Privacy Impact Assessments (PIAs)
Emerging Trends in Pursuit of the Silver Bullet

Mary Morshed and Adriane Urband

School of Information
University of California, Berkeley102 South Hall #4600, Berkeley, CA 94720-4600 USA
mary.morshed@ischool.berkeley.edu, adriane@ischool.berkeley.edu

Abstract

Privacy has been identified as a prerogative worth protecting for millennia. The definitions of what is private and what is personal information have evolved and expanded over those thousands of years. The advent of modern communications technologies has heralded a demand for even more precise definitions in order to better understand and create mechanisms to protect personal privacy in as many spheres as it can be violated. We examine a relatively new privacy risk management methodology, Privacy Impact Assessments (PIAs), in an attempt to determine the effectiveness of this tool and its supporting processes that are currently in use by government and business organizations. Trends uncovered during our research include: factors that influence the PIA process; techniques used to find personally identifiable information in organizational initiatives; and other tools or methodologies organizations are using to manage privacy risks. We apply our findings to an emerging consumer space, drones, as a test case for applying these tools and processes to new technologies and services in order to reduce privacy risks. Can we successfully create the universal tool to assess privacy impacts, and if so, who are the actors and whose risks are being managed?

Introduction

Privacy has long played an acknowledged role in ethics- but faces an unknown future as technology innovation drives both the use of personal information and creation of intrusive devices that operate in personal realms. Privacy exists as a domain with a large area of power, control and/or influence. Who has that power, control or influence is one of the questions constantly being debated by Congress, regulators, companies and individuals. The privacy sphere is complicated to navigate. Even more difficult to understand are the intricate interconnectedness of the self and personally identifiable information about the self. Looking back through time provides some helpful guidance to start this discussion.

There and Back Again; Three Privacy Tales

Around 400BC, a Greek document was written, entitled simply “Oath.” It contained twelve

items[1], one of which translated into English reads: "Whatever I see or hear in the lives of my patients, whether in connection with my professional practice or not, which ought not to be spoken of outside, I will keep secret, as considering all such things to be private." The historical progression of the Oath into modern medical ethics was slow; there was no record of its use before the Middle Ages, when it was rediscovered by church scholars who modified it to conform to their Christian doctrines. The first recorded use of the Oath was at the University of Wittenberg, Germany, in 1508[2]. In the eighteenth century, the Oath was first translated into English, and medical schools in both Europe and the United States began to use various versions of the Oath in their graduation ceremonies. It is now referred to as the Hippocratic Oath. Although the authorship is uncertain and the Oath is nonobligatory, it has endured in the medical profession and was the seed for what has grown into a complex set of rules and regulations in the US for managing health information, known as the Health Information Portability and Accountability Act (HIPAA).

Flash forward to 1890. An article was published in the Harvard Law Review titled, *The Right to Privacy*, authored by Samuel Warren and Louis Brandeis. Several developments in the late 19th century had created a privacy interest. Changes in the success of the press between 1850 and 1890 with the introduction of sensationalistic (yellow) journalism resulted in increased circulation by approximately 1000% - from 100 newspapers with 800,000 readers to 900 newspapers with more than 8 million readers[3]. In addition, technological developments, specifically the invention of instantaneous photography, had raised the issue of privacy concerns. One particular passage in the article says, 'Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that "*What is whispered in the closet shall be proclaimed from the house-tops*[4]*.*"' The view point of the article was that the law could and should provide protection for privacy. Society is still dealing with the concerns raised over one hundred years ago in this article, including the "right to be let alone."

A third privacy milestone occurred in the early 1970's, when the then US Department of Health, Education and Welfare (HEW) convened a committee in response to the increasing use of automated data systems that were collecting and storing information about individuals. As a

[1] http://www.einstein.yu.edu/publications/einstein-journal-biology-medicine/default.aspx?id=29998
[2] Smith, L. (2008). A Brief History of Medicine's Hippocratic Oath, or How Times Have Changed. *Otolaryngol Head Neck Surg* **139**:1-4.
[3] Solove, D. & Schwartz, P. (2009). *Privacy, Information, and Technology*, 12-23. Aspen Publishers. New York.
[4] Warren, S. D., & Brandeis, L. D. (1890). Right to Privacy. (K. Ziegler, Ed.)Harvard Law Review, 4(1), 72. Hart.

result, in 1973, the committee published a report[5] and developed what was called the Code of Fair Information Practices, a set of principles for protecting the personal information in record keeping systems. The report titled, *Records, Computers and the Rights of Citizens*, explained that, "An individual's personal privacy is directly affected by the kind of disclosure and use made of identifiable information about him in a record. A record containing information about an individual in identifiable form must, therefore, be governed by procedures that afford the individual a right to participate in deciding what the content of the record will be, and what disclosure and use will be made of the identifiable information in it." Companies and policymakers continue to refer to these principles today to make decisions about personally identifiable information (PII).

These three historical anecdotes help provide background context for studying privacy impact assessments by: shedding light on the historical significance of protecting information entrusted to a business or company, identifying that technological advancements have historically and continuously raised privacy and affirming that procedures should govern privacy decisions. Many other historical milestones in privacy have been investigated as part of this research paper and are documented in Appendix I, History of Privacy Mind Map diagram.

Public Opinion and the Public Sphere

Returning to Warren and Brandeis; they were concerned about the "incursions into privacy by the burgeoning print media" [6] and observed that privacy invasions caused "mental pain and distress", and "injury to the feelings." Today's communications systems, media and the Internet, make it easier to distribute information quickly and everywhere; yet there is no mechanism to ensure the veracity of a story. Stories of reputational harm are in the news every day. Recently, a teen was mistakenly identified as one of the Boston Marathon bombers and he panicked. He made his Facebook timeline private, and in one message now no longer visible, he announced he was going to clear his name[7]. In the social context, knowing information about an individual establishes the reputation of the individual. Solove states, "Our reputation is one of our most cherished assets,"[8]. It is an essential component to our freedom and is something that can impact the core of our identity. Reputation affects our ability to engage in society, yet is not

[5] http://epic.org/privacy/hew1973report/
[6] Solove, D. (2007). The Future of Reputation, Gossip, Rumor, and Privacy on the Internet. Yale University Press. New Haven & London.
[7] http://deadspin.com/the-boston-bombing-witch-hunt-bags-another-innocent-kid-476001019
[8] Solove, D. (2007). The Future of Reputation, Gossip, Rumor, and Privacy on the Internet. Yale University Press. New Haven & London.

solely our own to create. It depends on others to affirm and build. A reputation is fragile and can be easily damaged because of its construct. Knowing the identity of a person is to know that person's reputation as well.

Another privacy concern that didn't exist in 1890 is the "right to be forgotten." This issue has been heavily debated in Europe for the last few years; a proposed new EU regulation would add meaningful penalties for enforcement. This new legal framework addresses an emerging problem space specific to the Internet, where the persistence of information makes erasing or escaping the past very difficult. However, several dissenting opinions have been expressed about the way the new EU regulation is written and the unintended consequences of the regulation[9]. This "right to be forgotten" has also led to another initiative, called Do Not Track (DNT). In theory, a consumer would have a choice about whether or not his or her Internet activities are tracked. Current controversies surround the adoption of a DNT standard and agreement has not been reached on determining definitions[10]. Congress is growing impatient[11] with: (1) advertisers who are potentially the most impacted group of DNT and appear to be reluctant to self-regulate; and (2) the policy group, W3C, which is working to smooth out policy differences.

Lastly, a number of theorists conceive of privacy as a "form of control over personal information".[12] Charles Fried's definition of privacy states that "privacy is not simply the absence of information about what is in the minds of others; rather it is the control we have over information about ourselves." The relationships identified for public opinion and the public sphere are documented in Appendix II, Public Opinion & the Public Sphere of Personally Identifiable Information (PII).

Personally Identifiable Information

Personally Identifiable Information (PII) is a term used to associate informational privacy[13] with an individual. At a fundamental level it means information that identifies an individual, or can be reasonably linked to identify an individual. The definitions for PII are developed from global

[9] http://www.stanfordlawreview.org/online/privacy-paradox/right-to-be-forgotten There are potentially three categories for "right to be forgotten," as has been defined by Peter Fleischer (chief privacy counsel at Google) and each proposes progressively greater threats to free speech.
[10] http://adage.com/article/privacy-and-regulation/internet-group-lost-weeds-define-dnt/240610/ Important definitions and the overall standard is dependent upon how first party and third party cookies are defined.
[11] http://www.adweek.com/news/technology/rockefeller-goes-do-not-track-rant-hearing-148873
[12] Solove, D. & Schwartz, P. (2008). *Privacy and the Media,* 39-58. Aspen Publishers. New York.
[13] http://www.cse.unsw.edu.au/~cs4920/seminars/resources/Roger-Clarke-Intro.pdf Informational privacy, as defined by Clarke, is the interest an individual has in controlling, or at least significantly influencing, the handling of data about themselves.

laws. Appendix III identifies common privacy laws and their legal definitions for PII. Appendix IV, Definitions for Personally Identifiable Information (PII), documents a sampling of common and legal definitions as well. In addition, data elements from laws have been identified in Appendix V, Data Elements (Definitions) for Personally Identifiable Information (PII) and are derived from state data breach notification laws.

The definition of PII also develops from regulatory action. The Federal Trade Commission (FTC) was established in 1914, in an attempt to prevent monopolistic practices by US Corporations. In the mid 1960's, current events and public interest necessitated the FTC to assume the additional role of consumer protection. Privacy is a right that falls under the jurisdiction of consumer protection and in today's online world, the right to privacy manifests itself by taking on the form of information and data. The FTC investigates unfair and deceptive practices in many domains, including privacy. One way to understand the meaning of PII from the FTC's perspective is to look at how they use the term "personal information", in publications. The FTC publishes reports and guides for best practices as a means to influence privacy decisions. In reviewing "Protecting Privacy in an Era of Rapid Change, Recommendations for Businesses and Policymakers (March 2012)," the FTC takes advantage of the innate ambiguity in the use of the term and goes so far as to use other terms interchangeably, such as: user information, sensitive information, information about consumers, personal data and personal health information; however, this practice does not necessarily equate to inconsistent use.

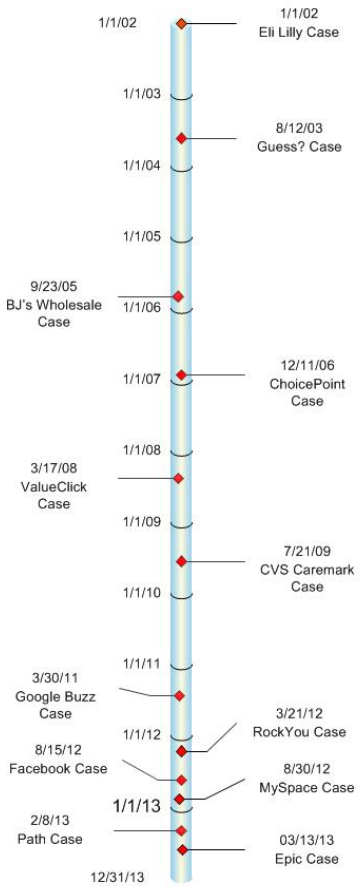
The primary use of the term "personal information" revolves around the notion of information-as-a-substance. The FTC has explained that information, in the Shannon[14] sense, flows, is transmitted, and can be shared in discrete units of measure. It can also move undetected, be stored, be collected and deleted. Personal information is processed, during which it undergoes a transformation and becomes data or was once data and is transformed into personal information. In relying heavily on the information-as-a-substance description for personal information, the FTC is able to manipulate the number and types of data elements associated with the term, adding new data elements as businesses change their practices. This allows the FTC to perform their core mission of consumer protection, even while technology and information collection and use practices undergo fast, radical changes.

[14] Shannon, C. E., & Weaver, W. (1949). *The mathematical theory of information*. *Urbana University of Illinois Press* (Vol. 97, pp. 623-656). University of Illinois Press.

Figure 1 illustrates the changing FTC definition for PII over time. The standard definition was defined in 2002 with the Eli Lilly case using the category name of “individually identifiable information”, and all subsequent cases were compared to those originally defined data elements. In 2011, with the Google Buzz case, a new category of data elements was created, called covered information, which included the data elements from the standard definition. The FTC then uses the new category to address the sharing of “covered information” with third parties. Then, again, in 2013, another new category is created during the Facebook case, called “non-public user information,” and again refers to the category of “covered information” to speak to the sharing of data elements. And, lastly, in 2013, the FTC adds more data elements to the covered information category and specifically calls out data elements on mobiles devices are included.

