Fecha de recepción: 31 de julio de 2014 / Fecha de aprobación: 14 de noviembre de 2014

Revista de Derecho Comunicaciones y Nuevas Tecnologías

Privacy by design. Implementing privacy as a good business decision

July Galindo Q

Artículo de reflexión

DOI: http://dx.doi.org/10.15425/redecom.12.2014.11

Universidad de los Andes
Facultad de Derecho
Revista de Derecho, Comunicaciones y Nuevas Tecnologías
No. 12, Julio - Diciembre de 2014. ISSN 1909-7786

Privacy by design. Implementing privacy as a good business decision

Abstract

The interaction between individuals and technology, and the constant creation of digital products and services requires the permanent use and access of personal information. Therefore companies are requested to keep an active role in what refers to the protection of consumer privacy. Privacy by Design emerges as a movement which promotes that companies, in addition to comply with the law, should implement privacy throughout different processes of the organization, as well as the assurance of the protection of privacy by default, whenever the consumer uses the service or product. Technology is not a threat against privacy likewise, privacy is not an obstacle against technology's development.

Keywords: Law and technology, privacy, privacy by design, privacy by default, privacy policy.

Privacidad por diseño. Implementando privacidad como una buena decisión empresarial

Resumen

La interacción entre los individuos y la tecnología, así como el desarrollo constante de servicios y productos digitales, hace necesario el acceso y uso permanente de información personal, por lo cual las empresas son llamadas a mantener un rol activo en cuanto a la protección de la privacidad de los consumidores. Privacidad por Diseño, surge como una corriente que promueve que las empresas, además de cumplir con la ley, implementen la privacidad en los diferentes procesos de la organización, así como la seguridad de protección de la misma, por defecto, al momento en que el consumidor haga uso del servicio o producto. La tecnología no es una amenaza para la privacidad, así mismo la privacidad no es un obstáculo en contra de su desarrollo.

Palabras clave: Derecho y tecnología, privacidad, privacidad por diseño, privacidad por defecto, políticas de privacidad.

Privacidade por desenho. Implementando privacidade como uma boa decisão empresarial

Resumo

A interação entre os indivíduos e a tecnologia, assim como o desenvolvimento constante de serviços e produtos digitais, torna necessário o acesso e uso permanente de informação pessoal, pelo qual as empresas são chamadas a manter um papel ativo sobre a proteção da privacidade dos consumidores. A privacidade por desenho surge como uma corrente que promove que as empresas, além de cumprir com a lei, implementem a privacidade nos diferentes processos da organização, assim como a segurança de proteção da mesma, por defeito, no momento em que o consumidor faça uso do serviço ou produto. A tecnologia não é uma ameaça para a privacidade, assim mesmo a esta última não é um obstáculo contra seu desenvolvimento.

Palavras-chave: direito e tecnologia, privacidade, privacidade por desenho, privacidade por defeito, políticas de privacidade.

Privacy by design. Implementing privacy as a good business decision*

July Galindo Q**

Sumario

* How to cite this article: Galindo J., (2014). Privacy by design. Implementing privacy as a good business decision. *Revista de Derecho, Comunicaciones y Nuevas Tecnologías*, 12. Universidad de los Andes (Colombia).

** uly Galindo Q. holds a law degree from Universidad de Los Andes in Bogotá (2007). Specialist in commercial law from the Universidad de Los Andes (2008). Assistant of Summer Course, emphasizing in transnational copyright and World Trade Organization, Georgetown University, Center for Transnational Legal Studies, London, United Kingdom (2010). Member of the Department of Intellectual Property, Information Technology and Entertainment at Cárdenas & Cárdenas Abogados (2007-2013). Master of Laws (LL.M.), Certificate in law & technology, University of California, Berkeley, School of Law, United States (2014). Currently she works as Senior Associate of the Privacy & Consumer Protection area of the law firm Cárdenas & Cárdenas Abogados. E-mail: jgalindo@cardenasycardenas.com, galindo.july@gmail.com

Introduction

The exponential growth of technology, and more specifically, the constant and unavoidable immersion of personal information during its use, indicates a need for a clear set of rules, principles and proceedings as to how companies can continue the technological race while still incorporating practices that protect people's personal data.

The consumer expects control over the information, security standards of the receiver and fairness of the business practices, from the developer of any service or product. These aspects are reflected in the company's management of personal information, which in the end, should respond to the users' expectations as to how a business executes the management of privacy. This moment requires a shift from the dominating privacy compliance/remedy approach to a more proactive role on the side of the companies. Privacy by design arises as an instrument to help organizations implement privacy by default. Privacy will be embedded accordingly from the earliest stages of the creation of a service or product, it will cease then to be a matter reserved only for lawyers, as privacy will also be a relevant aspect for the developers' design process. Certainly, how the organization locates the common interests of privacy, user protection, innovation and profitability will have an effect over the response to the ever-increasing challenges of data privacy management.

Privacy is a good business decision, and the ability to implement it as default gives organizations a competitive advantage. Nowadays, the consumer has become the target of constant messages (from government, news, peers, family members, etc.) related to the need to actively protect personal information. The context in which companies do business is different, the costumer is different, and smarter, and this change requires companies to provide the protection for which the costumer is asking. The company that is able to provide privacy protection will have a better market position and will even arise as the recipient of the group of costumers that have decided to abandon services and products that, in their opinion, do not fulfill, in a coherent and integral manner, their privacy expectations.

I. WHY PRIVACY BY DESIGN?

Each day users are more aware about their privacy, and how their personal information is managed. Failures to protect privacy and missuses of personal data, become newsworthy and public relations nightmares (for the company), and each day the public impact is greater. We can mention recent scandals involving privacy violations associated with entities from the public and private sector. The National Security Agency (NSA) was accused of espionage and surveillance programs over domestic (US) civilian communications; the programs were presumably even extended to tape German Chancellor Angela Merkel's mobile phone.[1] In 2012, Google

1 *See, A chronology of the NSA surveillance scandal*, DW.DE, http://www.dw.de/a-chronology-of-the-nsa-surveillance-scandal/a-17197740 (last visited March 25, 2014)

agreed to pay 22.5 million (the largest fine that the Federal Trade Commission (FTC) has ever issued), after the FTC concluded that Google misrepresented privacy assurances "to users of Apple Inc.'s Safari Internet browser that it would not place tracking "cookies" or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC."[2] Target Corporation faced a privacy security data breach that compromised personal information of costumers that purchased items from Target's US stores from November 27 to December 15, 2013.[3] The personal information involved in the data breach incident was known to be the customer name, credit or debit card number, and the card's expiration date and CVV.[4] These are only a few examples of privacy incidents[5] that have made it to the news, exposing the relevancy of privacy to the public eye while having a directly detrimental effect over the reputation of the entities therein involved.[6] These incidents, and their media exposure, increase people's expectations, which demands a response through the measures and practices that companies design, to engage in the correct management of personal information.

