purposes. As such, the System Practices identified primarily seek to evaluate the types of data collected and the sources where data is collected. This includes evaluating the varying degree of sensitivity of data as well as comparing manual and automatic sources of data.

Table 5 System Practices Categorized Under Data Minimization

DM-1	Types of Data Collected > Public > Written Posts
DM-2	Types of Data Collected > Personal > Multimedia > Photos
DM-3	Types of Data Collected > Personal > Multimedia > Video
DM-4	Types of Data Collected > Personal > Multimedia > Audio
DM-5	Types of Data Collected > Personal > Contact > Email
DM-6	Types of Data Collected > Personal > Contact > Postal Address
DM-7	Types of Data Collected > Personal > Contact > Phone Number
DM-8	Types of Data Collected > Private > Demographics > Age
DM-9	Types of Data Collected > Private > Demographics > Race
DM-10	Types of Data Collected > Private > Demographics > Gender
DM-11	Types of Data Collected > Sensitive > Activities
DM-12	Types of Data Collected > Sensitive > Purchase History
DM-13	Types of Data Collected > Sensitive > Location
DM-14	Types of Data Collected > Highly Sensitive > Financial
DM-15	Types of Data Collected > Highly Sensitive > Health
DM-16	Types of Data Collected > Highly Sensitive > SSN

DM-17	Sources of Data > Manual > Data Subject
DM-18	Sources of Data > Manual > Other Data Subjects
DM-19	Sources of Data > Automatic > Cookies
DM-20	Sources of Data > Automatic > Pixels
DM-21	Sources of Data > Automatic > Metadata

3.3.5. Use Limitation (UL).

Seventeen System Practices were identified under the Use Limitation FIPP, which emphasizes a system's duty to only use the data it collects for the purposes it states. As such, the System Practices identified primarily seek to evaluate the different uses of data as well as focusing on sharing practices. This includes comparing general use of data to more commercially or analytically motivated uses of data. In addition, sharing was evaluated based on who the recipient of the shared data was and where the recipient was geographically located.

Table 6 System Practices Categorized Under Use Limitation

UL-1	General > Provide Services to DS
UL-2	General > Communicate with DS
UL-3	General > Enable DS Customization
UL-4	Security > Improve Services
UL-5	Security > Diagnostics/Troubleshooting
UL-6	Commercial > Marketing
UL-7	Analytical > Profiling
UL-8	Sharing > Recipient > Affiliated Companies
UL-9	Sharing > Recipient > Third Party > General
UL-10	Sharing > Recipient > Third Party > Security
UL-11	Sharing > Recipient > Third Party > Commercial
UL-12	Sharing > Recipient > Third Party > Analytical
UL-13	Sharing > Recipient > Third Party > Government
UL-14	Sharing > Geography > Local
UL-15	Sharing > Geography > National
UL-16	Sharing > Geography > Regional
UL-17	Sharing > Geography > International

3.3.6. Data Quality and Integrity (DQI).

Five System Practices were identified under the Data Quality and Integrity FIPP, which emphasizes a system's duty to ensure that data is accurate, relevant, and complete. As such, the System Practices identified primarily seek to evaluate the storage and management practices of the system. This includes looking at where and for how long a system stores data as well as the system's retrieval, duplication, and backup procedures and protocols.

Table 7 System Practices Categorized Under Data Quality and Integrity

DQI-1	Storage > Location
DQI-2	Storage > Duration
DQI-3	Management > Retrieval
DQI-4	Management > Duplication
DQI-5	Management > Backup

3.3.7. Security (S).

Six System Practices were identified under the Security FIPP, which emphasizes a system's duty to protect its data through appropriate safeguards. As such, the System Practices identified primarily seek to evaluate the system's protections against certain risks, including loss, unauthorized access, and unintended disclosures.

Table 8 System Practices Categorized Under Security

S-1	Loss Prevention
S-2	Unauthorized Access / Use
S-3	Destruction
S-4	Modification
S-5	Unintended Disclosure > Breach Notification
S-6	Compliance

3.3.8. Accountability and Auditing (AA).

Five System Practices were identified under the Accountability and Auditing FIPP, which emphasizes a system's duty to comply with the FIPPs as a whole as well as other regulations. As such, the System Practices identified primarily seek to evaluate the system's compliance with federal regulations, its training procedures, and its auditing practices.

Table 9 System Practices Categorized Under Accountability and Auditing

AA-1	Complying
AA-2	Training > Data Protection Officer appointed
AA-3	Auditing > Mechanisms in place
AA-4	Auditing > Frequency of Auditing
AA-5	Auditing > Internal or External Auditor

3.4. Adding and Removing System Practices to the Framework

Despite the attempt to identify highly specific System Practices to produce a comprehensive evaluation of a system, there are other System Practices that may not be included. Alternatively, certain users of the framework may conclude that some of the included System Practices should be removed.