The FTC also considers the propositional use of the term, and begins with identifying harms that may result by knowing personal information about a consumer. The knowing is not necessarily wisdom, but possibly a knowledge with which some intention or action can occur. The harms identified in the report are associated with a lack of control of information and an implied property right, which leads to an information-as-substance meaning as well. In addition, knowing where someone is or where someone goes, via tracking or surveillance, incorporates a physical aspect to it because of the close association to the individual.

FTC's Data Elements for Personally Identifiable Information



2002 – Established standard definition. *Individually identifiable information from or about an individual consumer, including: first and last name, home or other physical address, email address or other online contact information such as instant messaging user identifier or screen name, telephone number, social security number, IP address or host name (computer device name,) persistent identifier such as a "cookie" or processor serial number, or any information that is combined with these.*

2003 – Adds to the Standard definition: credit and/or debit card information, including credit and/or debit card number and expiration date.

2005 – Adds to the 2003 definition: data stored on the magnetic stripe of a credit card or debit card.

2006 – Adds to the 2005 definition: date of birth and driver's license number.

2008 – Add to the 2006 definition: CVV or CVV2 security code contained in card magnetic stripes or other storage media or otherwise printed or maintained on card surfaces in any form.

2009 – Adds to the 2008 definition: other government-issued identification number, prescription information, a bank account number, a biometric record, and extends the term "consumer" to also mean employee and an individual seeking to become an employee.

2011 – Adds a new term to the Standard definition: **covered information** – means information that is collected from or about an individual and includes all of the common personally identifiable data elements previously indicated.

2012 – Adds to the 2011 definition: state-issued identification number, financial institution account number, non-public communications and content, photos, videos, and user ID. And adds a new term: **non-public user information** – covered information that is restricted by one or more privacy setting.

2013 – Adds to the definition: a combination of a last name or photograph of the individual with other information such that the combination permits physical or online contacting; or information concerning the child or the parents of that child that the operator collects online from the child and combines with an identifier described in this definition. Also, adds: users' browser cache and browser configuration; specifically, how a user's browser styles the display of a link to a specific URL. Also, adds to the definition of **covered information**: nonpublic communications and content posted on Defendant's website or within Defendant's applications; or communications and content stored on a consumer's mobile device.

Figure 1

Knowledge and Use of Personally Identifiable Information

When the FTC started expanding their categorization of PII to include the practice of sharing, such as the term "covered information", focus shifted from collecting, maintaining or processing, to the actual use of the PII. Having knowledge of personal information about an individual and how that knowledge is used is anther puzzle piece added to understand the privacy sphere and how to make privacy decisions. These changes have given rise to the concept of anonymization; users can transact business or engage in services without providing PII, or organizations that process PII do so using techniques that prevent identification and/or re-identification of the individual.

Appendix VI, Knowledge and Use of Personally Identifiable Information (PII), sketches out a high-level overview for consideration in this space; including: economics of PII, information

asymmetry, as well as harms and benefits to the individual when others possess PII about that individual.

Institutions Interested in Personally Identifiable Information

The final area of our research on the privacy sphere looked at institutions interested in PII. Identified were organizations, such as: the United Nations and Member States and their work on human rights frameworks, businesses, law enforcement and specific professional domains, e.g. attorneys. Appendix VII, Institutions for Personally Identifiable Information (PII) maps the path followed. One branch, informational privacy, is detailed in Appendix VIII, Informational Privacy (Institutions for PII).

The Need for Privacy Risk Management

As previously mentioned, privacy has a large sphere of influence and companies and people bump up against privacy choices every day. For example, a search on Google News for "privacy choice" returned 263,000,000 results and another search on "privacy breach" returned 79,000 results for that same day.

Many countries, such as: Australia, Canada, New Zealand, and the UK[15], target privacy risk management[16] methods to both government departments and the private sector,. Only the United States (US) has legislation that specifies the method that must be used by government agencies, called a Privacy Impact Assessment (PIA). There is no such legislative requirement in the US for the private sector companies. On March 13, 2013, Google was fined $7 million for a privacy breach associated with their Street View product. A coalition of 39 US state attorneys general found that Google Street View vehicles had collected private information from home and business wireless networks. The vehicles collected names, passwords and other PII from unencrypted wireless transmissions. Although the fine is minimal when compared to the projected company revenue this year, their company reputation "has taken a hit[17]."

Another high profile case in the US was a recent FTC Settlement Agreement with Facebook, in which the complaint charged that Facebook misled users about how private their information would be kept. As part of the agreement, Facebook was ordered to "maintain a comprehensive

[15] Wright, D. & De Hert, P. (2012). *Law, Governance and Technology Series 6. Privacy Impact Assessment*.(pp17-23). Springer. New York

[16] http://en.wikipedia.org/wiki/Risk_management Risk management is the identification, assessment and prioritization of risks, followed by coordinated and economical application of resources to minimize, monitor and control the probability and/or impact of unfortunate events or to maximize the realization of opportunities. The field of privacy risk management deals with risks associated with privacy issues.

[17] http://abcnews.go.com/Technology/google-hit-million-fine-street-view-privacy-breach/story?id=18717950#.UYbgmKHn-po

privacy program that is reasonably designed to (1) address privacy risks related to the development and management of new and existing products and services for consumers.[18]" In addition, the report requires that Facebook document their privacy program in writing, and include the following actions:

> A. The designation of an employee or employees to coordinate and be responsible for the privacy program.
>
> B. The identification of reasonably foreseeable, material risks, both internal and external, that could result in Respondent's unauthorized collection, use, or disclosure of covered information and an assessment of the sufficiency of any safeguards in place to control these risks. At a minimum, this *privacy risk assessment* should include consideration of risks in each area of relevant operation, including, but not limited to: (1) employee training and management, including training on the requirements of this order, and (2) product design, development, and research.
>
> C. The design and implementation of reasonable controls and procedures to address the *risks identified through the privacy risk assessment*, and regular testing or monitoring of the effectiveness of those controls and procedures.
>
> D. The development and use of reasonable steps to select and retain service providers capable of appropriately protecting the privacy of covered information they receive from Respondent and requiring service providers, by contract, to implement and maintain appropriate privacy protections for such covered information.
>
> E. The evaluation and adjustment of Respondent's privacy program in light of the results of the testing and monitoring required by subpart C, any material changes to Respondent's operations or business arrangements, or any other circumstances that Respondent knows or has reason to know may have a material impact on the effectiveness of its privacy program.[19]

Just as the FTC has expanded the definition for PII by identifying new data elements through their enforcement actions, in this way they also influence private companies by requiring the performance of privacy risk management activities.

---

[18] http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf
[19] http://www.ftc.gov/os/caselist/0923184/120810facebookdo.pdf

Another way the FTC influences private companies in making privacy decisions is by providing guidance in the form of reports, as mentioned earlier. The reports focus on outcomes instead of the method and process for identifying and reducing privacy risks. For example, the FTC released a report in February 2013 titled, "Mobile Privacy Disclosures – Building Trust Through Transparency," that outlines recommended outcomes for different actors in the consumer mobile device market, e.g. the platform providers, the mobile applications developers, the advertising networks and other third parties. One of the recommendations is that platform providers and mobile applications developers should "provide just-in-time disclosures to consumers and obtain their affirmative express consent before allowing apps to access sensitive content like geolocation." [20] Therefore, application developers don't need to guess about when to provide notices to consumers or whether or not to use opt-in or out-out notices. The FTC report clearly makes those decisions for them.

Components of Privacy Impact Assessments (PIAs)

Privacy Risk Management

Although this paper is not focused on researching the domain of risk management, it is helpful to introduce a few key concepts of privacy risk management in order to understand how a privacy impact assessment fits into the overall risk management structure for organizations. The Privacy Commissioner of Ontario Canada published a sample privacy risk management model[21], **Figure 2**, which will be used here. The first step of the model is establishing the context for the organization by integrating into the existing governance framework and creating accountability. Step two involves identifying privacy risks and establishing the processes to support these activities. Step three, analyzing and evaluating risks, comprises triaging risks which means ranking each of the identified risks and separating out the minor risks from the major risks. Treating risks is step four and involves traditional treatment options, such as: mitigating, transferring, avoiding or accepting the risks. The processes identified in step five include monitoring for continuous improvement in all of the previous steps; and lastly, step 6 identifies the significance of communications and consultation for the privacy risk management process, where "an organization needs to look far and wide for issues and solutions to enhance privacy performance."

[20] FTC. (2013). Mobile Privacy Disclosures – Building Trust Through Transparency. Web. http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf
[21] https://www.privacyassociation.org/media/pdf/knowledge_center/pbd-priv-risk-mgmt.pdf

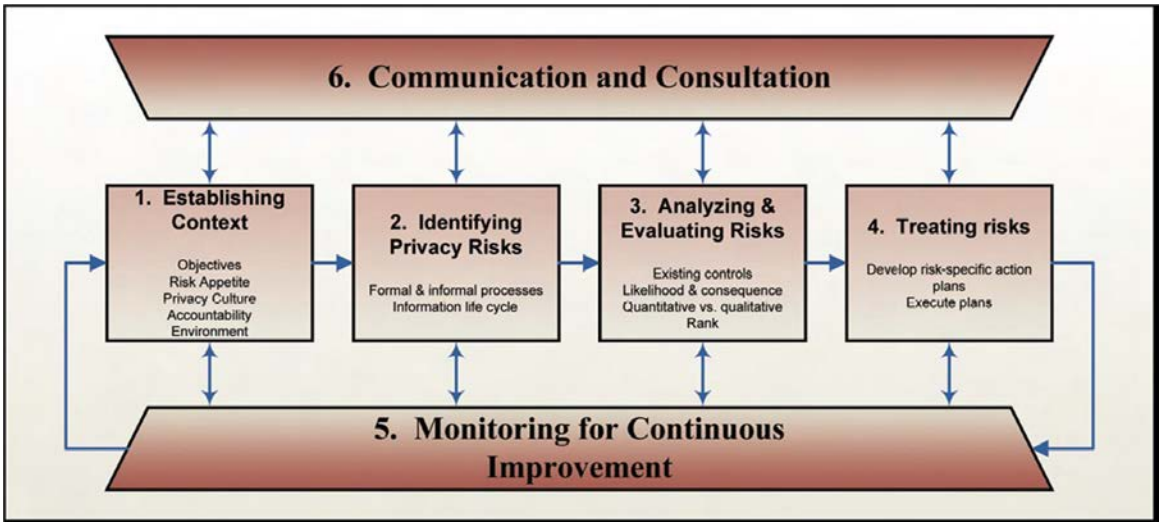


Figure 2 – Privacy Risk Management Model
Privacy Risk Management. Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed by default – Information and Privacy Commissioner, Ontario, Canada

Other Methodologies for Managing Privacy Risk

One tool or methodology for managing privacy risk is called Privacy by Design (PbD). The core objective is "ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage". [22] This methodology outlines structure that "privacy and data protection are embedded throughout the entire lifecycle of technologies, from early design to their deployment, use and ultimate disposal."[23] Another tool for managing privacy risks are traditional audits focused on the privacy domain. Lastly, the Privacy Impact Assessment, (PIA) is the method that will be discussed in detail here.

Privacy Impact Assessments (PIAs)

Wright and DeHert define a Privacy Impact Assessment (PIA) to be: ***"a methodology for assessing the impacts on privacy of a project, policy, program, service, product or other initiative which involves the processing of personal information and, in consultation, with stakeholders, for taking remedial actions as necessary in order to avoid or minimize negative impacts***."[24] We use this definition to standardize how we evaluate our research and findings.

[22] http://www.privacybydesign.ca/index.php/about-pbd/7-foundational-principles/ The PbD has 7 foundational principles: 1 – Proactive not Reactive, Preventative not Remedial. 2 – Privacy as a Default Setting. 3 – Privacy Embedded into Design. 4 – Full Functionality – Positive-Sum, not Zero-Sum. 5 – End-to-End Security – Full Lifecycle Protection. 6 – Visibility and Transparency – Keep it Open. 7 – Respect for User Privacy – Keep it User-Centric.
[23] http://en.wikipedia.org/wiki/Privacy_by_Design
[24] Wright, D. & De Hert, P. (2012). *Law, Governance and Technology Series 6. Privacy Impact Assessment*. Springer. New York.