Complying with standards and regulations related to privacy should not be considered by companies as a remedy or response to incidents that compromise personal information. Rather, privacy should be present throughout the entire creation and design process of a specific service or product. The challenge then is how to understand and translate users' privacy expectations, and existing standards and regulations, into the design and future use of the creation. Thinking of how to preserve and incentivize privacy, while including it in the development process of the product itself, is what privacy by design is about. After all, this concept corresponds to the action of realizing privacy standards, practices and expectations, through code.[7] In this sense, and by implementing a program of privacy by design[8], organizations will be able to actively achieve the compliance of privacy standards, regulations and expectations, and to prevent privacy inci-

2 *Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser*, FTC. GOV, http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (last visited March 25, 2014)

3 *See, A message from CEO Gregg Steinhafel about Target's payment card issues,* CORPORATE.TARGET.COM, https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca (last visited March 25, 2014)

4 *See id.*

5 *See* Acquisti, Alessandro; Friedman, Allan; and Telang, Rahul, *Is There a Cost to Privacy Breaches? An Event Study (2006). ICIS 2006 Proceedings.* Paper 94, *available at* http://aisel.aisnet.org/icis2006/94 (last visited March 26, 2014) (mentioning that a privacy incident, in a broad descriptive understanding, corresponds to "an event involving misuse of individuals' personal information. This misuse can consist of illegal sale, or usage, or lack of protection. It can be criminal, commercial, or ultimately innocuous. It can be intentional or unintentional. It can involve customers', partners', or employees' data.")

6 *See* Ira S. Rubinstein; Good, Nathaniel, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents,* 28 BERKELEY TECH. L.J. 1333, 1336 n.7 (2013) (discussing that in general, privacy incident correspond to privacy concerns and "not every privacy incident results from a design failure or causes harm. However, because privacy is highly cherished and causes anxiety if violated, many privacy incidents are associated with negative press coverage, reputational harm, regulatory investigations, and/or enforcement actions".)

7 *Id.* at 1341.

8 *Id.* at 1336. (making reference to the possibility of firms like Google and Facebook of averting privacy incidents if they had implemented privacy by design programs)

dents[9]. By virtue of this baseline principle, companies "promote consumer privacy throughout their organizations and at every stage of the development of their products and services".[10]

In February 2014, TIME magazine published an article[11] serving as an example of the importance that users nowadays give to the privacy of their information. In the article *"How I Quit Google,"* the author explains her reasons for ceasing to use any kind of service related to Google. It is relevant to clarify before continuing with this explanation (that by no means is here argued) that personal information should never be shared nor collected as a result of the user-product/service interaction. Nonetheless, it is no secret that a company's behavior towards privacy may be a deal breaker during the decision-making process of a user deciding between products or services with comparable purposes/functions. To this effect, the user's privacy practices and choices will directly correspond with the implemented privacy by design program.

In the article, Julia Agwin describes her privacy concerns after noticing the amount of personal information that Google collected about her. In her words "I had long been worried that Google knew too much about me — after all, like most people, I used Google search, Google maps, Google docs and Gmail on a daily basis. Not to mention the Google ads that tracked me across the Web."[12] After accessing the collected search queries that Google keeps from every user as part of its tracking feature, Agwin found that the information went back to the moment she opened her Gmail account in 2006. In total, she found 26,000 Google searches performed by her. She found that the categorized searches reflected her likes and interests, and were even a representation of the activities she had performed, and of her thoughts throughout the day. Agwin described the searches, as being more "intimate than a diary," to the point she affirmed, "my searches are among the most sensitive information about me". The extremely large amount of information, and the possibility of such information being used to obtain correlated results about her future interests and behavior (big data), led her to make the first decision: quitting Google search. She moved to a search engine called DuckDuckGo.

DuckDuckGo is a search engine that offers the search service without tracking the user; its premise is not collecting or sharing personal information. As an example of the "search leakage" that is involved in other search engines, DuckDuckGo explains in its privacy policy "when you do that private search, not only can those other sites know your search terms, but they can also know that *you* searched it. It is this combination

9 *See,* Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, (2011), http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf (last visited March 26, 2014) (explaining, that privacy by design should be preventative and not remedial. "…*Privacy by design* comes before-the-fact, not after").

10 Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policy makers* (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter FTC 2012 Report]

11 *See,* Julia Angwin, *How I Quit Google*, Time, http://time.com/9210/how-i-quit-google/ (last visited March 26, 2014)

12 *Id.*

of available information about you that raises privacy concerns. DuckDuckGo prevents search leakage by default. Instead, when you click on a link on our site, we route (redirect) that request in such a way so that it does not send your search terms to other sites. The other sites will still know that you visited them, but they will not know what search you entered beforehand."[13] Certainly, this type of anonymous search service is having some impact over users preferences. According to DuckDuckGo's traffic statistics, it went from having 1000000 average queries per day (as of July 2012) to 5000000 (in average) by January 2014.[14] Likewise, search engines like www.startpage.com and www.ixquick.com, describe themselves as the "world's most private search engine". Both offer the anonymous search service, and function under a "zero data collection policy."[15]

These are a few examples that provide relevant information as to how privacy by design can serve as the added value of a product or service. How a company incorporates privacy in its product design will likely have a direct effect over consumer preference. Certainly, understanding how to effectively implement privacy in a product and organization is a relevant aspect to consumer behavior. At the end, privacy by design is the realization of a creative process, which by mixing privacy and innovation implies a good business decision. An organization that implements privacy by design, offers privacy assurance as a "default mode of operation."[16] In contrast, an organization that lacks privacy by design will consider it only as a response to, for example, data breach incidents. If the costumer has privacy concerns similar to those of Julia Agwin, the good business decision will most likely come from the former organization rather than the latter. This decision is related to the fact that "privacy is becoming a business issue, and its protection is becoming an important aspect of an organization's ability to inspire and maintain consumer confidence, trust and loyalty".[17] Consequently, how privacy by design is efficiently embedded can serve as the tiebreaker.