3.5. Using the Framework

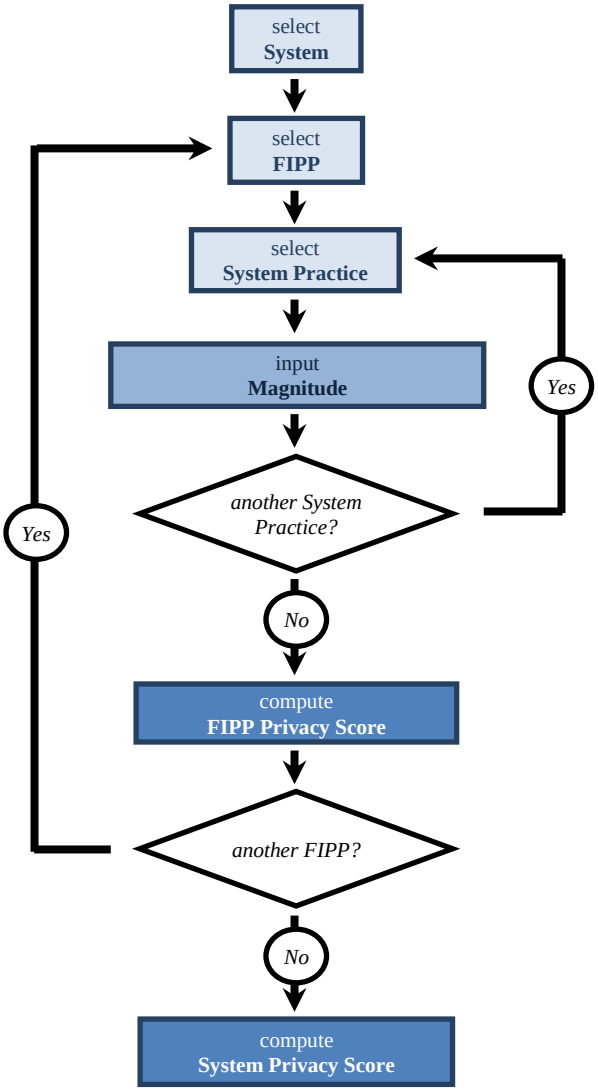
We describe a framework for comparing systems based on an arbitrary number of different privacy practices (referred to as System Practices in this paper) that the system follows.

The framework provides a Privacy Score for a system. This Privacy Score represents the impact of the system's System Practices on an individual who uses a system that processes and handles the consumer's PII. To evaluate the impact of the system, individuals use the framework to analyze each System Practice (identified above in Section 3.3) for intrusion into or protection of their privacy. Since the System Practices are organized according to the FIPPs, the framework will first compute a **FIPP Privacy Score**—a rating for each FIPP. The framework will then use the FIPP Privacy Scores to compute a **System Privacy Score**—a rating for the whole system. Figure 1 illustrates the framework using a flowchart. (While this work averages scores, other functions can be used, including ones that weigh the inputs of various individuals differently).

3.5.1. Assessment of Individual System Practices

The user of the framework will assess the System Practices by rating each of them according to their protection of or intrusion into the user's privacy (see Section 4.1 for an example). For each System Practice, the user determines the magnitude of the System Practice's impact. This magnitude quantifies the System Practice's protection of or intrusion into the user's privacy (scale from 1-5, highly intrusive to highly protective).

Figure 1 Using The FIPP-Inspired System Practice Framework



3.5.2. Assessment of Individual FIPPs

Once the System Practices have been assigned a magnitude, the framework will assess the individual FIPPs by calculating a FIPP Privacy Score (Figure 2). To calculate a FIPP Privacy Score for a FIPP, the framework averages the magnitudes inputted for each of the System Practices organized under that FIPP. This average is the FIPP Privacy Score. Since the framework will compute a FIPP Privacy Score for each of the eight FIPPs, there will be a total of eight FIPP Privacy Scores.

Figure 2 Individual FIPP Assessment: FIPPs and their Privacy Scores

SYSTEM *A*	
Fair Information Practice Principles	**FIPP Privacy Score**
Transparency	3.67
Individual Participation	3.19
Purpose Specification	1.83
Data Minimization	2.14
Use Limitation	2.24
Data Quality and Integrity	3.80
Security	1.67
Accountability and Auditing	3.40

In essence, FIPP Privacy Scores assess categories of similar System Practices for their protection of or intrusion into privacy. Using FIPP Privacy Scores to first assess categories, rather than jumping right to an overall assessment of the system, helps identify more specific strengths and weaknesses of the system. For instance, an overall assessment might not highlight the fact that a system is strong in Data Minimization but weak in Use Limitation. In contrast, assessing FIPPs first would highlight that difference.

3.5.3. Assessment of Overall System and Comparison with Other Systems

Once the framework calculates eight FIPP Privacy Scores, it will then use them to calculate a Privacy Score for the entire system (Figure 3). This Privacy Score represents the overall system's protection of or intrusion into an individual's privacy. To calculate a Privacy Score for the system, the framework averages all eight of the FIPP Privacy Scores. In turn, these score can then be used to compare and contract different systems.

Figure 3 Overall System Assessments: Using FIPP Privacy Scores to Compute System Privacy Scores

SYSTEM *A*	
Fair Information Practice Principles	**FIPP Privacy Score**
Transparency	3.67
Individual Participation	3.19
Purpose Specification	1.83
Data Minimization	2.14
Use Limitation	2.24
Data Quality and Integrity	3.80
Security	1.67
Accountability and Auditing	3.40
Average of FIPP Privacy Scores	**2.742**

SYSTEM	System Privacy Score
System A	2.742
System B	…
System C	…
…	…
…	…
…	…
…	…
…	…
…	…
…	…

Scale
1 – Highly intrusive of privacy; **5** – Highly protects privacy

4. EXAMPLE: APPLYING FIPP-INSPIRED SYSTEM PRACTICES FRAMEWORK TO FACEBOOK

4.1. Example: Assessment of Individual System Practices for Facebook

Appendix C represents one individual's assessment of the System Practices for the Facebook system as of June 2015. This assessment only reflects the Facebook system and its policies; it does not reflect any other systems that may work in conjunction with Facebook's systems. The left column shows each System Practice divided by FIPP, the middle column is the Magnitudes inputted by a user. The magnitude quantifies the System Practice's protection of or intrusion into the user's privacy (scale from 1-5, highly intrusive to highly protective). The right column shows the reasoning behind that user's selections.

4.2. Example: Assessment of Individual FIPPs for Facebook

Table 10 shows the Privacy Scores for each FIPP in the Facebook system. The framework calculated these Privacy Scores by taking the inputted data under each FIPP from Appendix C and averaging it to produce eight FIPP Privacy Scores (see Figure 2 in Section 3.5.2 for graphic illustration showing how FIPP Privacy Scores are calculated). The left column shows the FIPP and the right column shows that FIPP's Privacy Score, on a scale from 1 to 5 with 1 being high intrusion into the individual's privacy and 5 being high protection of the individual's privacy.