PIA's have been used as early as the 1970's[25] called a "privacy impact statement." Former Information and Privacy Commissioner of British Columbia, David Flaherty, said he could document the use of the term back to the 70s. In 1996, the US Internal Revenue Service (IRS) issued the IRS Privacy Impact Assessment[26]. On June 13, 1996, a panel session was held at the Privacy Issues Forum, Christchurch, NZ.The chair of the session was Blair Stewart (Manager of Codes and Legislation, NZ Privacy Commissioner's Office) and panel participants included Elizabeth Longworth (Longworth Associates), David Flaherty (British Columbia Privacy Commissioner), and Nigel Waters (Head of Privacy Branch, Australian Privacy Commissioner's Office). Chairman Stewart said, "In this session we consider not just the `here and now' of privacy but we speculate on whether a technique which we call PIA may enable us to steer towards a future in a more privacy-friendly direction. It seems to me that even if the future requires a trade-off in privacy in favour of some other material benefit a PIA allows us to make such choices rationally and with our eyes open as to their privacy `downside'."[27]

This dichotomy between privacy considerations and material benefits leaves room for skepticism that PIAs, as implemented, may not be as effective as intended in privacy risk identification and mitigation[28]. Most of the research in the privacy arena expresses some level of concern with this conflict of business and individual interests. In discussion of the potential harms to businesses, their partners and their customers (consumers as individuals), the exposed inequities will support these concerns as valid. Our research has uncovered other gaps as well, to be discussed in our findings. We offer recommendations on how to close these gaps and improve the processes in which PIA tools are embedded.

Metrics

The implementation of privacy metrics for an overall privacy program itself is still in its formative stages.[29] Searching on-line returns many hits on the term but few that describe what metrics would be useful or recommendations on their collection. Even the sample privacy risk management model and associated document[30], mentioned above, has little to say about useful

[25] See endnote 3 in Flaherty, D. Privacy Impact Assessments: An Essential Tool for Data Protection. Privacy Law and Policy Reporter, Vol. 7. No. 5, November 2000. Web. http://www.austlii.edu.au/au/journals/PLPR/2000/
[26] Internal Revenue Service. (1996). IRS Privacy Impact Assessment, Version 1.3, Washington DC. Web. www.cio.gov/documents/pia_for_it_irs_model.pdf
[27] Stewart, B. (1996,). PIAs – an early warning system. *Privacy Law & Policy Reporter.* Web. http://www.austlii.edu.au/au/journals/PLPR/1996/65.html
[28] Brown, E., & Kosa, T. A. Incorporating Privacy Outcomes: Teaching an Old Dog New Tricks. , 2008 Sixth Annual Conference on Privacy Security and Trust 232–239 (2008). doi:10.1109/PST.2008.27
[29] Herath, K. (2011). *Building a Privacy Program, A Practioner's Guide,* 158-163. An IAPP Publication. Portsmouth, NH.
[30] https://www.privacyassociation.org/media/pdf/knowledge_center/pbd-priv-risk-mgmt.pdf

measuring and monitoring activities. The model mentions monitoring trends in privacy incidents and complaints, and taking the time to review lessons learned.

The three key questions, suggested by Herath, guide choices for metrics collection are:

What is the privacy program trying to accomplish?
What does success look like?
What is the perceived value the privacy program adds to the organization?

According to literature published by the International Association of Privacy Professionals[31], early experience of privacy professionals suggests five domains for measurement: risk reduction, compliance, business enablement, value creation, and trust enhancement. The risk reduction approach is typically seen in the unregulated space of private companies, especially since the advent of breach notification laws[32]. The compliance approach to using privacy metrics is most common in jurisdictions and organizations subject to regulatory requirements and enforcement actions or in companies where risk appetite[33] is low. Business enablement comes into play for companies that are looking at expanding into other markets; for example: a US-based company that wants to expand services into Europe would look at metrics associated with privacy outcomes to ensure they are able to meet this new business objective. One example of a business enablement metric could be the number of business clients inquiring about Safe Harbor status. When a privacy initiative is directly tied to a favorable financial outcome for the organization, this falls under the value creation domain for measurement. One popular example is when a company reduces the retention time that personal data is kept before destruction and thus reduces the need for data storage media at the same time. And, lastly, trust enhancement can also be referred to brand value. A company's brand is an intangible asset[34], but there has been recent research focused on the negative impact of a data breach to a company's brand and bottom line.

[31] The International Association of Privacy Professionals is the largest and most comprehensive global information privacy community and resource, helping practitioners develop and advance their careers and organizations manage and protect their data. More than just a professional association, the IAPP provides a home for privacy professionals around the world to gather, share experiences and enrich their knowledge. https://www.privacyassociation.org/about_iapp
[32] Laws enacted at the state level that require notification to consumers when their PII has been, or is believed to have been, inappropriately disclosed or acquired by an unauthorized person. http://en.wikipedia.org/wiki/Security_breach_notification_laws
[33] Risk appetite is the level of risk an organization is willing to tolerate before action is deemed necessary to reduce it. http://en.wikipedia.org/wiki/Risk_appetite
[34] http://deloitte.wsj.com/riskandcompliance/2013/04/09/using-metrics-to-protect-brand-valuue/

In 2011, the Experian Data Breach Resolution sponsored a study of 850 executives. The research was independently conducted by Ponemon Institute LLC, and the findings included several interesting things related to brand impact:

- At best, companies lost twelve percent of their value from a data breach
- It took an average of one year for a victim organization to restore its reputation after a hacking incident
- Victim organizations lost anywhere from $184 million to more than $330 million in the value of their brands.

Problem Space and Critical Inquiry Method

The primary focus of this research is to answer the question of whether or not a universal tool, specifically the PIA process, is the best approach to managing privacy risks; and if so, what might the tool look like?

Although PIA's have been adopted in many sectors and many countries and even mandated for US government organizations, the tools (and in some cases the process itself) have been slow to mature and gain significant traction. Some PIA's have turned into compliance exercises, with little measureable value[35], which may or may not be problematic. The FTC defines privacy policy through their enforcement actions and requires private companies to perform privacy risk activities; identifying the best tool to help manage privacy risk is a value proposition.

We performed traditional research to learn more about the sphere of privacy, to identify connected domains and to review current literature on the subject of the PIA process and associated tools. We held interviews with Chief Privacy Officers and Privacy Managers representing six different government organizations and private sector companies. An interview protocol was developed and used during the interview process to ensure the same data elements were collected. We collected artifacts from the interviewees who could legally share them, from other resources that depicted data elements collected during the PIA intake process, and based on the types and number of questions being asked.

[35] Brown, E., & Kosa, T. A. Incorporating Privacy Outcomes: Teaching an Old Dog New Tricks. , 2008 Sixth Annual Conference on Privacy Security and Trust 232–239 (2008). doi:10.1109/PST.2008.27

We used qualitative data analysis and research software to code the transcribed interviews and PIA related artifacts to look for trends, patterns, and anomalies. Pre-defined code tags were configured and loaded into the tool based upon the interview protocol and the tags were refined as previously unidentified topics of interest emerged. See Appendix IX for a list of the codes used. **Figure 3** shows a screen shot of the tool used to code the transcribed interviews. The text version of the interview is loaded in the document as a primary document. The researcher selects the passages and quotes from the text, then applies one or more of the developed codes. Codes that have been applied display in the left hand window of the tool. Reports are then built based upon the grouping of the interviews and the coded informational sets.

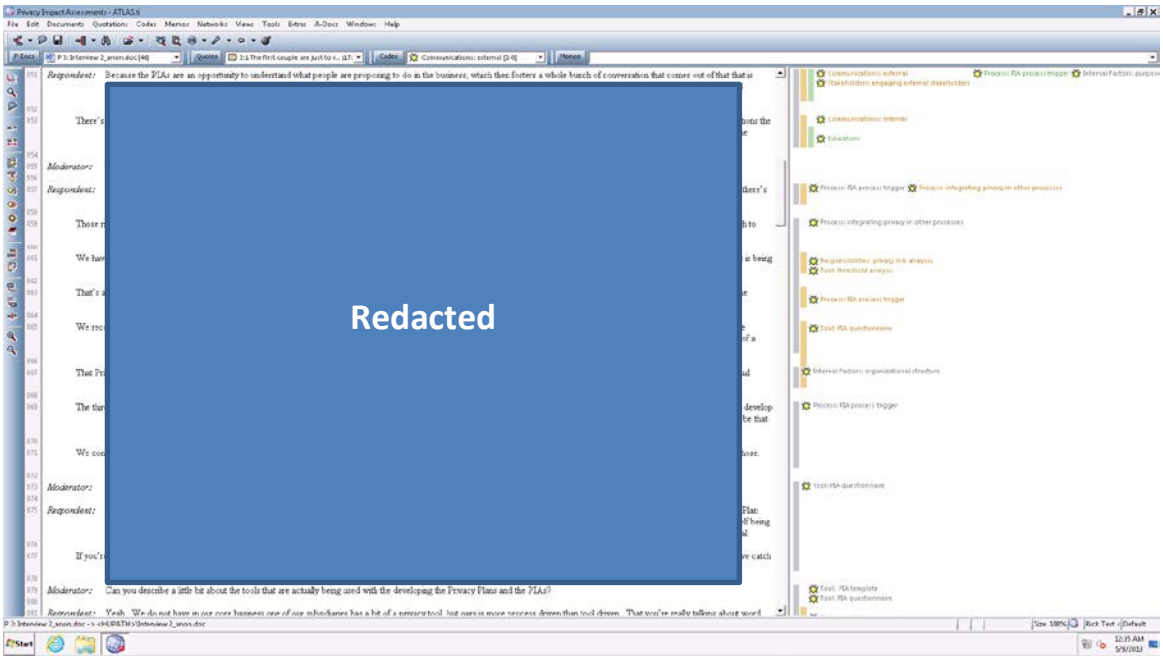


Figure 3

The resulting reports were analyzed and combined with traditional research findings to develop recommendations.

And, lastly, our research recommendations were tested against a new/emerging space with potentially high risk privacy implications, consumer drone technology. Questions we attempt to answer for the case study are:

1 - Is a PIA the right tool to use when assessing privacy impacts of consumer drones to individuals?

2 - If so, what is the appropriate scale, scope?

3 - Who should use the PIA tool/process; e.g. manufacturers, software or hardware developers, consumers from an awareness perspective, etc.?

4 - Could potential policy changes be moderated if PIA's were an integral part of any new privacy regulations?

Case Study: Droning On

When we think of drones, lay people frequently think of the military-grade Predator drones (MQ-1 Predator) most news stories focus on which have been designed to carry cameras, sensors and munitions over long distances and loiter for 14 hours overhead[36]. A very different design, consumer-grade drones must typically operate within line-of-sight of the operator, are reasonably priced and attractive to aerial photography hobbyists.[37] These drones have also sparked interest and innovation in other domains. For example, journalism schools at two US Universities have added programs that teach students the basics of flying unmanned autonomous vehicles and how to use still and video cameras to gather aerial information. The courses also include topics such as the ethics of operating flying cameras, FAA regulations and safety, and how to interpret aerial footage.[38] A recent story describes how drones will deliver beer during the OppiKoppi Music Festival in South Africa later this year, thus coining the term "beer drone"[39]. Even the UC Berkeley School of Information held its first Drone Lab class during the Spring 2013 semester, aimed at thinking about the "socially good things[40]" that could be done with drones.

One of the more popular consumer grade drones is called the "Parrot AR. Drone". It serves as the technical focus of this case study. It's a radio controlled flying quad-rotor helicopter, controlled by an application that users can load on iOS or Android devices. There are many websites dedicated to hacking the Parrot AR. Drone's open architecture, which runs on Linux. These sites share ideas, computer code, and recommendations for modifications. Typical reasons for hacking the platform include: increasing the battery life to last above the factory delivered maximum length of twelve minutes; upgrading the radio system to gain increased

[36] http://en.wikipedia.org/wiki/General_Atomics_MQ-1_Predator
[37] http://www.fastcompany.com/3005534/test-flying-drone-makes-anyone-aerial-photographer
[38] http://www.innovationtoronto.com/2013/03/drones-go-to-journalism-school/
[39] http://mashable.com/2013/05/05/beer-drones/
[40] http://www.ischool.berkeley.edu/newsandevents/news/20130416dronelab

control over longer distances; and adding better cameras or GPS sensors to the platform. [41] The manufacturer also provides the ability to fully reprogram the motor controller, has a built-in software-controlled emergency stop and the entire platform is fully reparable with parts and instructions available online[42].

The consumer drone space could be broken up into three quasi-discrete areas of control in which actors operate: the manufacturers, those that modify the hardware and or software, and the users. Each area focuses on a different view of privacy risk and potential responsibility. The primary technology that impacts privacy in consumer drones is also the one thing that makes them so interesting, cameras. Although camera functionality is included in many mobile devices and smartphones today, it is a different user and surveillance experience when the camera is being controlled remotely, from various heights and angles, and has the ability to "lock on" and follow an individual. When people see consumer drones in neighborhoods or parks, they are often curious to see what the camera is viewing. Drones have the ability to see into areas that are decidedly private, such as into a backyard surrounded by a six-foot privacy fence. When considering drones, it seems that the technical implementation, along with the user and data subject perceptions are an important part of the privacy risk conversation.