Quitting Google services may seem a somewhat extreme decision, considering that there is an substantial number of users who appreciate the service generated suggestions about shopping, searches and general interests that result from Google's tracking features.[18] This functionality facilitates daily life. A vivid example is the struggle Julia Agwin had to face after deciding to migrate to DuckDuckGo search engine. Google's search suggestions were not available anymore, which

13 DuckDuckGo, https://duckduckgo.com/privacy#s1 (last visited March 26, 2014)

14 *Id.* at https://duckduckgo.com/traffic.html

15 StartPage, https://startpage.com/eng/privacy-policy.html, (last visited March 26, 2014)

16 Cavoukian, *supra* note 8.

17 Ann Cavoukian, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers*, (2011), http://www.ipc.on.ca/images/Resources/pbd-law-policy.pdf, at 8 (last visited March 26, 2014)

18 *See* Cecilia Kang, *Google Announces Privacy Changes Across Products; Users Can't Opt Out*, Washington Post. (Jan. 24, 2012), http://www.washingtonpost.com/business/economy/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQArgJHOQ_story.html (last visited March 27, 2014) (explaining Google's combination of data of registered users across YouTube, Gmail and Google Search, will help it to better tailor its ads.)

implied an additional amount of effort to find the required information.[19]

Agwin's experience illustrates something more. It shows how a user went from interacting and appreciating a service rendered to becoming deeply concerned about a company's privacy practices. For this costumer, the company's (Google for the purpose of this example) privacy practices were out of proportion. And Agwin is not the only one, this number is significantly increasing.

After a survey conducted in December 2013, TRUSTe[20] was able to determine that "consumer online privacy concerns remain extremely high with 92% of US Internet users worrying about their privacy online compared with 89% in January 2013. The high level of concern is further evidenced by 47% saying they were always or frequently concerned and 74% were even more concerned than last year."[21] The TRUSTe Report also showed that "58% were concerned about businesses sharing their personal information with other companies and 47% were concerned about companies tracking their online behavior to target them with ads and content."[22] These numbers would be irrelevant if the user decided to disregard her privacy concerns[23], but this is not the case.

In the TRUSTe Report, it was possible to determine that 53% of the respondents strongly agreed with the statement of "I avoid doing business with companies who I do not believe protect my privacy online."[24] This percentage shows that the consumer is now willing to do something about privacy concerns, i.e. choose one product or service over another, or even decide to opt out.

Furthermore, through the TRUSTe Report it was established that "70% of US internet users feel more confident that they know how to manage their privacy online than one year ago"[25], meaning that consumers are becoming smarter about managing their privacy.[26] This can be translated nowadays into the increase of users' knowledge as to which company they should trust the management of their personal information. Hence, companies embark on the challenge of building trust, which may be achieved by putting into practice two complementary elements.[27] First, the company should be transpa-

19 *See* Agwin, *supra* note 11.

20 TRUSTe is described as a US company and global leader in Data Privacy Management (DPM) programs, *About TRUSTe*, http://www.truste.com/about-TRUSTe/ (last visited March 27, 2014)

21 TRUSTe, TRUSTe 2014 US Consumer Confidence Privacy Report Consumer Opinion and Business Impact (2014) [hereinafter TRUSTe Report], at 3 *available at* http://info.truste.com/lp/truste/Web-Resource-HarrisConsumerResearchUS-ReportQ12014_LP.html

22 *Id.* at 3.

23 *See id.* at 6 (determining that the top 6 reasons for increase in online privacy concerns in 2013, consisted of: Businesses sharing user's personal information with other companies (58%), companies tracking user's online behavior to target her with ads and content (47%), reports of government surveillance programs (e.g. NSA, PRISM) in the media (38%), privacy policies of Facebook and other social media sites (29%), companies tracking user's location via her smartphone (24%), privacy policies of Google and other search engines (21%))

24 *Id.* at 11.

25 *Id.* at 11.

26 *See id.* at 11.

27 *See* pwc, 10Minutes on Data Privacy: Build Consumer Trust Through Data Privacy (February 2014) [hereinafter pwc Report], *available at* http://www.pwc.com/en_US/us/10minutes/assets/pwc-data-privacy.

rent with the information it provides to the user through its privacy policies regarding the procedure of collecting, further use and sharing of the information. Second, the company as an organization, where different inner actors interact for the creation of a product, should be on the same page. This means "developing proactive processes for considering privacy in the design of products and other business processes that collect or use consumer data, rather than taking a reactive approach to dealing with privacy issues after they emerge."[28]

To acknowledge costumers' thoughts and behavior towards privacy is to recognize that privacy should be viewed by companies as a business matter, and not only as a compliance issue. Taking privacy by design into consideration, throughout the life cycle of a product or service, will help a company to execute a strategy where privacy is transformed into a competitive business advantage. Implementation of privacy by design will provide a company with the necessary tools to supply the demand of a specific market that is based on trust and privacy expectations.[29]

Take the mobile applications market as an example. This sector has been repeatedly involved in privacy related incidents in different jurisdictions.[30] In 2012, the Groupe Speciale Mobile (GSM)[31] (formed by the Confederation of European Posts and Telecommunications (CEPT)), addressed the mobile ecosystem that allows the interrelation of individuals while engaging with creative mobile applications and services.[32]

Likewise, GSM acknowledged that this connection relied "on the real-time access and use of personal information that is often transferred globally between applications, devices, and companies."[33]

Considering the amount of information that mobile app developers collect and the risks inherent to the activity, such as malicious access to a user's personal information, the GSM issued the Privacy Design Guideline for Mobile Appli-

pdf (explaining that "[A]t a minimum, customers want to know why you're collecting their data. In our consumer privacy survey, 80% of consumers said they were willing to share personal information if the company lets them know upfront how they are going to use it).

28 *Id.*

29 *See* Ann Cavoukian, The Privacy Payoff: How Building Privacy Into Your Communications Will Give You A Sustainable Competitive Advantage, Address Before the International Association of Business Communicators International Conference 2008, New York City, New York (June 24, 2008), *available at* http://www.ipc.on.ca/images/Resources/pbd-law-policy.pdf, at 8 (last visited March 26, 2014) http://www.ipc.on.ca/images/Resources/2008-06-24-IABC-NYC.pdf (last visited March 28, 2014).

30 *See* Kirsten Gollatz, *App Development: Is 'Privacy by Design' the New Standard*, Internet Policy Review. (Mar. 28, 2013), http://policyreview.info/articles/news/app-development-'privacy-design-new-standard/117 (last visited March 28, 2014) (addressing that privacy incidents have impacted mobile phones user behavior, and has raised concerns about how apps handle personal data. It has even got to the point of avoiding installing an application or even to opt-out.) (last visited March 28, 2014).