Table 10 FIPP Privacy Scores for the Facebook System

FIPP	FIPP Privacy Score
Transparency	3.67
Individual Participation	3.19
Purpose Specification	1.83
Data Minimization	2.14
Use Limitation	2.24
Data Quality and Integrity	3.80
Security	1.67
Accountability and Auditing	3.40

4.3. Example: Overall Assessment of Facebook and Comparison with Other Systems

Finally, the framework takes the eight FIPP Privacy Scores, averages them, and produces a final System Privacy Score for the Facebook system of **2.742** (see Figure 3 in Section 3.5.3 which shows how to calculated a System Privacy Score). This number reflects the individual's overall assessment of the Facebook system. Furthermore, the Privacy Score for the entire system can be compared against Privacy Score for other systems. For instance, if this individual also used the framework to evaluate Google's system and the framework came up with an overall Privacy Score of 3.257 for Google's system, then it becomes clear that the individual considers the Google system to be more protective of privacy than the Facebook system. Table 11 illustrates how overall Privacy Scores can be used to compare several systems.

Table 11 Comparisons of Multiple Systems' Overall Privacy Scores

System	System Privacy Score
Facebook	2.742
Google	3.257**
LinkedIn	2.482**
Twitter	1.956**
Uber	1.874**

**Numbers here are illustrative only and not based on actual inputs.

An ability to calculate Privacy Scores that can be used to compare systems is a unique feature of the framework. Such a comparison could be particularly useful to the system designers. For instances, low FIPP Privacy Scores can alert designers to specific areas where individuals may be highly concerned. In addition, comparing scores can provide designers of Company A with insight into how individuals' assess Company B's systems, helping designers from Company A produce competitive systems. Given these possibilities, this framework has implications for the Privacy By Design framework. The FIPP-Inspired System Practices can help ensure privacy is protected when designing and deploying new technologies.

5. COMPARING FRAMEWORKS

Comparing the FIPP-inspired System Practices with other sets of criteria to see where there might be overlap and which criteria best fit the user's needs can help identify strengths and weaknesses in the evaluation criteria as well as inform decisions about which criteria may be the best to use when conducting evaluations.

5.1 FIPP-Inspired System Practices and the Privacy Trust Framework

While there is some overlap between the System Practices and the 33 criteria used by Shore/Steinman (Appendix B), the two sets of evaluation criteria are not identical. However, these two sets of criteria provide a good opportunity for comparison. Such comparisons may produce a so-called "preferred" set of evaluation criteria that can be applied to any privacy policy or system; or each industry (social media, finance, medicine, etc.) may develop its own set of evaluation criteria. Table 12 compares the criteria used by Shore and Steinman with the FIPP-based System Practices identified in this paper. The numbering scheme used in the Privacy Trust Framework and adopted by Shore and Steinman has been preserved to enable easy reference. The letter and numbering scheme for the FIPP-based System Practices correspond to those used in Section 3.3. "Identified System Practices".

Table 12 Comparison of Shore / Steinman Criteria with FIPP-Inspired System Practices

Criteria Used by Shore and Steinman**	Comparable System Practice***
1.1 Privacy policy includes a short summary accurately describing the user's control of their data and all access to that data.	None
1.3 Privacy policy must not use passive structures ("we share" vs. "the sharing"), qualifying verbs and adverbs ("use" and "will" vs. "may," "occasionally," and "from time to time").	None
1.4 Privacy policy must have topic headings that link to plain language explanations of the type of data accessed and how the data are handled.	None
1.6 Privacy policy shall attain a Flesch-Kincaid Grade level score (reading level) of 12 or lower.	None
1.7 Privacy policy shall use a minimum 9 pt. font.	None
1.8 Privacy policy is available in the native language of organization's significant customer populations.	None
1.9 Privacy policy provides easy access to definitions of technical terms.	None
1.10 Privacy policy includes explicit language on process and notification of "material changes" and allows customers a defined timeline to opt out before policy changes.	IP-5. Consent > Options > Opt-out
2.1 Privacy policy states that personal information is collected only with informed consent, unless otherwise required by law.	PS-2. Authority Granter > Data Subject
2.2 Privacy policy must clearly state what the organization will and will not do with personal information.	PS-4. Types of Purpose > Provide Services PS-5. Types of Purpose > Market/advertise PS-6. Types of Purpose > Profile/analytics
2.3 Privacy policy fully describes use of internet monitoring technologies, including but not limited to beacons, weblogs, and cookies.	DM-19. Sources of Data > Automatic > Cookies DM-20. Sources of Data > Automatic > Pixels DM-21. Sources of Data > Automatic > Metadata
2.4 Privacy policy fully describes all data sharing circumstances that require a user to opt in.	None
2.5 Privacy policy fully describes what ability the user has to change, segment, delete, or amend their information.	IP-10. Access > Actions Permitted > View IP-11. Access > Actions Permitted > Download IP-15. Redress > Actions Permitted > Dispute IP-16. Redress > Actions Permitted > Correct IP-17. Redress > Actions Permitted > Update IP-18. Redress > Actions Permitted > Delete
2.6 Privacy policy fully describes who can access the information and when.	IP-8. Access > Frequency of Access > Time Dependent
2.8 Privacy policy fully describes with whom data are shared.	UL-8. Sharing > Recipient > Affiliated Companies UL-9. Sharing > Recipient > Third Party > General UL-10. Sharing > Recipient > Third Party > Security UL-11. Sharing > Recipient > Third Party > Commercial
	UL-12. Sharing > Recipient > Third Party > Analytical UL-13. Sharing > Recipient > Third Party > Government
2.12 Privacy policy describes the organization's process for receiving and resolving complaints.	IP-21. Redress > Difficulty > Instructions provided
2.13 Privacy policy describes a mechanism for Third Party resolution of complaints.	IP-21. Redress > Difficulty > Instructions provided
2.14 Privacy policy confirms that all persons with access to the data must comply with privacy policies.	None
3.2 System allows user to opt out at any time, and the opt-out process must be simple and clearly states in the privacy policy.	IP-1. Consent > Frequency of Consent > Time Dependent IP-6. Consent > Difficulty > Timely
3.3 System provides capability for all access to the user's data to be removed at any time. User has the ability to permanently delete all information upon closing an account.	IP-18. Redress > Actions Permitted > Delete
5.1 Any profiling must be optional (opt in) with the ability to opt out.	IP-2. Consent > Frequency of Consent > Usage Dependent
5.2 The system must allow users to clearly identify data used for profiling and targeting.	None
5.3 Users must be able to opt out of any profiling at any time. The opt-out process must be simple and clearly stated in the privacy policy.	IP-1. Consent > Frequency of Consent > Time Dependent IP-6. Consent > Difficulty > Timely IP-7. Consent > Difficulty > Inexpensive
5.4 The user may choose which specific data elements may be used for profiling and targeting.	None
6.1 System allows user to selectively release each element of their personal information.	IP-3. Consent > Frequency of Consent > Data Type Dependent
7.1 System allows user to delete, change, or annotate each element of their personal information.	IP-16. Redress > Actions Permitted > Correct IP-17. Redress > Actions Permitted > Update IP-18. Redress > Actions Permitted > Delete
7.2 The user may permanently delete their personal information from the system upon user request.	IP-18. Redress > Actions Permitted > Delete
8.2 System provides the functionality to control access to the data.	None
8.4 The ability to control the type of access that is provided to the system (e.g. read, write, delete) is controlled by the user.	None
8.5 The system specifies how long access to data is available (e.g., indefinitely or one week).	IP-8. Access > Frequency of Access > Time Dependent
11.1 Following discovery of a breach of personal information, organizations must notify each individual whose information has been accessed because of such breach.	S-5. Unintended Disclosure > Breach Notification
12.1 The organization must have a process [reported on the privacy policy] that enables users, advocates, employees and government regulators to report potential or actual privacy violations.	IP-15. Redress > Actions Permitted > Dispute
15.1 Users can expect to receive a copy of all disclosures of their information.	None