Findings

The interview protocol was designed to capture several categories of data in order to analyze trends. The following trends were identified in these categories. In addition, inputs and outputs to the process were also explored and recurrent themes emerged, discussed below.

Communications

Privacy professionals believe their role is more advisory than punitive and they approach the business lines in a collaborative and non-bureaucratic fashion. Important decisions are made jointly with other divisions. They also believe there is a marketing aspect to their job that requires they sell the ideas of using the privacy tools and educating the business about privacy risks. One Privacy Manager stated she uses the catch phrase of "looking for the gold" to communicate her role of a privacy professional, and to differentiate her role from that of the Chief Information Security Officer in the organization.

[41] http://www.hackmyparrotardrone.com/2013_02_01_archive.html, http://dronehacks.com/, http://diydrones.com/profiles/blogs/turning-the-parrot-ardrone
[42] http://ardrone2.parrot.com/ardrone-2/specifications/

Organizational Influence - Culture

Most of the interviewees indicate they use some form of decentralized privacy resource structure where employees with some level of privacy skills and responsibility are embedded in business groups, staying within that structure for reporting purposes. One interviewee also advised the challenge with this arrangement is being able to stay connected to the privacy specialists close enough to make sure that the specialists are rewarded for the work that they do. However, he also mentioned this organizational embedding assisted in breaking through the siloed structure and culture of the business units, increasing privacy communications throughout the organization. Larger, more mature privacy programs (defined as a privacy program with more than three full-time staff and in operation of over 5 years) routinely use a privacy group or committee with resources where the members are matrixed directly to the privacy program for tasks such as reviewing and deciding privacy policy for the organization. Less mature privacy programs rely more on individual relationships for establishing communications channels.

Responsibilities

Many interviewees reported that 30-40% of their time is spent on privacy impact assessment activities. These responsibilities include: education, risk analysis tasks, tracking of privacy projects and responding to external influences that relate directly to the PIA process.

Education

Education is seen as a responsibility inherent to the privacy job. In some cases, the education is built into the tools used to conduct the PIA. For example, guidance is provided in automated systems with warning messages and pop-up informational boxes. For non-automated tools, sample scenarios and guidance information is provided along-side data entry fields. Since some of the larger organizations distribute privacy responsibility widely, training is heavily utilized to increase the quality, capability and enablement of those staff in privacy roles. This includes training on how to use privacy tools and methodologies. In addition, the role of privacy certifications, such as those provided by the International Association of Privacy Professionals (IAPP), is seen as a valuable way to educate employees holding privacy roles and responsibilities in the organization.

PIA education is also achieved by day-to-day exposure wherein privacy resources attend business meetings, design sessions and are involved in change management processes. Most organizations also have internal web pages maintained as a privacy resource for employees who interact with the PIA process.

Process Management

The PIA process is not always ingrained or integrated in other organizational processes; as a result interviewees identified that some of their work involves tracking privacy projects. For those organizations that have a single PIA automated system for managing privacy risks, they have less entry points to monitor for entry into the PIA process, but still spent time tracking activities. Some organizations determined a one-size-fits-all approach for automating the PIA process presents unique challenges. The PIA process itself is described as "an opportunity to understand what people are proposing to do in the business, which then fosters a whole bunch of conversations that come out of that. That conversation is broader than just the response of a PIA."

Each interviewee stated the privacy impact assessment process is engaged in his or her organization at many levels because of the multiple workflows. Triggers and gates are implemented in order to ensure all projects or major revisions to existing products and services flow through the PIA process. Some of these methods include:

- Integration into existing IT processes, such as: change management, project management, and product or service design/engineering;
- Gates at funding decision points where the privacy official's signature is required before new projects are approved;
- Privacy awareness training to educate employees and provide guidance on the PIA process.

It is believed by most interviewees that the majority of initiatives required to go through the PIA process are being captured. Some companies require all new initiatives or initiatives with significant changes to go through the PIA process while others only required systems or services that handle PII to undergo PIAs, the difference being the level and type of screening or threshold assessment that is done.

Threshold Assessments

Threshold assessments are used as a screening tool to see if further questions need to be asked about a project or initiative. All companies interviewed use a threshold assessment, but may call it something else. One interviewee said this about the threshold assessment he uses, "It's just a few simple questions and the heart of the question is to understand if the product or service will be somehow touching or handling information about people. Essentially, I ask four

questions and I ask that same question four different ways, just to make sure they answered it appropriately."

Risk Analysis

Risk analysis takes many forms, depending upon the tools being used. In those organizations where a universal PIA tool is being used, risk analysis is built into the tool. One interviewee said the following: "We actually employed engineers to help us design this thing, and it has a backend rules engine." Other organizations using a universal PIA tool explained they take the content from policy, standards, and specifications; building intelligence within the tool based on an internally created algorithm. For those organizations that do not use a single PIA tool, the risk analysis is conducted by the privacy staff; risks are identified based on compliance to privacy policies and the knowledge of the privacy professional conducting the analysis.

Mitigation Process

All companies interviewed expressed some level of dependence on their technical or engineering resources to assist with this step, especially the technical security resources in the organization. It is unclear what role automated PIA systems played in the mitigation process for those companies using them. However, discussion of the privacy analysis reports that are produced as a result of the automated process revealed they are reviewed and discussed between the privacy personnel and the project teams in the business lines.

Escalation Process

Most organizations have an escalation process defined, but their similarities ended. Some organizations do not use the escalation process, while others employ it on a regular basis. Those that do not exercise the escalation process cite mandatory compliance with privacy policies, principals and standards as the reason. Business lines rarely deviate from the instituted privacy policies and controls or standards against which new projects or initiatives are measured.

Approval Process

The approval process for a PIA typically involves a verification step that plans and mitigation strategies proposed and agreed to in the PIA report are actually implemented, as a condition of approval.

PIA Tools - Approaches

Leveraging Existing Tools to Include PIA Component

Only one company we spoke with uses this approach. It was designed for threshold assessments and as an in-take collection system only. This company has a culture of using a single application to centrally manage all business processes; when they implemented a PIA process, they created a PIA workflow in the application. The interviewee expressed some challenges in using this particular tool when trying to track all global privacy initiatives.

All-in-One Universal Tools

Few companies use a universal PIA tool, which includes all stages of the PIA process, from threshold assessment to approval. This approach lends itself to very large organizations that have a structured business model and mature processes and policies. These tools are built to assess compliance with the policy infrastructure, making it possible to build in rules and algorithms to prioritize risk.

Forms for Manual Integration into Business Processes

The most prevalent methodology for PIA tool integration is for companies to use forms, questionnaires, templates or checklists that reside outside of existing automated systems or processes to manage threshold assessments and intake activities only. The companies build in hooks to business processes, where possible, to trigger the PIA process. Many of the interviewees who use this approach said they need to be flexible in order to integrate with the business when it changes; so they prefer this approach.

Customization

One further finding, many of the companies take advantage of the ease in which forms are used to customize the content for each line of business, so privacy can be defined in a way that makes sense for the context in which it is applied. This approach may also be implemented in the universal tools.

Other Tools Used to Manage Risk

There are many other privacy risk management tools utilized by the interviewed organizations. Here is a sampling of them.

- Embedding privacy resources in all areas of the company, or at least privacy trained resources

- Having privacy awareness programs with internal websites for reference information
- Instituting accountability to drive compliance
- Established committees or governance groups with members from all areas of the organization that meet on a regular basis to discuss privacy direction for the organization
- The Privacy by Design framework
- A database of people in the company who have privacy responsibilities; it tracks their level of authority and placement in the company for assigning privacy work. This database also is used for managing exception requests and assigning incidents.
- All of the organizations admitted that they aren't using metrics or don't believe they are using them very well. One interviewee candidly said when asked if they were using metrics: "We do, but I'll be honest with you I've never felt like they really measure it well. I'm always a bit skeptical that we've done a great job there."

External Influence

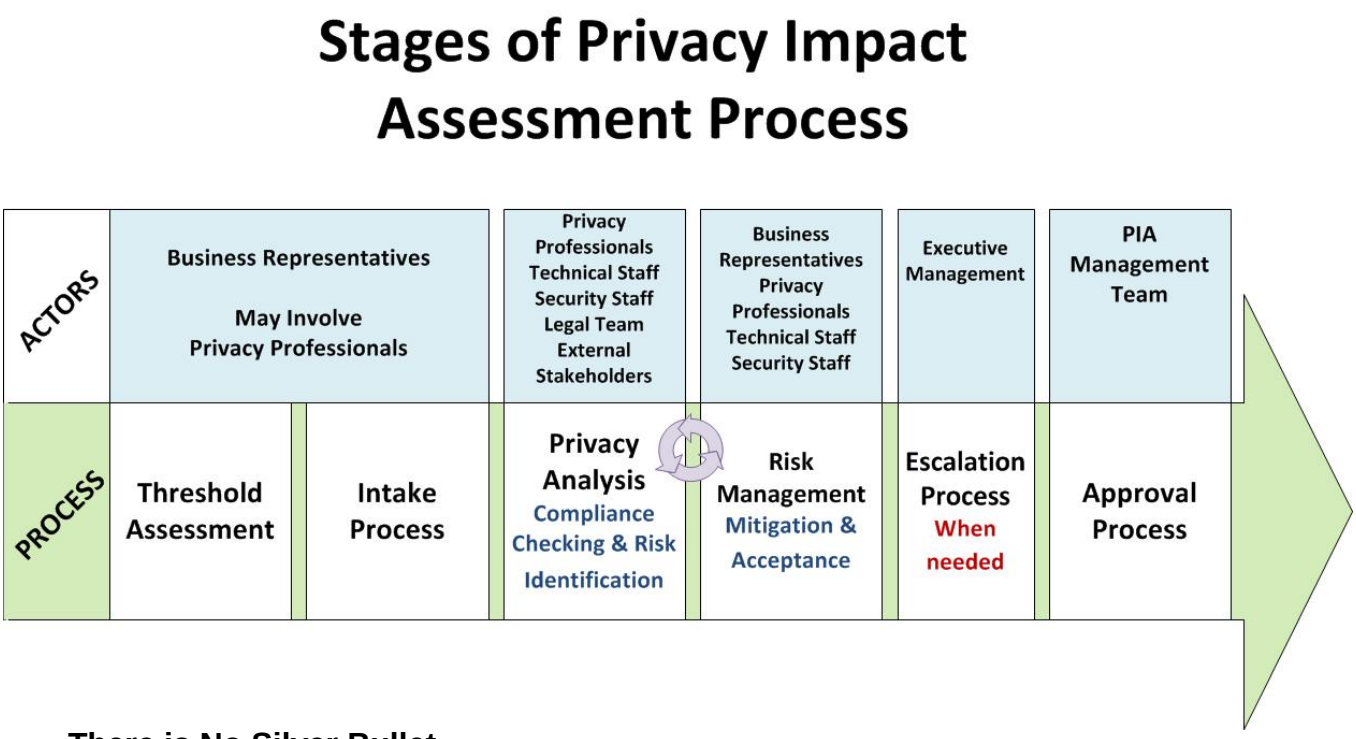
Interviewees advised that external influences to the PIA process are driven by changes to the regulatory landscape. For those organizations using a non-automated process, the changes from external influences are handled by updating a questionnaire, or survey or template form. Organizations using a fully automated process are not as agile in adapting to regulatory changes. One interviewee mentioned challenges with adopting the EU ePrivacy Directive , also called the "Cookie Directive"[43] into the PIA system.

PIA Process Stages Emerge

Our findings identify a high-level PIA process, broken up into six stages. These stages are depicted in **Figure 4**, along with the actors associated with the respective stages.

[43] http://en.wikipedia.org/wiki/Directive_on_Privacy_and_Electronic_Communications

Figure 4



There is No Silver Bullet

Originally, as a secondary goal of our research, we wanted to produce a universal PIA tool. Based on modular template construction, the tool would allow for any needed customization, with dropdown selections and pop-up instructional windows. Given our findings above, in which we discuss how differing organizational structure and culture play roles in decision-making processes, we were forced to conclude this silver bullet would be impossible to implement.

Recommendations

Our analysis has led to several sets of recommendations for easing process “pains”, improvements to create “gains”, new definitions, and the creation of valid and valuable metrics.

The tools utilized in the PIA process should be easy to update and customizable to translate privacy requirements into a technical language understood by each business line. Privacy liaisons who are SMEs in their own business groups as well as educated privacy professionals can facilitate this customization, create open communication between their groups and the privacy office, and help educate their co-workers to increase buy-in to the PIA process. Identify appropriate points that would act as triggers for the PIA process to become involved, e.g. new initiatives; changes to design, infrastructure or process; funding stages. As a PIA process matures, integration into the overall product, service or relationship lifecycle is key to embedding

privacy standards into the company culture. Privacy officers would do well to remember social organization principles and utilize their “soft tools” to present themselves as helpers; a guide to facilitate value-added processes that will only help improve any business group’s success.