31 *See id.* ("The GSM Association - a worldwide industry network of mobile operators - was quick to react with the publication of Privacy Design Guidelines for Mobile Application Development. Although explicitly supported by the largest European operators, these guidelines, so it is hoped, should serve as a framework for what is to become a global standard").

32 GSM, Mobile and Privacy: Privacy Guidelines for Mobile Application Development (February 2014), at 1 *available at* http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf (last visited March 28, 2014).

33 *Id.*

cation Development[34]. Moreover, the GSM stated "even applications that legitimately access and use personal information may fail to meet the privacy expectation of users and undermine their confidence and trust in organizations and the wider mobile ecosystem. Problems occur when users are not given clear and transparent notice of an application's access and use of the personal information, or when they are not given an opportunity to express meaningful choice and control over the use of their information for secondary purposes and beyond that necessary to the operation of an application or service."[35] By adopting a privacy by design approach, the GSM intended to "ensure that mobile applications are developed in ways that respect and protect the privacy of users and their personal information."[36] In the following example, the GSM Privacy by Design Guidelines provide information about the practical implementation and design of the privacy principles, by advising the mobile app developer as to how he should translate and implement the concerns and expectations about the transparency of the practices, while creating the technical features of the specific product:[37]

Guideline	Implementation	Use case and examples
Identify yourself to users Users must know who is collecting or using their personal information and how they can contact that entity for more information...	Before a user downloads or activates an application, he or she must be made aware of the identity of any entities that will collect or use personal information in the scope of the application, including a company or individual name and a country of origin. Users must have easy access (via a link or menu item) to brief contact details of the organization.	The app landing page is an excellent place to publish key privacy facts, contact information and provide a hyperlink to a more detailed privacy statement. There is no single solution to providing users with information about you, your organization, their privacy and what you'll do with their data. Be creative and encourage users to explore how best to manage their privacy — but don't burden them and keep it simple and easy.

It showed how in practice the technical development is coordinated since the initial moment, with the underlying privacy principle (in this case, transparency). In a similar fashion, to the GSM Guideline, the FTC in April 2013, and through its Business Center, issued a guide in order to help mobile app developers to observe, among other matters, privacy principles. The Marketing Your Mobile App Guide,[38] calls app developers to "build privacy considerations in from the start"[39], highlighting the relevancy of providing user with tools and features as to how she can control her personal information (i.e. privacy settings, opt-outs, etc.)

34 *See id.*

35 *Id.*

36 *Id.*

37 *See id.* at 5.

38 Fed. Trade Comm'n, *Marketing Your Mobile App: Get It Right From The Start* (April 2013), http://business.ftc.gov/documents/bus81-marketing-your-mobile-app (last visited March 28, 2013)

39 *Id.* at 2.

In the following sections of this article, I will address the Fair Information Practices (FIPs), and their evolution, as the starting point to understand what it means to design products and services with privacy in mind.[40] Then, I will turn to address the seven elements of a particular privacy by design program, along with suggestions for their implementation within an organization. Hopefully altogether, this information will help to explore how privacy, as a competitive advantage, and through privacy by design, can be put into practice.

II. FAIR INFORMATION PRACTICES (FIPS)

Since their existence, FIPs have played a key role in the regulation and behavior of entities (public and private sector) while addressing the management of personal data. These rules have been described as a "set of internationally recognized practices for addressing the privacy of information about individuals"[41]; they determine obligations to be met by organizations that process personal information.[42] They provide the underlying principles for many laws in different jurisdictions, and have contributed to the shape of US privacy statutes and European data protection law[43] while addressing privacy and data protection matters.

In order to delimit the scope of application of FIPs, it must be mentioned that they only apply to Personal Identifiable Information (PII). It has been said in that regard that, "although there is no uniform definition of PII, privacy laws 'all share the basic assumption that -in the absence of PII-, there is no privacy harm'".[44] Although it is not the purpose of this article to do so, it must be pointed out that PII does not correspond to a pacific definition. Even experts debate if the conceptualization of PII should be strictly kept to information that directly identifies a person (identified information), or if its scope should be broader. For the most part, it has been suggested that the PII approach should be revaluated (especially by US regulatory entities) in order to acknowledge the relevancy of PII as information that may include de-identified data that could be used to re-identify an individual.[45]

Considering FIP's influence, and their influence over a company's behavior while taking privacy decisions (such as privacy by design), and while processing PII, it is important to address the origin and evolution of FIPs.

40 *See* Rubinstein, Good, *supra* note 6, at 1335.

41 Robert Gellman, *Fair Information Practices: A Basic History*, (March 18, 2011), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf (last visited March 30, 2014).

42 Paul M. Schwartz; Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information,* 86 N.Y.U. L.Q. Rev. 1814 (2011) at 1824-1825, available at: http://scholarship.law.berkeley.edu/facpubs/1638 (last visited March 31, 2014)

43 *See* Rubinstein, Good, *supra* note 6, at 1337 n10.

44 *Id.* at 1357.

45 *See* Schwartz, Solove, *supra* note 44 (addressing three approaches to the PII concept, their problematic and if it should be treated as a rule or a standard, in order to respond to technology developments)

A. FIPs Origin

FIPs first started in 1973 when the Code of Fair Information Practices was enacted, originating as a contribution from the DHEW (Department of Health, Education, Welfare) Advisory Committee on Automated Data Systems.[46] This Committee was established as a response to the growing use of computers by entities of the private and public sector, which certainly implied the use of automated data systems that dealt with information about individuals.[47]

After observing the creation of the 1973 US FIPs and subsequent privacy laws enacted by member countries, the OECD decided in 1980 to issue the OECD Privacy Guidelines. The intention of said document was to provide "basic rules governing the transborder flow and the protection of personal data and privacy, in order to facilitate the harmonization of national legislation."[48] Through these Privacy Guidelines the OECD addressed problems related to, at the time, emerging international data networks and "the need of balancing competing interests of privacy on the one hand and freedom of information on the other, in order to allow a full exploitation of the potentialities of modern data processing technologies in so far as this is desirable".[49]

Similar developments took place in Europe by 1980, when the Council of Europe adopted the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data.[50] To both the OECD and the Council of Europe Convention, the US FIPs served as a baseline. Both entities "relied on FIPs as core principles, although neither document used the term. Both organizations revised and extended the original US statement of FIPs, with the OECD Privacy Guidelines being the version most often cited in the subsequent years. The OECD, Council of Europe, and the European Union expressly recognized that disparities in national privacy legislation might create obstacles to the free flow of information between countries…The goal of harmonization helped to raise interest in privacy among the business community".[51]

B. FIPs Evolution

In 2012 the FTC issued the FTC 2012 Report [52] about privacy. In this report the FTC recognized the existence of technological developments such as smart phones and smart cars,

46 *See* EPIC, *The Code of Fair Information Practices, available at http://epic.org/privacy/consumer/code_fair_info.html* (last visited March 31, 2014)

47 *See* Gellman, *supra* note 43 at 2.