** Numbering scheme used in Privacy Trust Framework and adopted by Shore and Steinman. Preserved to enable easy reference.

*** Numbers correspond to those used in Section XX "Identified System Practices".

5.2 FIPP-Inspired System Practices and the Privacy Risk Management Framework

In addition, NISTIR 8062 includes some components that can be compared to the Privacy Trust Framework and System Practices. Although NISTIR 8062 primarily lays out an objectives-based, risk-mitigation model, it also features a set of criteria that in some ways resemble the "System Practices" identified by this paper and the criteria used by Shore and Steinman. To mitigate risk, the NISTIR 8062 model looks at the personal information collected or generated by a system, the data actions performed on that personal information, and any contextual factors.[9] These data actions are similar in nature to System Practices. While the data actions are not meant to act as criteria used in assessing and evaluating systems (NISTIR 8062 is not proposing a criteria-based assessment model), they are nevertheless an attempt to list all the different actions that a system follows—much in the same way that the System Practices seek to identify the practices that a system follows. Table 13 compares the data actions identified in NISTIR 8062 with the System Practices identified by this paper.

[9] "Privacy Engineering Objectives and Risk Model – Discussion Deck," *National Institute of Standards and Technology*, (April 2014). Accessed 16 June 2015, http://www.nist.gov/itl/csd/upload/nist_privacy_engr_objectives_risk_model_discussion_deck.pdf.

Table 13 Comparison of Problematic Data Actions with FIPP-Inspired System Practices

Problematic Data Actions *(Occur when the data actions of an information system contravene the objectives of predictability, manageability, or confidentiality)*	**Comparable System Practices**
Appropriation: personal information is used in ways that exceed an individual's expectation or authorization	**UL-1.** General > Provide Services to DS **UL-2.** General > Communicate with DS **UL-3.** General > Enable DS Customization **UL-4.** Security > Improve Services **UL-5.** Security > Diagnostics/Troubleshooting **UL-6.** Commercial > Marketing **UL-7.** Analytical > Profiling **UL-8.** Sharing > Recipient > Affiliated Companies **UL-9.** Sharing > Recipient > Third Party > General **UL-10.** Sharing > Recipient > Third Party > Security **UL-11.** Sharing > Recipient > Third Party > Commercial **UL-12.** Sharing > Recipient > Third Party > Analytical **UL-13.** Sharing > Recipient > Third Party > Government **UL-14.** Sharing > Geography > Local **UL-15.** Sharing > Geography > National **UL-16.** Sharing > Geography > Regional **UL-17.** Sharing > Geography > International
Distortion: the use or dissemination of inaccurate or misleadingly incomplete personal information	**S-5.** Unintended Disclosure > Breach Notification
Induced Disclosure: pressure to divulge personal information	*None*
Insecurity: lapses in data security	**S-1.** Loss Prevention **S-2.** Unauthorized Access / Use **S-3.** Destruction **S-4.** Modification **S-5.** Unintended Disclosure > Breach Notification **S-6.** Compliance
Surveillance: tracking or monitoring of personal information that is disproportionate to the purpose or outcome of the service	**PS-5.** Types of Purpose > Market/advertise **PS-6.** Types of Purpose > Profile/analytics **UL-6.** Commercial > Marketing **UL-7.** Analytical > Profiling
Unanticipated Revelation: non-contextual use of data reveals or exposes an individual or facets of an individual in unexpected ways	**S-5.** Unintended Disclosure > Breach Notification
Unwarranted Restriction: the improper denial of access or loss of privilege to personal information	**IP-8.** Access > Frequency of Access > Time Dependent **IP-9.** Access > Frequency of Access > Data Type Dependent **IP-10.** Access > Actions Permitted > View **IP-11.** Access > Actions Permitted > Download **IP-12.** Access > Difficulty > Timely **IP-13.** Access > Difficulty > Inexpensive **IP-14.** Access > Difficulty > Instructions Provided

6. FUTURE WORK: CROWDSOURCING

Previous research by others has focused on using crowdsourcing to make privacy policies more concise, accessible, and easy for individuals to digest. It is no secret that privacy policies in the past have been long and complex, and as a result, barely read. To remedy this problem and improve the usability of privacy policies, Patrick Kelly, Joanna Bresee, and Lorrie Faith Cranor, researchers from Carnegie Mellon University, have used crowdsourcing to determine which parts of a complex and convoluted privacy policy are most important to users. Once these key areas have been identified, these researchers combined them into an easy-to-read privacy policy that is significantly simpler than the original. Often, these condensed privacy policies rely heavily on graphic design, taking the form of privacy "nutrition labels" to convey the important elements of the privacy policies identified by the crowds.[10] Overall, their focus has been on using crowdsourcing to make existing privacy policies more user-friendly.