Recommendations for New Ways of Defining PII Data Elements

As the FTC and governments continue to add data elements to the list of what represents PII, a more nuanced approach, one focused on risk and the likeliness of harm should be considered. What is being left out by lumping data elements under the definition of a single term? They are all treated the same within the term and no data elements are considered more important than others when it comes to how they should be handled, considered, or the associated harms. But, isn’t some information more personal than other information? Don’t we think differently about information that exists just by being in the world, as opposed to information that describes an individual? And, aren’t the harms different based upon how close the information is to the person? Instead, consider several different categories of data elements. For example, we could look at a spectrum, ranging from data elements closest to the individual at one end, to data elements farther away from the individual at the other. These categories could include: information that is the individual, sensitive information, information about the individual, information that is directly linked to the individual and information that is indirectly linked to the individual. (The category of sensitive information refers to information that by itself is not personally identifiable, but because it is used to grant access to data or services, it requires a higher level of protection.) The spectrum might look something like **Figure 5**.

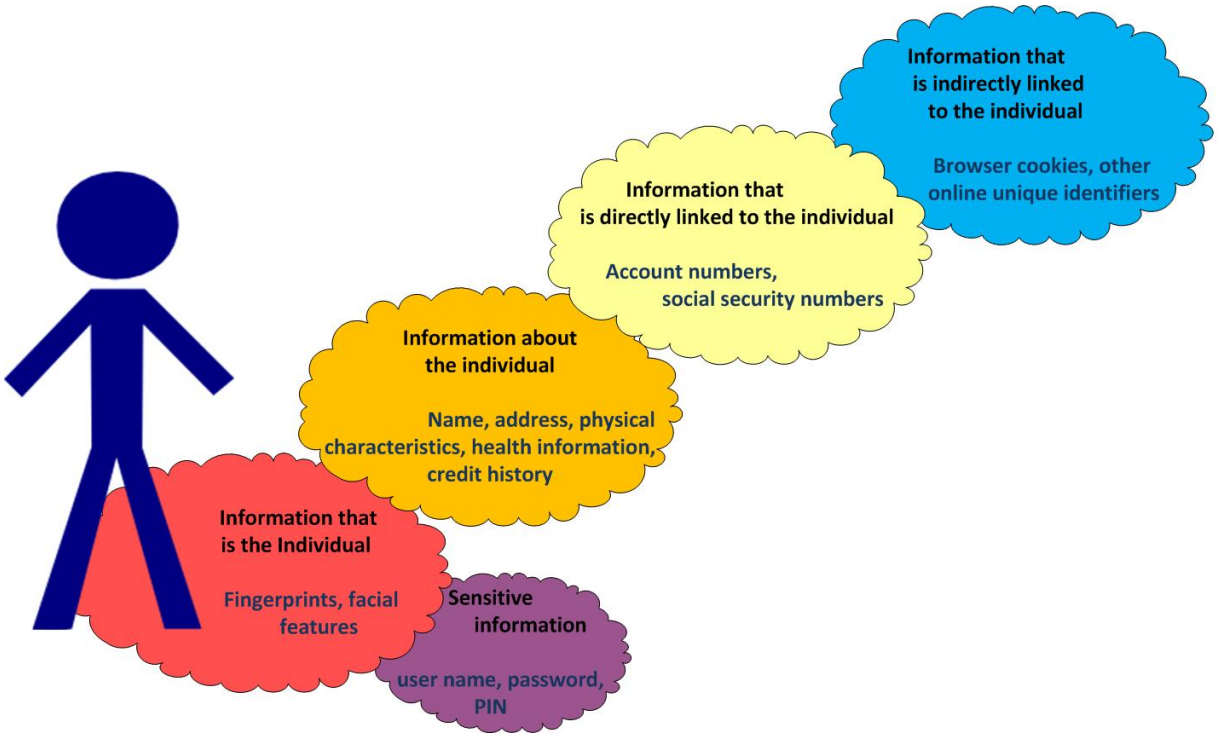


Figure 5

Using this spectrum, one could prioritize the data elements in order to address the different categories of personal information in a more nuanced way that is more closely aligned with societal norms and in a way that potentially reduces costs for businesses collecting, using and managing personal information. The rules associated with security, notice, consent and choice could also be tailored based upon these categories as well. Swartz and Solove argue for a standard rather than a rule associated with PII that utilizes a continuum of risk identification. In addition, categorizing the date elements alone does not prescribe the optimal privacy decisions for the data, but organizations must also consider the additional risks, or absence thereof associated with the environment where the data operates.

Recommendations for Metrics

Although developing privacy measurements that address all areas of a privacy program haven't been widely adopted, implementing them within the Privacy Impact Assessment (PIA) process, which is only one part of the overall program, seems to be a reasonable approach and a good starting point for companies that are struggling with defining useful metrics. The PIA process is

purposed as a tool to identify and manage privacy risk. Similarly, the information security domain has mature process for identifying and managing security risks, called vulnerabilities. Although not all of the components of the security vulnerability management process are readily transferrable to the privacy domain, it seems useful to think about categorizing risks with a standard set of criteria and in a repeatable way. For example, the Common Vulnerability Scoring System (CVSS) is an open framework for communicating the characteristics and impacts of IT vulnerabilities[44]. Most US federal and state agencies, along with many privacy sector organizations, utilize this framework and it also contains some security vulnerabilities that impact privacy. One such privacy-related vulnerability is: CVE-2012-0585. The Private Browsing feature in Safari in Apple iOS before 5.1 allows remote attackers to bypass intended privacy settings and insert history entries via JavaScript code that calls the (1) pushState or (2) replace State method. It was published 03/08/2012 and has a CVSS Severity Rating of Medium (5.0). Although the risk of a particular vulnerability to an organization cannot be judged solely on these common rating scores because it is also dependent upon the uniqueness of each organization's risk tolerance and infrastructure architecture, it is a way to adopt a widely accepted framework and provide some measureable numbers for process improvement.

Some of the companies we interviewed built risk rating into their enterprise PIA tool. Other companies performed the risk analysis in a more ad hoc fashion. Regardless of the form in which the risk rating process takes places, companies could start building metrics off of the risk rating process that could result in process improvement. For example, tracking metrics on all of the risks identified as HIGH and their managed outcomes; e.g. mitigated, accepted, avoided, or transferred, could provide insight into whether or not they were managed appropriately. In addition, they could be used to feed into other enterprise risk management reporting to augment existing data to provide a better risk profile for executive management. Another area for metrics in the PIA process could be to track issues (e.g. breaches and privacy complaints) and have a mechanism for tracking those back to the original identified risk. Privacy professionals could then use the issue information to reassess the previously assigned risk rating and adjust the risk analysis process accordingly. Or, if it was a previously unidentified risk, it could be added at that time.

[44] http://nvd.nist.gov/cvss.cfm and http://www.first.org/cvss/cvss-guide.html

Drone Case Study – Part II

As mentioned earlier, drones have discrete areas of control where actors operate, including: the manufacturers; those that modify the hardware and or software; and the users. However, it is a bit more complicated than that. A comparison with mobile devices is an interesting way to look at identifying the actors; uncovering that many consumer drones are also controlled by applications running on mobile devices, see Appendix X – Drone Platform. Clearly, risks associated with the consumer drone platform could also extend into the mobile device space, and vice versa.

Using a PIA to identify and treat privacy risks is a process for organizations to use, in which they have the ability to control products, assets and services. It's also potentially a cheaper proposition because use of a PIA process revolves around compliance activities regarding mostly known privacy risks. Once products are sold to consumers, manufacturers lose the ability to control the device. Instead the manufacturers must take a different approach to manage future risks for products they have deployed; therefore, a PIA is not the correct methodology to manage consumer drone risks. In its place, a Privacy by Design (PbD) approach would be more effective in reducing privacy risks to manufacturers and the end users because it focuses on building privacy into the platform itself which is where the manufacturer still maintains some level of control.

Other tools that could be used to augment the privacy by design approach include guides and privacy best practices, similar to those produced by the FTC and the California Attorney General's office for recommended privacy outcomes for mobile applications. In August 2012,The International Association for Chiefs of Police recently approved a publication, "Recommended Guidelines for the Use of Unmanned Aircraft[45]," to guide police organizations when using drones in their operations. Privacy is not the only potential policy issue facing drone technology; new rules are needed to manage the airspace where they operate. Privacy considerations will also play a role, if and when the airspace is regulated for consumer grade and potentially commercial grade drones. In April 2013, The Center for Democracy and Technology (CDT) submitted a comments paper[46] to the Federal Aviation Administration on Unmanned Aircraft System (UAS) Test Site Program. The CDT outlines a number of compelling reasons way the UAS are different than manned aircraft (cheaper to operate and

[45] http://www.aclu.org/blog/technology-and-liberty/police-chiefs-issue-recommendations-drones-look-how-they-measure
[46] https://www.cdt.org/files/file/CDTComments_FAA-UAS.pdf

better maneuverability are high on the list,) and also what privacy policies and practices should be implemented and by whom. Using the CDT paper as a guide, the UAS operators could apply a PIA approach for managing the privacy risks associated with in this new, emerging space.

Future Areas for Research

Gaps were documented during our research and we believe an additional area for meaningful inquiry is privacy risk management, including: threat modeling, risk identification, risk rating and risk management. Although all of the companies that participated in this study discussed risk analysis, there was no visibility into how privacy risks were identified, analyzed within the appropriate context and environment, or how decisions were made when applying the appropriate treatment. Since the goal of PIA's is three-fold; reducing risk for the organization, reducing risks for business partners and reducing risks for the individual, it would be valuable to build a model for privacy risk decision–making, something above a compliance-checking model. As the definition for PII grows to include more data elements, the way in which privacy risks are managed should also change.

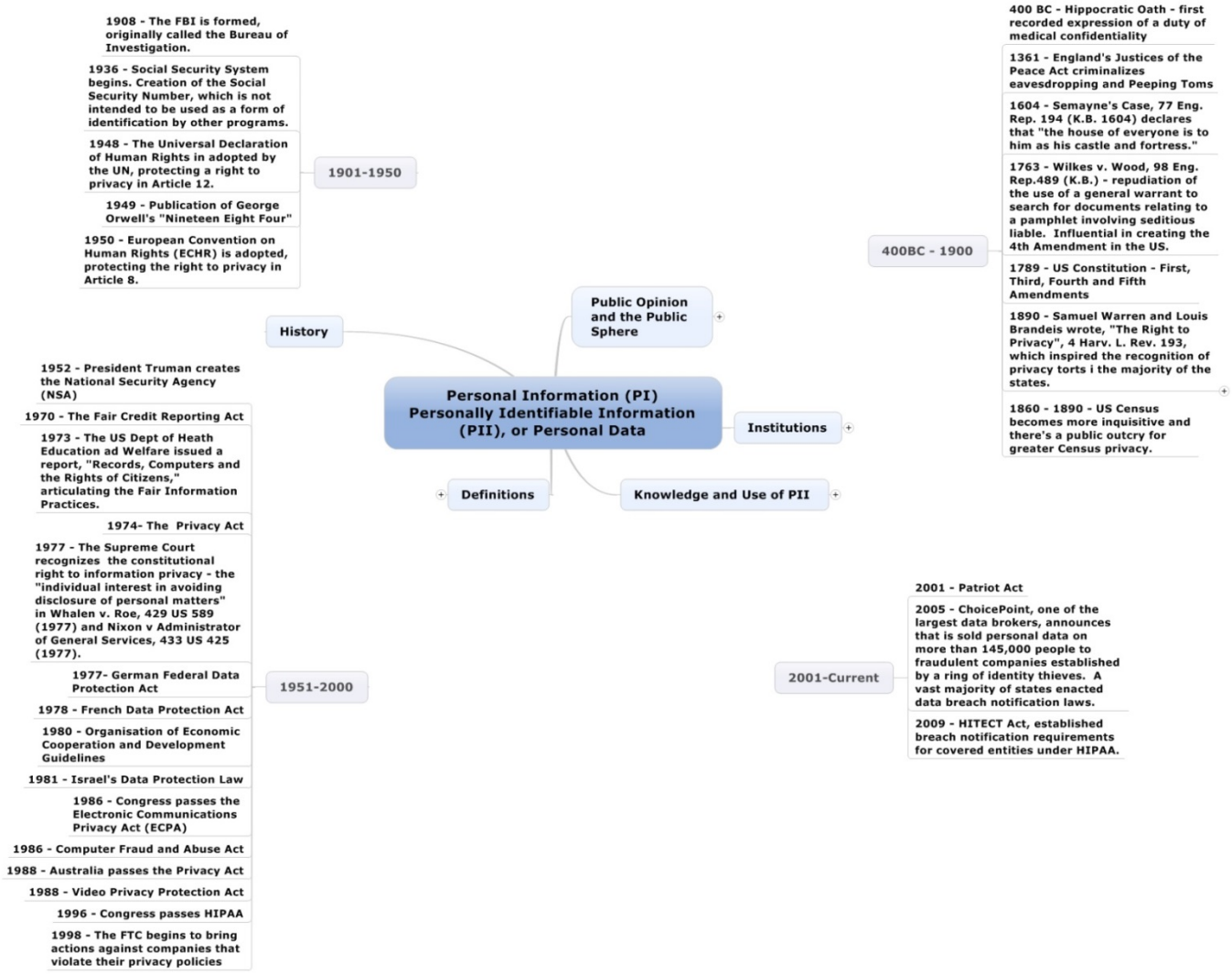
Secondly, we found no standard for useful privacy risk assessment metrics and these metrics seemed to be missing for the overarching privacy programs as well. We feel there would be value to expand this research to develop a methodology for identifying such metrics.