48 OECD, 1980 Guidelines on the Protection of Privacy and Transborder Flows, available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3 (last visited April 1, 2014) (In this 1980 Privacy Guidelines, the OECD, identified eight principles of national application: Collection limitation principle, data quality principles, purpose specification principle, use limitation principle, security safeguards principle, openness principle, individual participation principle, accountability principle.") see http://www.oecd.org/internet/ieconomy/the30thanniversaryoftheoecdprivacyguidelines.htm (last visited April 1, 2014)).

49 *Id.*

50 *See* Council of Europe, *http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm* (last visited April 1, 2014)

51 *See* Gellman, *supra* note 43 at 7-8.

52 *See* Fed. Trade Comm'n, *supra* note 10 at i.

that allowed companies to perform constant collection, storing and sharing of information through the use of such devices. The intention of the FTC 2012 Report was to line up standards as to how companies could use the information to deliver better services and products without doing so "at the expense of consumer privacy".[53] Although the FTC 2012 Report is consistent with the FIPs articulated in 1970s, it added three new recommendations to the previous privacy framework: privacy by design, simplified choice for business and consumers, and greater transparency.[54] These recommendations come relevant at a time when the FTC has had an active role in privacy enforcement actions[55], that were mainly based on the "fairness" of the practice, and the response to privacy "consumers expectations".[56] In particular, and by encouraging privacy by design, the FTC 2012 Report invites companies to "promote consumer privacy throughout their organizations and at every single stage of the development of their products and services",[57] and to "incorporate substantive privacy protections into their practices, such as data security, reasonable collection limits, sound retention practices and data accuracy".[58]

Similarly, in 2013 the OCDE issued the 2013 OECD Privacy Guidelines[59], which consisted of the first update to the 1980 original version. The revision was necessary since "as compared with the situation 30 years ago, there has been a profound change of scale in terms of the role of personal data in our economies, societies, and daily lives. The environment in which the traditional privacy principles are now implemented has undergone significant changes".[60]

As part of this revision, the OCDE introduces the privacy management program as the medium through which to implement the newly introduced privacy by design concept. Both hold relation with the accountability principle "as a means to promote and define organisational responsibility for privacy protection"[61]. The data controller must be able to demonstrate that the privacy management program is appropriate and includes the necessary safeguards needed to protect the information by implementing privacy by design; "whereby technologies, processes and practices to protect privacy are built into system architectures, rather than added on later as an afterthought".[62]

53 *Id.*

54 *See id.*

55 The FTC has initiated administrative investigations over companies' privacy practices. FTC's complaints were initiated against Facebook Inc., and Google Inc. These cases are not an exhaustive list, but provide further information of the FTC's considerations, while analyzing the "fairness" and "consumer expectations" prongs. *See In the matter of Google Inc.* US FTC File No. 102 3136, (complaint filed March 30, 2011); *see also United States v. Google, Inc.*, No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012); *see also In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (complaint filed Nov. 29, 2011).

56 *See* Rubinstein, Good, *supra* note 6, at 1346.

57 Fed. Trade Comm'n, *supra* note 10 at vii.

58 *Id.*

59 *See* OECD, *2013 OECD Privacy Guidelines,* available at http://www.oecd.org/sti/ieconomy/privacy.htm (last visited April 1, 2014)

60 *Id.* at 3.

61 *Id.* at 23.

62 *Id.* at 24.

Although nowadays there may be dissimilar FIPs formulations that vary in crucial respects, "the different version coalesce around the following nine principles:

1. Defined limits for controllers and processors of personal information on the collection, processing and use of personal data (often referred to as data minimization);

2. Data quality (accurate, complete, and timely information);

3. Limits on data retention;

4. Notice to individual users;

5. Individual choice or consent regarding the collection and subsequent use of personal information;

6. Reasonable security for stored data;

7. Transparent processing systems that affected users can readily understand and act on;

8. Access to one's personal data; and

9. Enforcement of privacy rights and standards (including industry self-regulation, organizational measures implemented by individual firms, regulatory oversight and/or enforcement and civil litigation)."[63]

Aside from different recommendations as to which FIPs are relevant and how they must be adjusted, the evolution of the FIPs, after the FTC's and OECD's revision, agree in significant aspects: both guidelines are consistent in the importance of implementing privacy by design as a way to provide a coherent organisational response to consumer expectations, as well as the promotion of national legislation and the harmonization of international standards. Even more, companies' self-regulation, with proper privacy management, plays a crucial role.

III. PRIVACY BY DESIGN (PBD)

It was explained in the previous section that FIPs, have embodied how the proper collection and use of personal data should be executed, since the 1970s. Privacy by Design (PbD) comes to play a key role. PbD is the translation and inclusion of the FIPs, and relates to the company's self-regulatory privacy practices, while creating a product or service that responds to the interest of the consumer/market and applicable regulations.

Privacy by Design is a concept created by Ontario's Information and Privacy Commissioner, Ann Cavoukian, who presented a set of foundational principles to serve as a guide by which to achieve a balance between regulation and innovation, while keeping consistency with FIPs. It corresponded to an approach of embedding privacy into the design of the product, as a response to the high threats to online privacy that were escalating by 1990s.[64] In 2010, the Center for Democracy and Technology (CDT)

63 Rubinstein, Good, *supra* note 6, at 1343

64 *See* Cavoukian, *supra* note 18, at 3

recognized the relevancy of privacy by design as a tool to implement FIPs. Even more, the CDT had been aware of the FTC process which later would be the FTC 2012 Report that brought to the attention of said authority to observe privacy by design, "we urge the FTC to encourage the integration of Privacy by Design into corporate practices and innovation".[65] This concept was adopted by the FTC as part of its recommendations, and is one of the key points of the FTC 2012 Report.[66]