In addition to leveraging crowdsourcing to make privacy policies more assessable, researchers have also used it to model the privacy preferences of individuals who interact with systems that process their PII. In doing so, these researchers hope to give individuals more control over how a system processes and handles their data. A team of researchers from Carnegie Mellon University and Rutgers University developed one methodology for modeling the privacy preferences of individuals. They propose measuring individuals' expectations of how a system will handle PII and then comparing those expectations with how the system actually uses the PII. In this way, they hope to label systems that use an individual's information in completely unexpected ways, distinguishing such systems from those whose practices more closely align with an individual's expectations. This "privacy as expectation" approach seeks to use crowdsourcing to identify those systems whose operations significantly diverge from a user's expectations.[11]

In another case, Alissa Cooper, John Morris, and Erica Newland from the Center for Democracy and Technology also use crowdsourcing to uncover user preferences. This research sought feedback from crowds to identify a set of privacy preferences that individuals could combine in different groups to best reflect their own preferences. Whatever combination of rules those individuals created would become the privacy preferences that a system must abide by.[12]

This paper recognizes that the process of evaluating a system is highly qualitative. Both the criteria-based and risk-based approaches to assessing privacy protection only seek input from

---

[10] Patrick Gage Kelley, Joanna Bresee, Lorrie Faith Cranor, and Robert W. Reeder, "A 'Nutrition Label' for Privacy" (paper presented at the Symposium On Usable Privacy and Security (SOUPS) 2009, Mountain View, California, July 15-17, 2009). Accessed 24 July 2015, https://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf.

[11] Jialiu Lin, et. al., "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing" (paper presented at UbiComp' 12, Pittsburgh, Pennsylvania, September 5-8, 2012). Accessed 24 July 2015, http://www.winlab.rutgers.edu/~janne/privacyasexpectations-ubicomp12-final.pdf.

[12] Alissa Cooper, John Morris, and Erica Newland, "Privacy Rulesets: A User-Empowering Approach to Privacy on the Web" (paper presented at W3C Privacy Workshop, London, United Kingdom, July13-14, 2010). Accessed 24 July 2015, http://www.w3.org/2010/api-privacy-ws/papers/privacy-ws-12.html.

a single individual, a single company, or a single agency. This limited scope leads to relatively subjective measurements. Future frameworks focused on evaluation, assessment, and risk-mitigation could adopt a crowdsourcing approach that considers the views, interpretations, and interests of a wide variety of people and organizations. For instance, crowdsourcing techniques could be used to further compare criteria used in evaluation and assessment focused frameworks as well as deployed during the assessment phases of risk-mitigation frameworks to better reveal the concerns of individuals who use systems. Crowdsourcing shows great potential for analyzing systems and comparing their privacy policies and actions. Whereas one individual assessing a privacy policy can produce highly biased results, employing an entire crowd of individuals (with different interests, concerns, and interpretations) to assess the privacy policy can lead to more meaningful data and thus more accurate statements about a system's privacy protections.

7. SUMMARY

This paper proposes a criteria-based, evaluation and assessment framework inspired by the Fair Information Practice Principles. The FIPPs are used to identify 93 System Practices, which are then used as criteria to evaluate, assess, and ultimately compare information systems that process and handle data. Compared to existing frameworks, the FIPP-inspired System Practices seeks to provide more generalized criteria that can be adopted and modified according to the specific data handled by the information system. While the System Practices do overlap with criteria used in other frameworks, there do still exist some novel ones. Furthermore, when assessing and evaluating systems, additional System Practices may exist, or the ones already identified may be excluded. Ultimately, this paper seeks to operationalize the FIPPs for use in evaluating, assessing, and comparing systems as well as to provide a comparison of existing criteria-based privacy frameworks.

APPENDICIES

APPENDIX A: Comments Submitted to NIST on DRAFT Publication NISTIR 8062

Submitted by Lance J. Hoffman and Sam Klein on July 28, 2015
http://static1.squarespace.com/static/53b2efd7e4b0018990a073c4/t/55b7daf1e4b099e1393e797b/1438112497005/NIST+Comments+Writeup+v05.pdf

Understanding the concerns of individuals is crucial to properly assessing the privacy risk of a system. An individual is a data subject: a person whose personal information is collected, generated, processed, disclosed or retained by a privacy system. Their concerns are important because properly identifying problems, and the risks they pose, requires insight into what individuals' value most and what they are most worried about.

The Privacy Risk Management Framework (PRMF) recognizes the important role individuals' concerns play in risk assessment. This is evident in the "Assess System Design" process of the PRMF, which seeks to make "the concerns of individuals visible to agencies and how these concerns correlate to the behavior of the system," (p. 15, lines 556-7).

Agencies use the Privacy Risk Assessment Methodology (PRAM) to carry out the processes of the PRMF. To carry out the "Assess System Design" process, the PRAM calls for an agency to map the data processing within its system to identify data actions and personal information being processed as well as to catalog the contextual factors involved. Contextual factors are the circumstances surrounding a system's processing of personal information. By including these contextual factors, the PRAM attempts to account for the concerns of individuals in its privacy risk calculation–one of the goals of the PRMF.