And, finally, PIA's are used in organizations along with other privacy risk management methodologies, such as Privacy by Design (PbD). In our findings, the PbD is used in very specialized business lines for specific purposes. Determining why two different approaches are employed, along with identifying the business costs associated with each approach, would help guide Privacy Officers and Privacy Managers in selecting the right privacy risk method for their organizations.

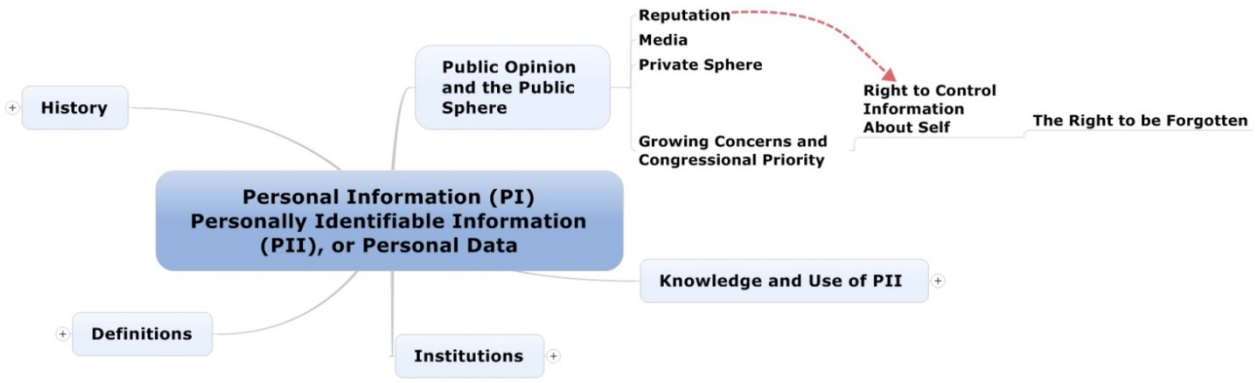
The topic of privacy risk management has come nowhere close to being exhausted as a field of valid and viable research.

Appendix I
History of Personally Identifiable Information (PII)
Mind Map Diagram (available in active PDF)

Development of Privacy Law and Other Milestones, a Sampling



Appendix II
Public Opinion & the Public Sphere of Personally Identifiable Information (PII)
Mind Map Diagram (available in active PDF)



Appendix III
Personally Identifiable Information (PII) – Defined in Laws

And Other Associated Definitions and Sources

US Code of Federal Regulations, Title 45, Part 160.103 (HIPAA)

- *Individually identifiable health information*

Information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past present, or future payment for the provision of health care to an individual; and
That identifies the individual; or

With respect to which there is a reasonable basis to believe the information can be used to identify the individual

California Civil Code Section 1798.3 Information Practices Act

- *Personal information*

The term "personal information" means any information that is maintained by an agency that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number,

education, financial matters, and medical or employment history. It includes statements made by, or attributed to, the individual.

California Civil Code Section 1798.29 et seq. California Breach Notification Law (SB 1386)[47]

[47] Similar but doesn't include medical and health except as specified: AK, AZ, AK, CO, CN, De, FL (adds MN and LN) Georgia (Any of the items contained in subparagraphs (A) through (D) of this paragraph when not in connection with the individual's first name or first initial and last name, if the information compromised would be sufficient to perform or attempt to perform identity theft against the person whose information was compromised), HA, ID, IL, IA (adds other unique id # created or collected by a government body, unique electronic identifier or routing code, in combination with any required security code, access code, or pw that permit access to a financial account, unique biometric data, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data) KS, LA, MR (individual taxpayer identification number) ME (Account number or credit card number or debit card number if circumstances exist wherein such a number could be used without additional identifying information, access codes or password), MA, MI, MN, MO(adds medical and heath), MS, MT (An individual's name, signature, address, or telephone number, in combination with one or more additional pieces of information about the individual, consisting of the individual's passport number, driver license or state identification number, insurance policy number, bank account number, credit card number, debit card number, passwords or personal identification numbers required to obtain access to the individual's finances, or any other financial information as provided by rule. A Social Security Number, in and of itself, constitutes p), NB (adds biometric), NV (both are unencrypted), NH, NJ (Dissociated data that, if linked, would constitute PI is PI if the means to link the dissociated data were accessed in connection with access to the dissociated data), NY uses term private information to mean data, and personal information to mean Information concerning a natural person which, because of name, number, personal mark, or other identifier, can be used to identify such natural person,, NC (adds digital signature and passport); ND adds dob, mother's

- *Personal information*

Breach notification:
g) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
(1) Social security number.
(2) Driver's license number or California Identification Card number.
(3) Account number, credit or debit card number, in combination with any required security **code**, access **code**, or password that would permit access to an individual's financial account.
(4) Medical information.
(5) Health insurance information.
(h) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local
Government records.
(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.
(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

California State Constitution

- *Privacy*

SECTION 1. All people are by nature free and independent and have Inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy.

California Civil Code Section 1747.08 Song Beverly Credit Card Act

- *Personal information*

For purposes of this section "personal identification information," means information concerning the cardholder, other than information set forth on the credit card, and including, but not limited to, the cardholder's address and telephone number.
California Supreme Court ruled in 2011 that this includes zip code information. "In light of the statute's legislative purpose of addressing "the misuse of personal identification information for, *inter alia*, marketing purposes," zip codes should constitute PII because they are "both unnecessary to the transaction and can be used, together with the cardholder's name, to locate his or her full address." The Court noted that a contrary interpretation would "permit retailers to obtain indirectly what they are clearly prohibited from obtaining directly, 'end-running' the statute's clear purpose" and "vitiat[ing] the statute's effectiveness."

---

maiden name, ID # assigned by employer and digital signature, OH, OK, OR(adds passport and foreign nation id#),PA, PR adds tax information and work-related evaluations, RI, SC, TN, TX (both unencrypted- including medical info), UT, VT, VA, WA, WV.

Family Educational Rights and Privacy Act (FERPA) 34 CFR Part 99

- *Personally identifiable information*

The term includes, but is not limited to: the student's name; the name of the student's parent or other family members; the address of the student or student's family; a personal identifier, such as the student's social security number, student number, or biometric record; other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name; other information that, alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or information requested by a person who the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Organization for Economic Cooperation and Development Guidelines (OECD)

- *Personal data*

"personal data" means any information relating to an identified or identifiable individual (data subject)

Personal Information Protection and Electronic Documents Ace (PIPEDA)

- *Personal information*

Personal information means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing, (a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual, (b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved, (c) any identifying number, symbol or other particular assigned to the individual, (d) the address, fingerprints or blood type of the individual, (e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations, (f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence, (g) the views or opinions of another individual about the individual, (h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and (i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual, but, for the purposes of sections 7, 8 and 26 and section 19 of the Access to Information Act, does not include j) information about an individual who is or was an officer or employee of a government (institution that relates to the position or functions of the individual including, (i) the fact that the individual is or was an officer or employee of the government institution, (ii) the title, business address and telephone number of the individual, (iii) the classification, salary range and responsibilities of the position held by the individual, (iv) the name of the individual on a document prepared by the individual in the course of employment,

and (v) the personal opinions or views of the individual given in the course of employment, (k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services, (l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and (m) information about an individual who has been dead for more than twenty years;

Non-Legal Associated Definitions

Oxford English Dictionary Definition

- 5. a. Knowledge communicated concerning some particular fact, subject, or event; that of which one is apprised or told; intelligence, news.

> 1956 A. Wilson *Anglo-Saxon Attitudes* i. i. 7, I should be glad of any personal information you may care to provide me with upon this neglected and important young poet.

Solove & Swartz, Privacy, Information and Technology 2nd edition – p.1

- *Information privacy*

Concerns the collection, use, and disclosure of personal information.

Solove & Swartz, Privacy, Information and Technology 2nd edition – p.1, 2

- *Decisional privacy*

Traditionally about the freedom to make decisions about one's body and family, but information privacy incorporates the elements of decisional privacy as the use of data both expands the limits of individual autonomy.

Solove & Swartz, Privacy, Information and Technology 2nd edition – p.2

- *Information privacy law*

An interrelated web of tor law, federal and state constitutional law, federal and state statutory law, evidentiary privileges, property law, contractual law, and criminal law information.

- *Information privacy law*

Raises a related set of political, policy and philosophical questions.

Solove & Swartz, Privacy, Information and Technology 2nd edition – p.2

- *Information privacy*

Concerns the power of commercial and government entities over individual autonomy and decision making.

- *Information privacy*

Issue of growing public concern, has become a priority on the legislative agenda of Congress; new laws and legal development regarding information privacy.

Solove & Swartz, Privacy, Information and Technology 2nd edition – p.2

- *Privacy*

An issue of paramount significance for freedom, democracy and security.

Rosen, The Unwanted Gaze – the Destruction of Privacy in America, p.25

- *Recording and exchange of personal information*

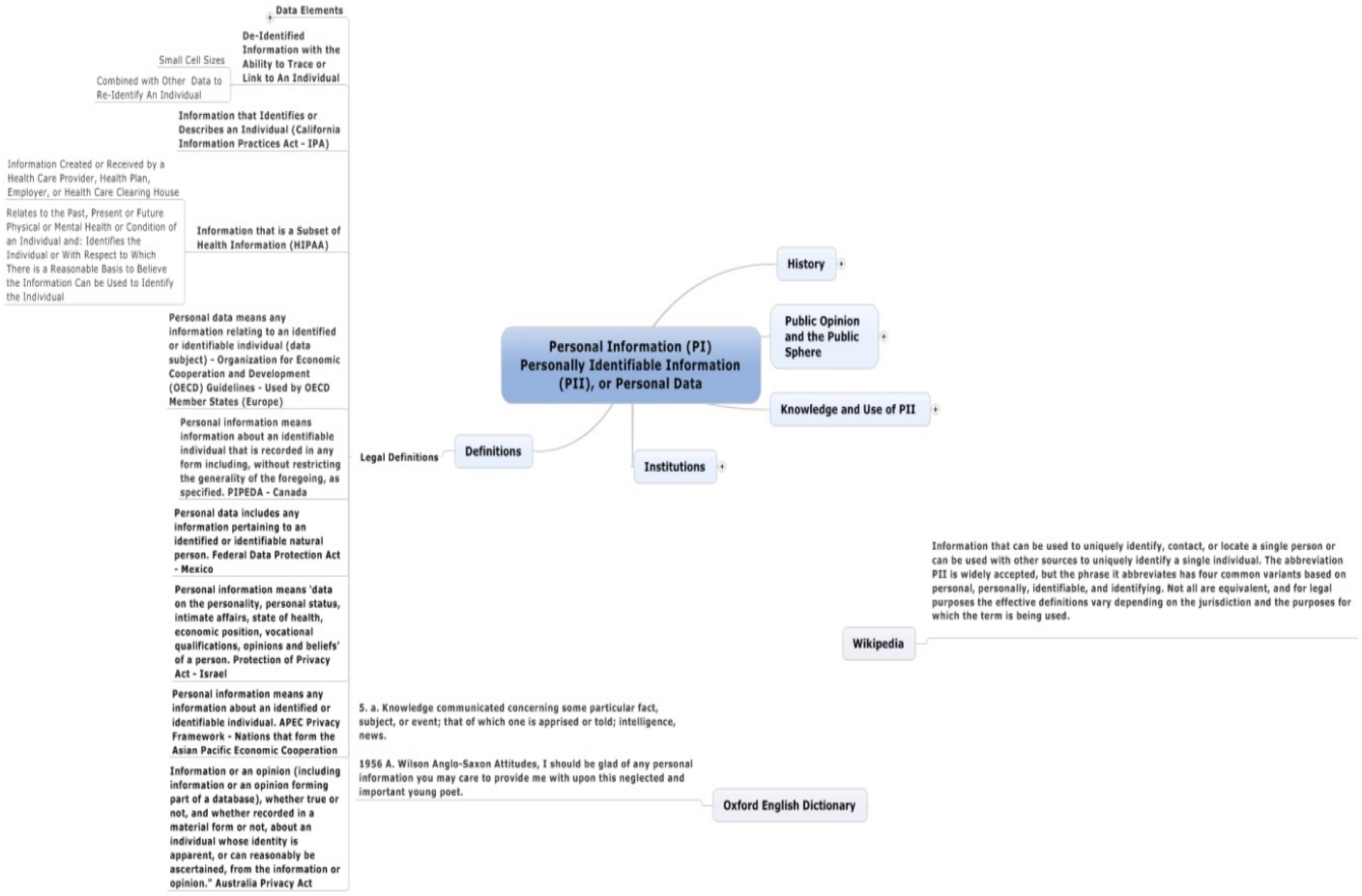
The danger of misjudging people by confusing information with knowledge in an economy that is increasingly based on the recording and exchange of personal information.