A relevant aspect of today's promotion of privacy by design is the failure of the notice and consent model. This model requires businesses to provide privacy policies that inform users how personal information is collected and used. Considering the difficulties with the readability of the privacy policy, the information displayed may not achieve the goal of providing the user with the tools to make a well-informed decision. This circumstance was noted in 2010 by the US Department, stating that "according to the comments we received, it seems the level of effective transparency and awareness of current privacy practices is low. Privacy policies are the current framework's primary mechanism for informing consumers of companies' privacy practices. The shortcomings of many privacy policies… are widely recognized: they can be dense, lengthy, written in 'legalese,' and 'overwhelming' to the few consumers who actually venture to read them."[67] Privacy policies are regarded as incomprehensible. Research performed in 2012, related to the user's understanding after reading Facebook's API service privacy policy, concluded that "less than 40 percent of Facebook users understood how –it– can be used to access and view public –user– information."[68]

Companies' have directed their privacy efforts to a legalistic and compliance approach of FIPs, giving preponderance to consumer consent-choice. However, this approach has changed. As indicated by the FTC 2012 Report, privacy conceptualization is broader. It is not anymore enough for a company to inform the user about its privacy policy, but it must also implement privacy protections by default. Meaning that, "privacy by design requires the translation of FIPs into engineering and design principles and practices"[69]. This matter can be explained with the following example: "one of the FIPs, the purpose specification principle, is the basis for limits on how long a company may retain personal data. But there is a vast difference between a company promising to observe reasonable limitations on data retention and designing a database that automatically tags personal and/or sensitive in-

65 Center for Democracy & Technology, *The Role of Privacy by Design in Protecting Consumer Privacy,* available at https://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy

(last visited April 7, 2014)

66 *See* Fed. Trade Comm'n, *supra* note 59.

67 Department of Commerce, Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,* (2010) at 32, available at http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-greenpaper.pdf (last visited April 7, 2014)

68 Emil Protalinski, *Survey: Facebook, Google privacy policies are incomprehensible*, ZDNET, http://www.zdnet.com/blog/facebook/survey-facebook-google-privacy-policies-are-incomprehensible/12420 (last visited April 7, 2014)

69 *See* Rubinstein, Good, *supra* note 6, at 1341.

formation, keeps track of how long the information has been stored, and deletes it when a fixed period of time has expired. To adapt a familiar distinction, one is just words, while the other is action realized through code."[70]

A. *Seven foundational principles of privacy by design*

The seven foundational principles are presented by Cavoukian as a way to accomplish privacy by design objectives by "ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage".[71] The seven foundational principles are described as:[72]

• Proactive not reactive and preventative not remedial: The organization should diligently strive to anticipate privacy issues before they arise. The organization should avoid acting exclusively with a remedial approach.[73]

• Privacy as the default setting: An organization should consider how to make privacy the default. If the "do nothing" option exists, then privacy must be built into the systems keeping users' privacy intact. This default principle should be consistent with users' expectations.[74]

• Privacy embedded into design: Privacy should be considered at the earliest of brainstorm stages. Privacy should not be included after the fact. One possible implementation tool is a "checklist" properly tailored to the relevant business group.[75] "The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral into the system without diminishing functionality".[76]

• Full functionality – *Positive-sum, not Zero-sum*: It is possible to have privacy and security and both privacy and functionality. Avoid to understand privacy measures as detrimental to the quality of the product or service.[77] "*Privacy by Design* seeks to accommodate all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both."[78]

• End-to-End Security – Full lifecycle protection: Implement security of the data throughout its lifecycle (full lifecycle protection). Know who has access to the data, internally and externally, and how it is shared with third parties. Have certainty as to which are the security measures, retention periods, and destruction of data (if applicable).

70 *Id.*

71 *See* Cavoukian, *supra* note 9

72 *See Id.*

73 *See* International Association of Privacy Professionals "IAPP Global Privacy Summit", March 5-7, 2014, Washington DC, *Workshop: A Step-by-Step Guide to Integrating PbD at Your Organization.*

74 *See Id.*

75 *See Id.*

76 Cavoukian, *supra* note 9

77 *See supra.*

78 *See Id.*

Workers should be trained and there should be full awareness of the activities of the staff.[79]

• Visibility and Transparency – Keep it open: put users in notice of the information you are actually collecting. Privacy policy should reflect the real condition of the privacy practices and processes, immersed in the product. Determine how aware the users/consumers are of privacy and security practices. Beware of possible verifications and audit, even from regulators. Avoid having the regulator telling the organization "what to do".[80] Trust is allowed, but also the verification of the performance of the organization.

• Respect for User privacy – Keep it user-centric: Maintain users' privacy interests as the paramount. It will help to empower the company (competitive advantage), and to set privacy as something more than just protection. Provide training, keep awareness, and have accessible internal policy statements and guidelines.[81] There should be user-friendly options.

By following the previous principles, privacy is built as an integral process, and not just by remedying situations that could in fact have been foreseen.

The legalistic approach to privacy has lead companies to commit the mistake of believing that any privacy policy is appropriate and adequate to satisfy their privacy obligations, and to engage in privacy as a "copy paste" exercise. Privacy is unique to each organization, and ignoring this fact will situate the organization under an unnecessary risk. By shifting from this legalistic understanding to an organizational mandate of following the privacy by design approach, including its seven foundational principles, a company will be able to avoid considering privacy as the final obstacle that impairs the launching of a product to the market. Likewise, the company will avoid loses in productivity since the lack of privacy compliance will probably cause the additional burden of having to redesign the product in order to adjust it to privacy standards. Companies should also keep in mind that building a product presently requires the interaction of different agents within the same organization, i.e. legal, security engineers, and what has been called as UX designers.[82] Having all agents in sync on the privacy goals of the organization and the directive of how to embed in privacy, will avoid contemplating privacy as an obstacle. Privacy will be viewed as a vehicle to continue to build trust and meet consumer's expectations, which at the end will prove to be the main benefit of the privacy by design approach. After all, privacy should be a *Positive-Sum*, *not Zero-Sum* exercise.

B. Suggestions to implement a privacy by design program, in a organization

Privacy by design may be used to assess and/or protect privacy based on the needs of the orga-

79 *See Id.*

80 *See Id.*

81 *See Id.*

82 *See* Rubinstein, Good, *supra* note 6, at 1352. (Addressing which is the optimal way to approach who is responsible within an organization for designing in privacy, and explaining the importance of including UX designers in the privacy and product design, since privacy perceptions also respond to consumer social stances.)

nization. The following suggestions, which by no means are intended to be exhaustive, are developed from the recent workshop (and its supporting material): *A Step-by-Step Guide to Integrating PbD at Your Organization,* organized by the IAPP during the 2014 Global Privacy Summit.[83] These suggestions are intended to help implement privacy by design across the entire organization, instead of a project-by-project basis. The implementation agrees with Cavoukian's suggestion of privacy by design "be applied across the board to IT systems, accountable business practices, physical design and networked infrastructure, touching every aspect of an organization".[84]

In general, a privacy by design program (PbD), should be implemented by following five main steps:

1. Initiating a PbD program:

● Identify the challenges; specially at large organizations that have multiple divisions/subsidiaries:

- Regulations: Having a clear understanding of which are the regulations (from all different jurisdictions) that must be met in order to avoid additional risks (i.e. COPPA – special restrictions for the collection of information of children under the age of 13, EU Directive). Understand the product, and how to define its scope.