However, in contrast to the PRAM's efficient and straightforward mapping process for identifying data actions and personal information, its approach to cataloging contextual factors is ad hoc and as a result does not sufficiently ensure that the concerns of individuals are made visible. We suggest extending it, using a model that provides a framework for quantifying existing contextual factors as well as identifying new ones. In doing so, the model will reveal the concerns of individuals so that system designers can better assess their designs and agencies can better calculate their privacy risk. And by taking advantage of the "wisdom of crowds [*The Wisdom of Crowds*, James Surowiecki]," the PRAM can better achieve its goals.

The model leverages a crowdsourcing methodology to determine how various individuals interpret a privacy system's implementation of Fair Information Practice Principles (FIPPs). Users of the model are the data subjects whose personal information is being processed by the privacy system they are evaluating; the users are the individuals who are trying to make their concerns known to the agency in charge of the privacy system. By using the model to evaluate a privacy system, individuals can make their concerns about that privacy system known.

More specifically, our model (http://www.cspri.seas.gwu.edu/crowdsourcing-privacy-risk-assessment/) evaluates a privacy system's implementation of the FIPPs by subdividing them into 93 system practices that a privacy system might follow. (For instance, the Transparency FIPP is broken down into six system practices, one of which being how frequently a privacy system provides notifications to its users). Using a scale of 1-5, individuals analyze each system practice

for intrusion into or protection of their privacy. The model will compute a function of their ratings (e.g., the average) for each system practice within a single FIPP, generating a privacy score for that FIPP (known as a FIPP Privacy Score). To compute a privacy score for the entire privacy system, (known as a System Privacy Score), the model will average or otherwise compute the eight FIPP Privacy Scores.

When using the model, an individual will rank a privacy system's practices according to that individual's interpretation of how those practices impact the individual's privacy. These rankings provide an agency with direct insight into how individuals interpret that system's privacy practices, and consequently, can make the concerns of an individual about that system visible to the agency. For example, one contextual factor from Appendix G is "what is known about the privacy interests of the individuals whose information is being process by the system," (p. 56; line 1352). If a variety of individuals' repeated use of the model results in low ratings for the agency's practices regarding transparency, then the agency can conclude that these individuals consider transparency to be an important privacy interest and are concerned about it and can take action to improve their system.

The example above relied on a contextual factor already identified in Appendix G. But the actually goes further and can reveal previously unconsidered contextual factors. For instance, geography is an important contextual factor not previously identified in Appendix G. The model includes provisions for evaluating an individual's concerns regarding the geographic location of their data. These provisions can reveal important concerns that may impact the agency's risk calculations and future system deployment decisions.

The PRAM calls for mapping the data processing within the system as a methodology for identifying data actions and personal information being processed. However, only an ad hoc methodology exists for cataloging contextual factors. While Appendix G provides a good organizational framework for thinking about contextual factors, it does not help agencies fully quantify or identify them. In contrast, our model can provide agencies with more concrete data about contextual factors that can reveal the concerns of individuals and more accurately calculate privacy risk.

When an agency itself is the only one conducting an assessment of its systems, it can limit its ability to fully anticipate how others might perceive and interact with the system. By extending the PRAM using crowds during the assessment processes of the PRMF, (especially when using the PRAM to catalogue contextual factors), the perspectives of a wide range of individuals can be leveraged to provide a more comprehensive assessment.

APPENDIX B: Shore / Steinman Criteria Used to Evaluate and Assess Facebook

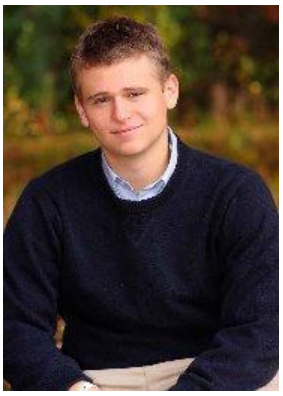
No.*	Criteria
1.1	Privacy policy includes a short summary accurately describing the user's control of their data and all access to that data.
1.3	Privacy policy must not use passive structures ("we share" vs. "the sharing"), qualifying verbs and adverbs ("use" and "will" vs. "may," "occasionally," and "from time to time").
1.4	Privacy policy must have topic headings that link to plain language explanations of the type of data accessed and how the data are handled.
1.6	Privacy policy shall attain a Flesch-Kincaid Grade level score (reading level) of 12 or lower.
1.7	Privacy policy shall use a minimum 9 pt. font.
1.8	Privacy policy is available in the native language of organization's significant customer populations.
1.9	Privacy policy provides easy access to definitions of technical terms.
1.10	Privacy policy includes explicit language on process and notification of "material changes" and allows customers a defined timeline to opt out before policy changes.
2.1	Privacy policy states that personal information is collected only with informed consent, unless otherwise required by law.
2.2	Privacy policy must clearly state what the organization will and will not do with personal information.
2.3	Privacy policy fully describes use of internet monitoring technologies, including but not limited to beacons, weblogs, and cookies.
2.4	Privacy policy fully describes all data sharing circumstances that require a user to opt in.
2.5	Privacy policy fully describes what ability the user has to change, segment, delete, or amend their information.
2.6	Privacy policy fully describes who can access the information and when.
2.8	Privacy policy fully describes with whom data are shared.
2.12	Privacy policy describes the organization's process for receiving and resolving complaints.
2.13	Privacy policy describes a mechanism for Third Party resolution of complaints.
2.14	Privacy policy confirms that all persons with access to the data must comply with privacy policies.
3.2	System allows user to opt out at any time, and the opt-out process must be simple and clearly states in the privacy policy.
3.3	System provides capability for all access to the user's data to be removed at any time. User has the ability to permanently delete all information upon closing an account.
5.1	Any profiling must be optional (opt in) with the ability to opt out.
5.2	The system must allow users to clearly identify data used for profiling and targeting.
5.3	Users must be able to opt out of any profiling at any time. The opt-out process must be simple and clearly stated in the privacy policy.
5.4	The user may choose which specific data elements may be used for profiling and targeting.
6.1	System allows user to selectively release each element of their personal information.
7.1	System allows user to delete, change, or annotate each element of their personal information.
7.2	The user may permanently delete their personal information from the system upon user request.
8.2	System provides the functionality to control access to the data.
8.4	The ability to control the type of access that is provided to the system (e.g. read, write, delete) is controlled by the user.
8.5	The system specifies how long access to data is available (e.g., indefinitely or one week).
11.1	Following discovery of a breach of personal information, organizations must notify each individual whose information has been accessed because of such breach.
12.1	The organization must have a process [reported on the privacy policy] that enables users, advocates, employees and government regulators to report potential or actual privacy violations.
15.1	Users can expect to receive a copy of all disclosures of their information.