Wikipedia - http://en.wikipedia.org/wiki/Personally_identifiable_information

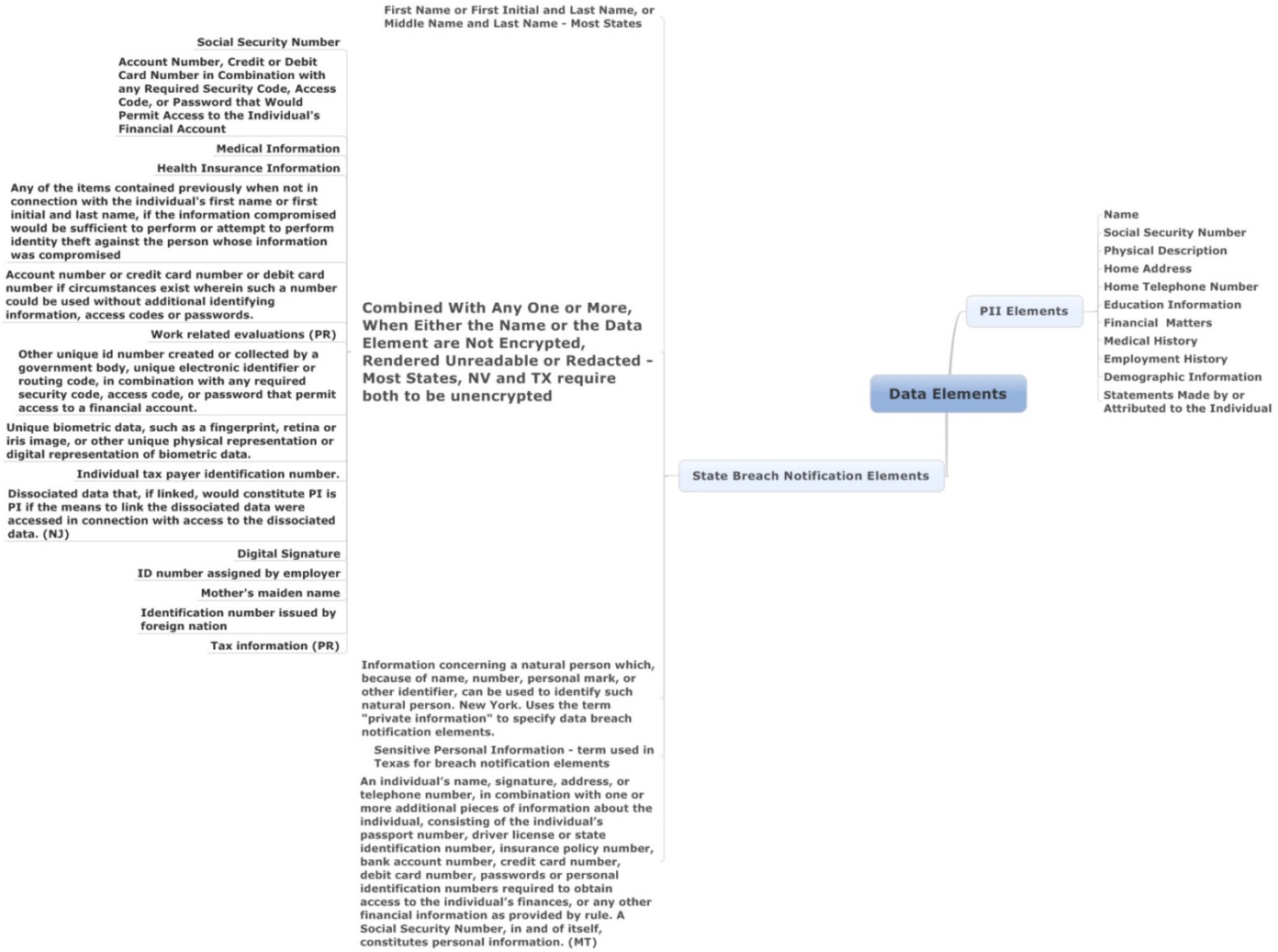
- *Personally identifiable information*

Information that can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual. The abbreviation PII is widely accepted, but the phrase it abbreviates has four common variants based on *personal*, *personally*, *identifiable*, and *identifying*. Not all are equivalent, and for legal purposes the effective definitions vary depending on the jurisdiction and the purposes for which the term is being used.

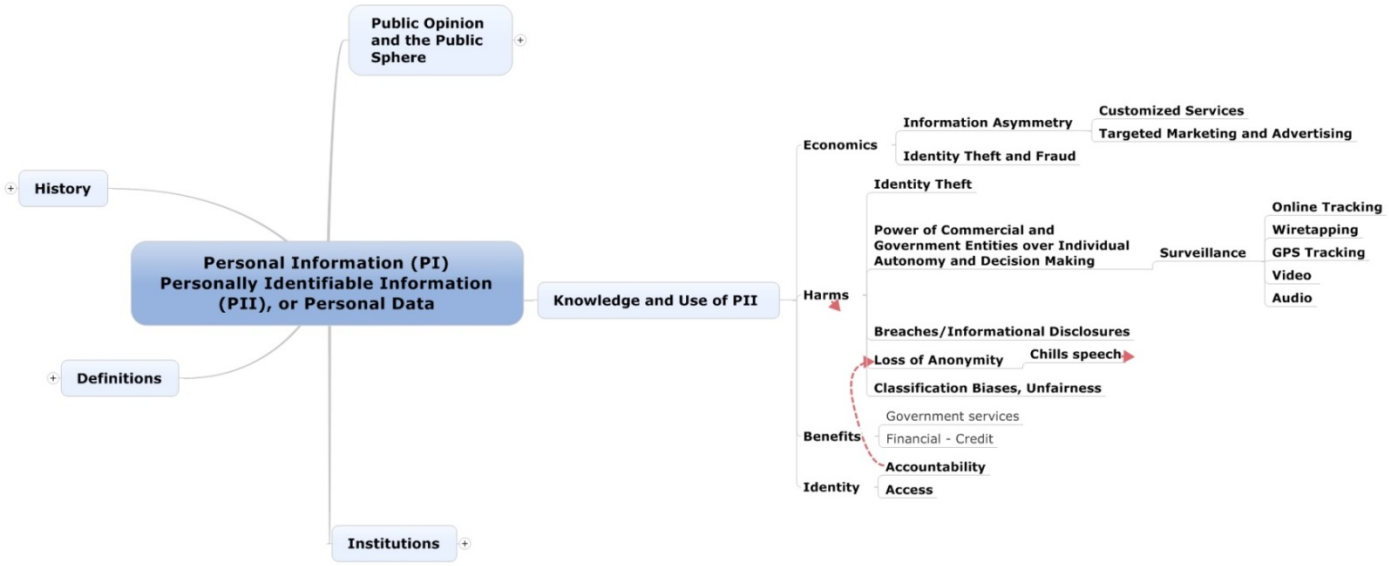
Appendix IV
Definitions for Personally Identifiable Information (PII)
Mind Map Diagram (available in active PDF)



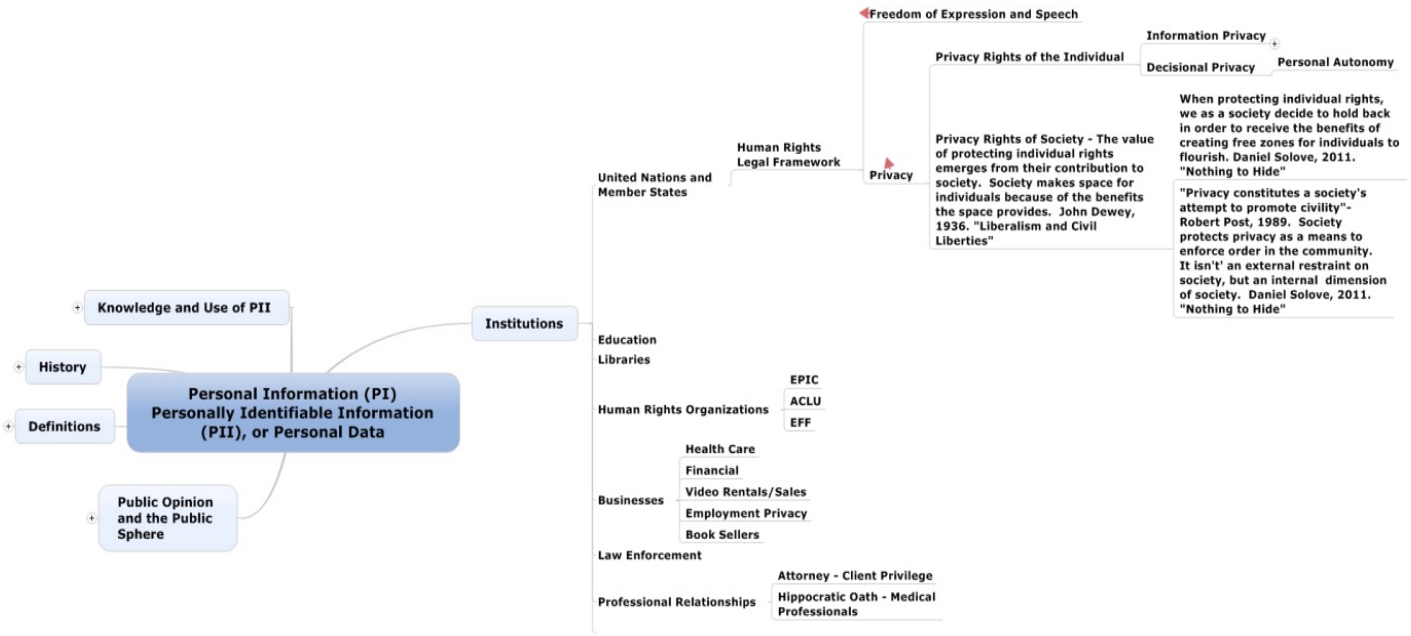
Appendix V
Data Elements (Definitions) for Personally Identifiable Information (PII)
Mind Map Diagram (available in active PDF)