- If consent is a requirement, the organization must assure that it is keeping evidence of it. This mechanism may easily be a part of the privacy design process, if the organization has properly identified the jurisdictions where it must be complied with.

- Is the company interested in limiting privacy by design to personal data? Identify how the privacy directive is going to work, how to deal with PII, and the possibility of re-identification. Is the personal data definition broad enough to comply with requirements from different agencies?

- Determine if your privacy practices are friendly enough or need to be improved.

- Costs and benefits of the privacy by design program: They should be estimated in the short and long run. A challenge may be how to address the benefits in a manner that may require the allocation of resources within the company. Perhaps a way to enhance the interest from senior management could be the creation of new strategies to monetize data, and cross-border transfer strategies.

● Identify the motivation behind the privacy scheme. It will be more evident in organizations that correspond to highly regulated sectors (e.g. health, finance, government).

● Enlist the support that is required and which are the key divisions, and chose a privacy coordinator from each one of them. Also, the organization should define wich is the role of the

83 *See supra* note 77

84 Cavoukian, *supra* note 18, at 14

Chief Privacy Officer. In case this position does not exist, define who will be in charge of assuring that privacy is being properly implemented throughout the organization.

• Promote privacy and create incentives for the developers, to actively participate in the privacy by design program.

2. Privacy Steering Committee

• This Committee, along with the Chief Privacy Officer, will be in charge of the promotion of privacy throughout the organization, i.e. in the event of a change in the administration that evidences no interest in privacy, this Committee will deal with privacy reorganization.

• Privacy Coordinators from all key divisions should be included in the Privacy Steering Committee. These Coordinators should receive special training in privacy, it will help to have a more effective implementation of the privacy by design program. Training should also be extended to executives and people that may have access to PII on random or daily basis. The training of executives/senior management will generate a better assessment of privacy risks. Some people within the organization may not know what PII is, and that it can be even collected from a simple phone call. They should be aware of the danger of unauthorized access to PII.

• At this stage the organization should establish the Privacy Coordinator responsibilities, as to:

- Coordinate privacy assessments

- Be the division privacy representative, on an incident response team

- Coordinate division privacy training

- Review division data management/vendor practices

- Work with teams on review of privacy by design checklists

• This Committee should provide training for relevant people. It will help to have them all speak the same language, and also for the understanding of the roles and responsibilities within the organization.

3. Assessment/Remediation

• A detailed questionnaire or survey for each relevant business unit will help to determine the privacy practices status, and what is subject to be improved, inserted or adjusted. Assessment of the privacy practices and how they can be improved, as well as matching privacy practices with privacy policies is necessary. The organization should always keep present the FTC's principle of '*say what you do, do what you say*.'

• If the organization has limited resources, the implementation will depend on a strategic plan created as a result of the assessment/remediation stage. The following two steps may help to a better resources distribution:

- Educate people within the organization, they can be the eyes and ears. This can help privacy management, or Chief Privacy Officer, to

be closer to the risks or malfunctioning of the privacy program.

- Identify the biggest risks of the organization. One way could be determining which are the top products of interest, and work around them.

● Schedule remediation after complying with proper audits over business units actual practices. Afterwards, address variances from privacy policies and take the necessary measures to remediate the practices.

4. Internal PbD guidelines/Checklists/Training

● Internal guidelines based on the seven foundational principles of privacy by design, and actual business unites practices should be drafted.

● Have checklists based on the guidelines. Checklists will help to establish a process for the review of the guidelines compliance.

● In order to develop proper guidelines that will require the involvement of legal and product developers, the organization should take into consideration the internal data lifecycle. This comes relevant whenever it is necessary to design product and service features. What follows are suggestions for each data lifecycle stage in order to shape the corresponding guideline that will integrate the privacy principles and the purpose of the product developed by the company, while creating privacy by default:

✔ Collection:

♦ Determine the data and purpose specification: Know what personal data are you collecting, and how and why are you collecting it.

♦ Establish the notice and choice mechanism (design feature). Determine which data will be subject to opt-in or opt-out feature.

♦ The guidelines should be clear as to what is the use that the business is authorized to perform from the information collected. There might be the assumption that the information is available for everyone to use, when indeed this might be restricted depending on the business unit and the initial purpose and specification, for example.

♦ Data minimization: It is advisable to collect only as much personal data as is reasonably necessary to fulfill the business purpose. This comes relevant to protect the information from unauthorized access and to limit the linkability of data to personal identifiers. Minimization has been described as one of the techniques to limit linkability. Minimization may include "not recording IP addresses and/or not enabling User ID cookies, or using a third party proxy server to strip out an IP address; and a variety of techniques that protect, shield and minimize location data, from which identity is readily inferred".[85] This technique will reflect privacy as a task

85 *See* Rubinstein, Good, *supra* note 6, at 1357.

not only for lawyers, but also for product developers.

♦ Determine beforehand if the collection of sensitive data is allowed, or if not how the feature should be addressed in the product. This should be clear in the privacy policy.

✓ Use:

♦ Inform users how their data will be used. Keep the process transparent, and user centric.

♦ Consider ways to give users control over particular uses, especially those tended for marketing purposes. Specific features should be designed, preferably of an opt-in nature.

♦ User control features should be prominent, easy to understand and easy to use. Privacy by default intends to be user friendly at all times.

✓ Share:

♦ Whenever personal data is shared with service providers and/or business partners, it is relevant to understand how those entities manage data. Special review should be performed over their practices. In the EU, there are different roles and obligations depending on the participation during the data processing. Roles such as the controller and the processor have different duties, and it is important to know that the organization trusts the information collected to a processor that has the capability to keep it safe, and comply with legal and contractual obligations.

♦ Some relevant questions can be what data they will receive, how will they use the data, will the data be shared, how will it be protected.

♦ Including special contractual provisions and technical features, that may help to govern the practices of service providers and business partners with whom the sharing takes place.