* Numbering scheme used in Privacy Trust Framework and adopted by Shore and Steinman. Preserved to enable easy reference.

APPENDIX C: FIPP-Inspired System Practices Used to Evaluate and Assess Facebook

System Practice	Magnitude	Comments
TRANSPARENCY		
T-1. Methods of Notification > Privacy Policy	3	Fairly clear / concise way to notify DS about data policy
T-2. Methods of Notification > Popup	5	Some use of popups to notify DS about data policy
T-3. Methods of Notification > Email	4	Emails used to notify changes to policies; not used to explicitly notify DS about specific policies
T-4. Frequency of Notification > Time Dependent	3	Notifies sometimes
T-5. Frequency of Notification > Usage Dependent	5	Notifications often present at many stages of data processing
T-6. Frequency of Notification > Data Type Dependent	2	Doesn't necessarily give more notification when more sensitive information is collected
INDIVIDUAL PARTICIPATION		
IP-1. Consent > Frequency of Consent > Time Dependent	1	Only asks first time
IP-2. Consent > Frequency of Consent > Usage Dependent	4	Distinguishes based on data usage (i.e. asks for consent before sharing with 3rd party)
IP-3. Consent > Frequency of Consent > Data Type Dependent	3	Sometimes asks for consent when collecting more sensitive information, (i.e. location)
IP-4. Consent > Options > Opt-in	2	Opt-in option is rarely available; only pops up for certain actions (i.e. to allow a 3rd party to access information)
IP-5. Consent > Options > Opt-out	1	Have option to opt-out, but can be difficult to get to
IP-6. Consent > Difficulty > Timely	3	Consent for some things easier than for others; settings can be buried
IP-7. Consent > Difficulty > Inexpensive	5	Free to consent
IP-8. Access > Frequency of Access > Time Dependent	5	Can access whenever DS wants
IP-9. Access > Frequency of Access > Data Type Dependent	3	Some information easier to access than others; some can only be accessed via download
IP-10. Access > Actions Permitted > View	4	https://www.facebook.com/help/405183566203254
IP-11. Access > Actions Permitted > Download	3	https://www.facebook.com/help/131112897028467/
IP-12. Access > Difficulty > Timely	3	Faster to access some data over others (which need to be downloaded)
IP-13. Access > Difficulty > Inexpensive	5	Free to access
IP-14. Access > Difficulty > Instructions Provided	3	Access to download relatively easy
IP-15. Redress > Actions Permitted > Dispute	1	No mention of dispute mechanisms
IP-16. Redress > Actions Permitted > Correct	4	Edit features provided
IP-17. Redress > Actions Permitted > Update	4	Edit features provided
IP-18. Redress > Actions Permitted > Delete	2	Can delete, but some data stays even after account deleted
IP-19. Redress > Difficulty > Timely	3	Correcting / updating easy; deleting information more difficult
IP-20. Redress > Difficulty > Inexpensive	5	Free to redress
IP-21. Redress > Difficulty > Instructions provided	3	Deleting information clear to familiar users, but can be unclear to new users
PURPOSE SPECIFICATION		
PS-1. Authority Granter > None	1	None
PS-2. Authority Granter > Data Subject	1	No mention of the authority that permits the collection of PII; might have found one in the SRR; https://www.facebook.com/legal/terms
PS-3. Authority Granter > Law	1	Law doesn't require them to collect PII; no relevant legislation is mentioned
PS-4. Types of Purpose > Provide Services	4	Clear articulation of purpose for which PII is used
PS-5. Types of Purpose > Market/advertise	4	Clear articulation of purpose for which PII is used
PS-6. Types of Purpose > Profile/analytics	4	Clear articulation of purpose for which PII is used
PS-7. Articulation Method for Authority / Purpose > Privacy Policy	2	Located in data policy, but hard to find
PS-8. Articulation Method for Authority / Purpose > Popup	1	Not used to articulate authority/purpose
PS-9. Articulation Method for Authority / Purpose > Email	1	Not used to articulate authority/purpose
PS-10. Frequency of Articulation > Time Dependent	1	Only mentioned in privacy policy; not regularly articulated
PS-11. Frequency of Articulation > Usage Dependent	1	Not articulated at each step in processing of data
PS-12. Frequency of Articulation > Data Type Dependent	1	Not articulated for different data types
DATA MINIMIZATION		
DM-1. Types of Data Collected > Public > Written Posts	1	DS voluntarily gives
DM-2. Types of Data Collected > Personal > Multimedia > Photos	2	DS uploads
DM-3. Types of Data Collected > Personal > Multimedia > Video	2	DS uploads
DM-4. Types of Data Collected > Personal > Multimedia > Audio	2	DS uploads
DM-5. Types of Data Collected > Personal > Contact > Email	2	Required
DM-6. Types of Data Collected > Personal > Contact > Postal Address	2	DS voluntarily gives