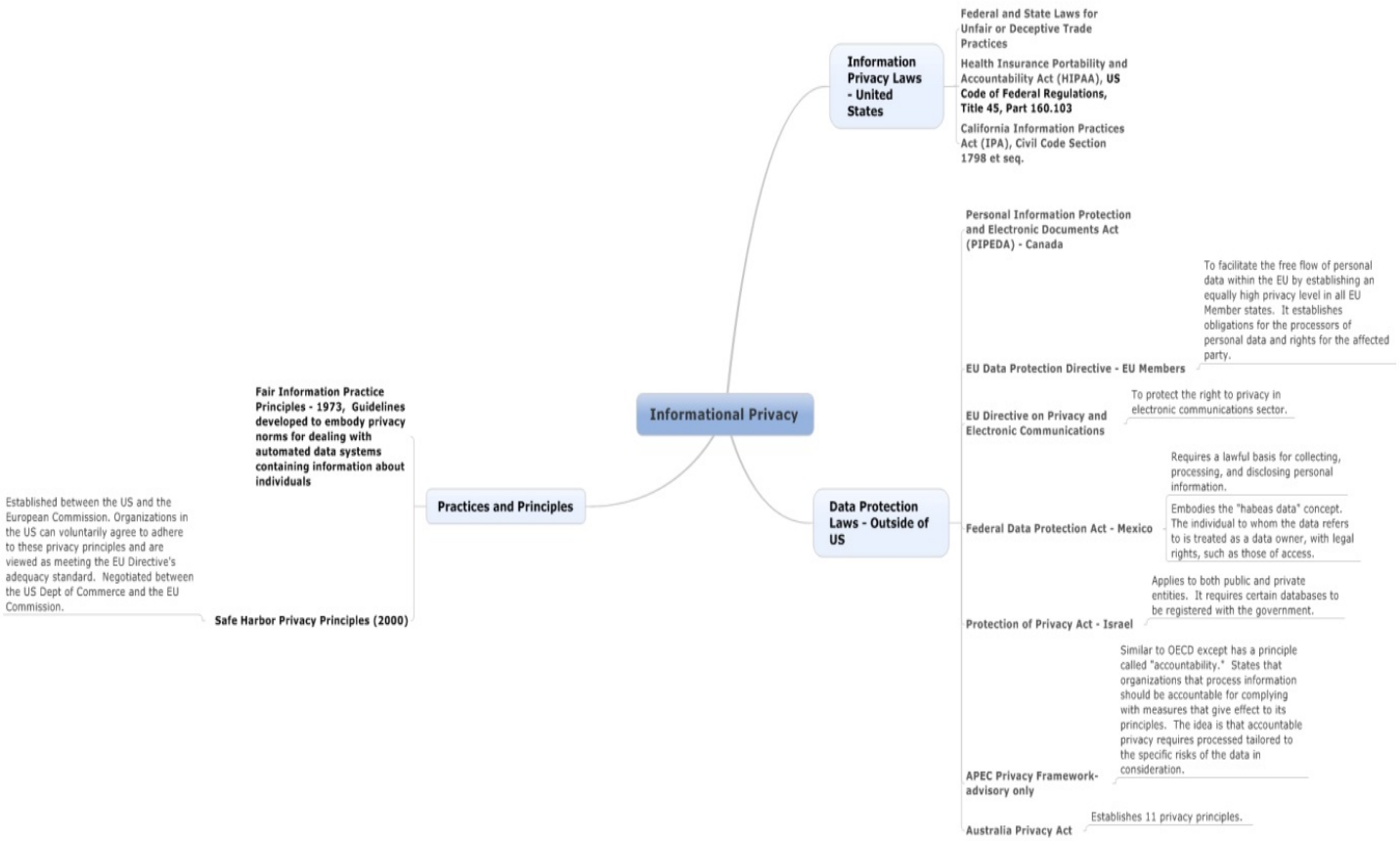
Appendix VI
Knowledge and Use of Personally Identifiable Information (PII)
Mind Map Diagram (available in active PDF)



Appendix VII
Institutions for Personally Identifiable Information (PII)
Mind Map Diagram (available in active PDF)



Appendix VIII
Informational Privacy (Institutions for PII)
Mind Map Diagram (available in active PDF)



Appendix IX
PIA Interview Codes

Communications: internal
Communications: soft tools
Communications: external

Education

Governance: executive management
Governance: steering committee

Internal Factors: culture influence on PIA process
Internal Factors: organizational structure
Internal Factors: percentage of time spent on PIA process
Internal Factors: PIA policies
Internal Factors: purpose of PIA

Job title/function

Methods: other risk management practices
Methods: other privacy best practices

Metrics

Process: automated
Process: escalation process
Process: integrating privacy in other processes
Process: PIA process trigger
Process: updating and maintaining

Relationships: auditors
Relationships: business groups
Relationships: executives
Relationships: internal SME's
Relationships: IT security
Relationships: legal office

Resources: other

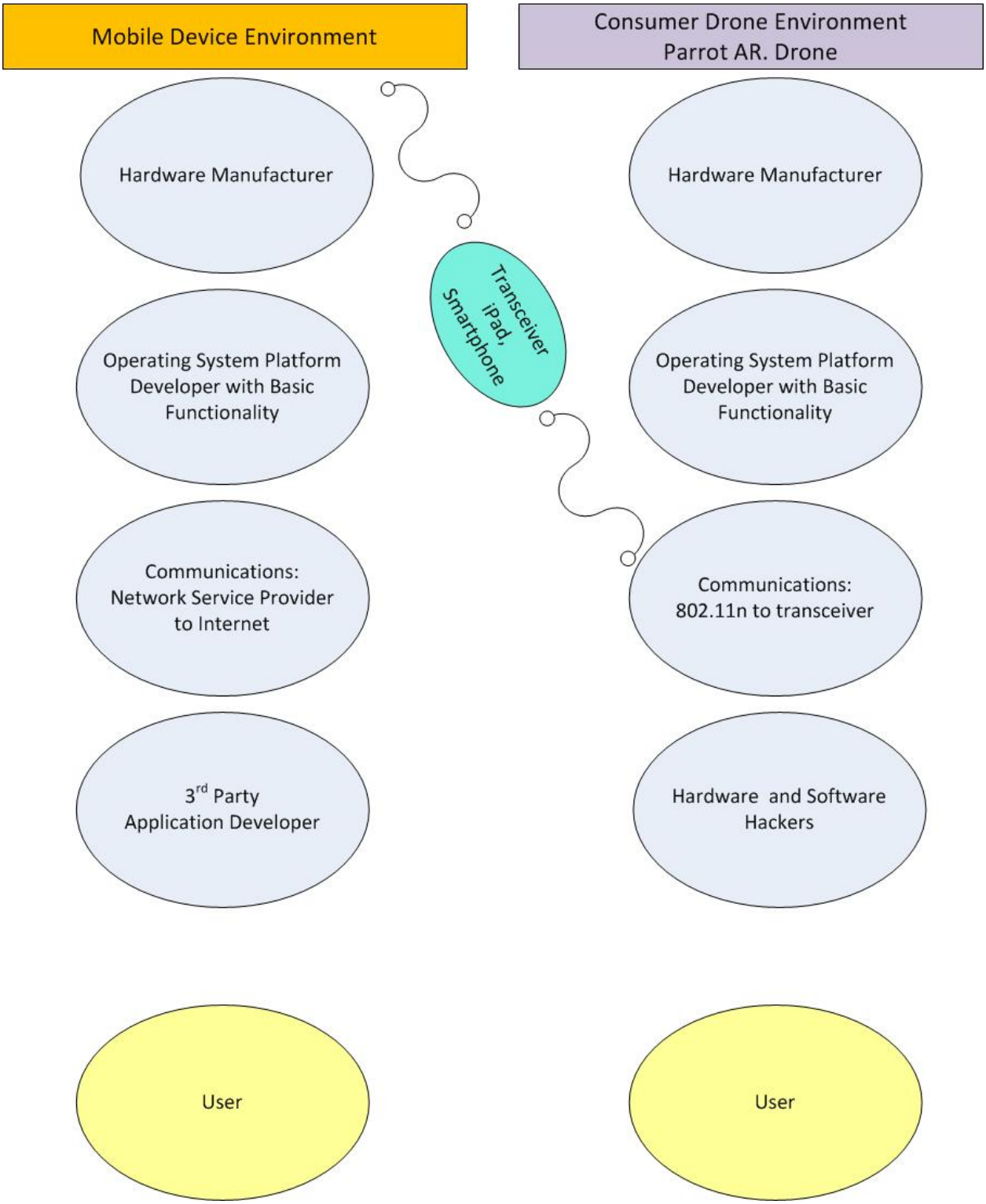
Responsibilities: approval
Responsibilities: compliance
Responsibilities: privacy resources in the organization
Responsibilities: risk mitigation
Responsibilities: audits

Stakeholders: engaging external stakeholders
Stakeholders: internal resources

Tool: intake tool

Tool: interaction
Tool: other privacy risk management tools
Tool: PIA questionnaire
Tool: PIA template
Tool: threshold analysis
Tool: tracking
Tool: universal PIA management system
Tool: updating and maintaining

Appendix X – Drone Platform



REFERENCES

Abu-Nimeh, S., & Mead, N. R. (2009). *Privacy Risk Assessment in Privacy Requirements Engineering*. *Requirements Engineering and Law RELAW 2009 Second International Workshop on* (pp. 17-18). IEEE. doi:10.1109/RELAW.2009.10

British Columbia Office of the Government Chief Information Officer. (2012). Privacy Impact Assessment Form. Web. https://www.privacyassociation.org/resource_center /2012_07_25_privacy_impact_assessment_form

Brown, E., & Kosa, T. A. Incorporating Privacy Outcomes: Teaching an Old Dog New Tricks. , 2008 Sixth Annual Conference on Privacy Security and Trust 232–239 (2008). doi:10.1109/PST.2008.27

California Department of Justice. (2013). Privacy on the Go. Recommendations for the Mobile Ecosystem. Web. http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf

Department of Homeland Security. (2007). Privacy Impact Assessments - Official Guidance .Web. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_guidance_may2007.pdf

Farivar, C. (2012). Proposed EU law would have hit Google with nearly $1 billion in fines. ars technica. http://arstechnica.com/business/2012/04/proposed-eu-law-would-have-hit-google-with-nearly-1b-in-fines/

FTC. (2012). Mobile Apps for Kids: Current Privacy Disclosures are Disappointing. Web. http://www.ftc.gov/os/2012/12/121210mobilekidsappreport.pdf

FTC. (2012). Protecting Consumer Privacy in an Era of Rapid Change. Recommendation for Businesses and Policymakers. Web. http://www.ftc.gov/os/2012/03/120326privacyreport.pdf

FTC. (2013). Mobile Privacy Disclosures – Building Trust Through Transparency. Web. http://www.ftc.gov/os/2013/02/130201mobileprivacyreport.pdf

Glancy, D.J.(2012) *Privacy in Autonomous Vehicles*, 52 Santa Clara L. Rev. 1171. Web. http://digitalcommons.law.scu.edu/lawreview/vol52/iss4/3

Herath, K. (2011). *Building a Privacy Program, A Practioner's Guide,* 158-163. An IAPP Publication. Portsmouth, NH.

Ico. (2007). *Privacy Impact Assessment Handbook*. *Privacy Impact Assessment Handbook*. Office of the Privacy Commissioner. Retrieved from http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html

Information and Privacy Commissioner, Ontario Canada. (2010). Privacy Risk Management. Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default. Web. https://www.privacyassociation.org/media/pdf/knowledge_center/pbd-priv-risk-mgmt.pdf

Jaycox, M.M. (2011). New Agreement Between the United States and Europe Will Compromise the Privacy Rights of International Travelers. EFF.org. https://www.eff.org/deeplinks/2011/12/new-agreement-between-united-states-and-europe-will-compromise-privacy-rights

Morris, J., Davidson, A. (2003). Public Policy Considerations for Internet Design Decisions. Web. http://tools.ietf.org/id/draft-morris-policy-considerations-00.txt

Newcomer, A. (2013). Google to Pay $7 million Fine for Street View Privacy Breach. abcnews.com. http://abcnews.go.com/Technology/google-hit-million-fine-street-view-privacy-breach/story?id=18717950#.UYbgmKHn-po

Schwartz, P. M., & Solove, D. J. (2011). The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *Security*, *86*(6), 1814–1894. doi:10.2139/ssrn.1909366

Solove, D. (2007). *The Future of Reputation, Gossip, Rumor, and Privacy on the Internet*. Yale University Press. New Haven & London.

Solove, D. (2011). *Nothing to Hide. The False Tradeoff between Privacy and Security,* 47-52. Yale University Press. New Haven & London.

Solove, D. & Schwartz, P. (2008). *Privacy and the Media,* 39-58. Aspen Publishers. New York.

Solove, D. & Schwartz, P. (2009). *Privacy, Information, and Technology*, 39-59. Aspen Publishers. New York.

Solove, D. & Schwartz, P. (2011). *Privacy Law Fundamentals,* 68-70. An IAPP Publication. Portsmouth, NH.

Stewart, B. (1996,). PIAs – an early warning system. *Privacy Law & Policy Reporter.* Web. http://www.austlii.edu.au/au/journals/PLPR/1996/65.html

Tancock, D., Pearson, S., & Charlesworth, A. (2010). The Emergence of Privacy Impact Assessments. Development.

Tancock, D., Pearson, S., & Charlesworth, A. (2010). *A Privacy Impact Assessment Tool for Cloud Computing*. *Cloud Computing Technology and Science CloudCom 2010 IEEE Second International Conference on* (pp. 667-676). IEEE. doi:10.1109/CloudCom.2010.27

Warren, S. D., & Brandeis, L. D. (1890). Right to Privacy. (K. Ziegler, Ed.)*Harvard Law Review*, *4*(1), 72. Hart.

Wright, D. & De Hert, P. (2012). *Law, Governance and Technology Series 6. Privacy Impact Assessment*. Springer. New York.

Acknowledgements Much appreciation to our advisor, Deirdre Mulligan for her guidance and connections; the anonymous government and corporate Chief Privacy Officers and Managers for consenting to be interviewed about their PIA processes and for their candid discussions; members from the UC Berkeley School of Information Drone Lab class, along with other industry experts for insight on consumer drone technology; Michael Schaffer, and the School of Information UC Berkeley Info298-18 Directed Group Study class for insight, comment and discussion.