✓ Store:

♦ The product developer should consider whether or not it would be possible to design a mechanism that would facilitate user control and/or access to the data.

♦ The organization should employ reasonable physical, technical, and administrative safeguards to protect the data.

✓ Delete:

♦ Clarify the policy by which the company will implement reasonable data retention and data disposal.

♦ Design features that will allow developers to delete or anonymize data when it is no longer needed or required.

♦ Organizations should thoroughly consider whether or not to delete information. Reducing the volume lowers the risk of possible data breaches.

5. Accountability tools

• Acknowledge the organization's responsibilities and duties towards data.

• How the accountability tools will have to be shaped depends upon for which sectors the product or services are directed. Controlling, monitoring and assessing will vary depending of the sector. The companies' behavior will differ if the accountability is examined from the web, cloud, mobile or advertising sectors, to cite a few examples.

• The guidelines should clearly state the organizations' duties towards a product or service that fits the determined sector.

III. CONCLUSION

A real inclusion of privacy by design will have a collateral effect. When the time comes, the drafting of the privacy policy will be an easier and more transparent process. The knowledge an organization will have of its own privacy practices and how those practices are embedded from the conceptualization stage of the products and services will help fulfill the FTC's guideline "*say what you do, do what you say*." A company that is not fully aware of its privacy by design program, and therefore does not understand how unique that program is to each organization, will most likely assume the unnecessary risk of unfair and deceitful conduct. Such company will also suffer from a lack of knowledge of consumers' expectations, which in the end will only damage the competitiveness of the organization's products and services.

Privacy by default is a good business decision. Companies should move towards a market where the privacy interests of consumers are satisfied by implementing a structured privacy by design program. Such a program will increasingly become a selling point for consumers, as reputation of the company continues to improve in a directly proportional manner.

References

A chronology of the NSA surveillance scandal, Dw.De, http://www.dw.de/a-chronology-of-the-nsa-surveillance-scandal/a-17197740

Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser, Ftc.Gov, http://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented

A message from CEO Gregg Steinhafel about Target's payment card issues, Corporate.Target.Com, https://corporate.target.com/discover/article/Important-Notice-Unauthorized-access-to-payment-ca

Acquisti, Alessandro; Friedman, Allan; and Telang, Rahul, *Is There a Cost to Privacy Breaches? An Event Study (2006). ICIS 2006 Proceedings.* Paper 94, *available at* http://aisel.aisnet.org/icis2006/94

Ira S. Rubinstein; Good, Nathaniel, *Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents,* 28 Berkeley Tech. L.J. 1333, 1336 n.7 (2013)

Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, (2011), http://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples.pdf

Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for businesses and policy makers* (2012), http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf [hereinafter FTC 2012 Report]

Julia Angwin, *How I Quit Google*, Time, http://time.com/9210/how-i-quit-google/

DuckDuckGo, https://duckduckgo.com/privacy#s1

StartPage, https://startpage.com/eng/privacy-policy.html

Ann Cavoukian, *Privacy by Design in Law, Policy and Practice: A White Paper for Regulators, Decision-makers and Policy-makers*, (2011), http://www.ipc.on.ca/images/Resources/pbd-law-policy.pdf

Cecilia Kang, *Google Announces Privacy Changes Across Products; Users Can't Opt Out*, Washington Post. (Jan. 24, 2012), http://www.washingtonpost.com/business/economy/google-tracks-consumers-across-products-users-cant-opt-out/2012/01/24/gIQArgJHOQ_story.html

TRUSTe, TRUSTe 2014 US Consumer Confidence Privacy Report Consumer Opinion and Business Impact (2014), http://info.truste.com/lp/truste/Web-Resource-HarrisConsumerResearchUSReportQ12014_LP.html

pwc, 10Minutes on Data Privacy: Build Consumer Trust Through Data Privacy (February 2014), http://www.pwc.com/en_US/us/10minutes/assets/pwc-data-privacy.pdf

Ann Cavoukian, The Privacy Payoff: How Building Privacy Into Your Communications Will Give You A Sustainable Competitive Advantage, Address Before the International Association of Business Communicators International Conference 2008, New York City, New York (June 24, 2008), *available at* http://www.ipc.on.ca/images/Resources/pbd-law-policy.pdf

Kirsten Gollatz, *App Development: Is 'Privacy by Design' the New Standard*, Internet Policy Review. (Mar. 28, 2013), http://policyreview.info/articles/news/app-development-'privacy-design-new-standard/117

GSM, Mobile and Privacy: Privacy Guidelines for Mobile Application Development (February 2014), http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/gsmaprivacydesignguidelinesformobileapplicationdevelopmentv1.pdf

Fed. Trade Comm'n, *Marketing Your Mobile App: Get It Right From The Start* (April 2013), http://business.ftc.gov/documents/bus81-marketing-your-mobile-app

Robert Gellman, *Fair Information Practices: A Basic History*, (March 18, 2011), http://bobgellman.com/rg-docs/rg-FIPShistory.pdf

Paul M. Schwartz; Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information,* 86 N.Y.U. L.Q. Rev. 1814 (2011), http://scholarship.law.berkeley.edu/facpubs/1638

EPIC, *The Code of Fair Information Practices,* http://epic.org/privacy/consumer/code_fair_info.html

OECD, *1980 Guidelines on the Protection of Privacy and Transborder Flows,* available at http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#part3

Council of Europe, *http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm*

In the matter of Google Inc. US FTC File No. 102 3136, (complaint filed March 30, 2011); *see also United States v. Google, Inc.*, No. CV 12-04177 SI (N.D. Cal. Nov. 16, 2012); *see also In the Matter of Facebook, Inc.*, FTC File No. 092 3184 (complaint filed Nov. 29, 2011).

OECD, *2013 OECD Privacy Guidelines,* http://www.oecd.org/sti/ieconomy/privacy.htm

Center for Democracy & Technology, *The Role of Privacy by Design in Protecting Consumer Privacy,* https://www.cdt.org/policy/role-privacy-design-protecting-consumer-privacy

Department of Commerce, Internet Policy Task Force, *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework,* (2010), http://www.commerce.gov/sites/default/files/documents/2010/december/iptf-privacy-green-paper.pdf

Emil Protalinski, *Survey: Facebook, Google privacy policies are incomprehensible*, ZDNet, http://www.zdnet.com/blog/facebook/survey-facebook-google-privacy-policies-are-incomprehensible/12420

International Association of Privacy Professionals "IAPP Global Privacy Summit", March 5-7, 2014, Washington DC, *Workshop: A Step-by-Step Guide to Integrating PbD at Your Organization.*