DM-7.	Types of Data Collected > Personal > Contact > Phone Number	2	DS voluntarily gives
DM-8.	Types of Data Collected > Private > Demographics > Age	3	Required
DM-9.	Types of Data Collected > Private > Demographics > Race	1	Doesn't collect
DM-10.	Types of Data Collected > Private > Demographics > Gender	3	DS voluntarily gives
DM-11.	Types of Data Collected > Sensitive > Activities	4	Automatically collected
DM-12.	Types of Data Collected > Sensitive > Purchase History	4	Automatically collected
DM-13.	Types of Data Collected > Sensitive > Location	4	DS consents to give
DM-14.	Types of Data Collected > Highly Sensitive > Financial	5	Automatically collected
DM-15.	Types of Data Collected > Highly Sensitive > Health	1	Doesn't collect
DM-16.	Types of Data Collected > Highly Sensitive > SSN	1	Doesn't collect
DM-17.	Sources of Data > Manual > Data Subject	1	DS gives most of importation
DM-18.	Sources of Data > Manual > Other Data Subjects	2	Other information comes from DSs friends/connections
DM-19.	Sources of Data > Automatic > Cookies	1	Used
DM-20.	Sources of Data > Automatic > Pixels	1	Used
DM-21.	Sources of Data > Automatic > Metadata	1	Don't think metadata is collected
USE LIMITATION			
UL-1.	General > Provide Services to DS	1	Obvious / benign use
UL-2.	General > Communicate with DS	1	Obvious / benign use
UL-3.	General > Enable DS Customization	1	Obvious / benign use
UL-4.	Security > Improve Services	2	Obvious / benign use
UL-5.	Security > Diagnostics/Troubleshooting	2	Obvious / benign use
UL-6.	Commercial > Marketing	3	Data regularly used for marketing purposes
UL-7.	Analytical > Profiling	4	Data regularly used for analytical purposes
UL-8.	Sharing > Recipient > Affiliated Companies	1	Obvious / benign sharing
UL-9.	Sharing > Recipient > Third Party > General	1	Obvious / benign sharing
UL-10.	Sharing > Recipient > Third Party > Security	2	Obvious / benign sharing
UL-11.	Sharing > Recipient > Third Party > Commercial	3	Data regularly shared for marketing purposes; consent is required first
UL-12.	Sharing > Recipient > Third Party > Analytical	4	Data regularly shared for analytical purposes
UL-13.	Sharing > Recipient > Third Party > Government	5	https://govtrequests.facebook.com/country/United%20States/2014-H2/
UL-14.	Sharing > Geography > Local	1	No local entity
UL-15.	Sharing > Geography > National	5	All data transferred to and processed in the US
UL-16.	Sharing > Geography > Regional	1	No regional entity
UL-17.	Sharing > Geography > International	1	No international entity
DATA QUALITY AND INTEGRITY			
DQI-1.	Storage > Location	2	Foreign DS's data moved to US
DQI-2.	Storage > Duration	2	Some kept even after account delete
DQI-3.	Management > Retrieval	5	http://www.pcworld.com/article/2042979/the-tao-of-facebook-data-management.html; https://www.facebook.com/notes/facebook-engineering/tao-the-power-of-the-graph/10151525983993920
DQI-4.	Management > Duplication	5	Advanced data stores / management
DQI-5.	Management > Backup	5	Advanced data stores / management
SECURITY			
S-1.	Loss Prevention	1	No mention of loss prevention techniques https://www.facebook.com/help/131719720300233/
S-2.	Unauthorized Access / Use	3	Some mechanisms for preventing against unauthorized use (i.e. TFA)
S-3.	Destruction	1	No mention of mitigating destruction of data
S-4.	Modification	1	No mention of mitigating modification of data
S-5.	Unintended Disclosure > Breach Notification	3	Breaches / vulnerabilities posted to security blog https://www.facebook.com/security
S-6.	Compliance	1	No compliance page
ACCOUNTABILITY AND AUDITING			
AA-1.	Complying	3	Facebook seems to be in compliance (http://www.huffingtonpost.com/2013/04/25/facebook-privacy-audit_n_3153801.html); Facebook Ireland asked to make improvements in 2011/2012 (https://dataprotection.ie/documents/press/Facebook_Ireland_Audit_Review_Report_21_Sept_2012.pdf)
AA-2.	Training > Data Protection Officer appointed	3	No data protection officer, but has two chief privacy officer (one for policy and one for products)
AA-3.	Auditing > Mechanisms in place	3	FTC requires audit https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep
AA-4.	Auditing > Frequency of Auditing	4	Every 2 years for 20 years
AA-5.	Auditing > Internal or External Auditor	4	External auditor



Samuel Klein *earned his B.A. from The George Washington University where he majored in International Affairs and minored in Chinese Language and Literature. His undergraduate honors thesis investigated China's information warfare strategies and objectives to assess the possibility of a Chinese cyber-attack targeting US critical physical infrastructure. This past summer he interned at GW's Cyber Security Policy and Research Institute. Previously, he received a Fulbright GPA Scholarship to conduct education policy research in China and was a Congressional intern on Capitol Hill.*

Professor of Computer Science and Director

Lance J. Hoffman *is Director of the Cyber Security Policy and Research Institute (CSPRI) at The George Washington University. Professor Hoffman developed the first regularly offered course on computer security at the University of California, Berkeley in 1970, after working with the legendary Professor Alan Westin on a National Academy of Sciences project that produced the book Databanks in a Free Society. A Fellow of the Association for Computing Machinery, Dr. Hoffman institutionalized the ACM Conference on Computers, Freedom, and Privacy. He has served on a number of Advisory Committees including those of Federal Trade Commission, the Department of Homeland Security, and the Center for Democracy and Technology.*

His research has spanned multiple aspects of cybersecurity, including models and metrics for secure computer systems, cryptography policy, risk analysis, computer viruses, societal vulnerability to computer system failures, portable security labs, privacy/data protection, and statistical inference for data mining.

He is the initiator and principal investigator for GW's CyberCorps scholarship program that has produced dozens of cybersecurity experts with degrees in at least ten majors. All have had cross-disciplinary instruction that recognizes cybersecurity as a discipline with technology, policy, and management components, often presented by government and industry information security leaders who regularly visit the GW campus to provide timely topical briefings. These graduates have gone on to work for dozens of different organizations.

Dr. Hoffman earned his Ph. D. in Computer Science in 1970 from Stanford University, after a B.S. in Mathematics from Carnegie Mellon University.