USF | Muma Case Review
A publication of the Muma College of Business | University of South Florida

Volume 3 Number 11 31 DEC 2018

ONOCHIE FAN-OSUALA

A NOTE ON PRIVACY[1]

In October 2010, following a Wall Street Journal (WSJ) investigation, Facebook admitted to a privacy breach where some of its most popular applications including Farmville and Texas Hold 'em shared personally identifiable information of users with advertisers (Steel and Fowler, 2010). Some of the affected users had used Facebook's most stringent privacy settings on their account, yet personal information of users was shared with advertisers including names and names of friends. Facebook settled charges regarding some of its privacy violations with the Federal Trade Commission (FTC) which includes having periodic privacy audits for 20 years (Pepitone, 2011). In 2009, a web developer named Jason Fortuny was made to pay almost $75,000 in damages following an infamous "Craiglists Experiment" that led to the exposure of names, photos, emails and responses of individuals who responded to a fake sex baiting advertisement placed by him on Craigslist (Marsan, 2012). Similarly, Google was fined $142,000 by the French government following privacy concerns related to the Google Street View – a technology in Google Maps that provides panoramic views of a street or location. Google Street View at that time showed individuals engaged in such activities as picking up prostitutes, leaving strip clubs, or entering adult bookstores. Since then, Google has included features that allow for the blurring of images such as faces and licenses on their Street View. More recently, Nomi Corporation, a company that provides information on consumers' physical shopping behavior by tracking their cell phones, settled with the FTC for violating its own privacy policy by failing to provide consumers with an opt-out option when it had pledged to do so in its privacy policy (Vinton, 2015). The above cases point out that privacy remains a major issue, more so, in the digital age and that its violation – by companies or individuals – has some social and economic implications. According to a Gartner report (Casper, 2011), privacy protection is important for organizations that want to gain and maintain the trust of its consumers and employees. In this note, I present a brief description of privacy and privacy concerns in the online context.

Definition of Privacy

A broad and general definition of privacy is still very much lacking often as a result of its varied use, value, and scope across multiple domains and cultures (Stanford, 2013). For instance the concept of privacy varies across different cultures around the world. Even in a one culture environment, what is considered an invasion of privacy in the big cities, may not be considered an invasion of privacy in the small towns. For instance, while it might be okay for people to know and pry into one another's personal affairs in a small town, it may be considered an invasion of privacy in the big city. It has also been argued that privacy is heterogeneous, fluid and multidimensional (Friedewald et al, 2013). Despite the lack of a generalizable definition, privacy can loosely be described as encompassing: "freedom of thought, control over one's body, freedom of surveillance, solitude in one's home, control over information about oneself,

Editor: T. Grandon Gill

protection of one's reputation, and protection from searches and interrogation" (Solove, 2002). It is important to note from this description that privacy involves more than information privacy or the highly restrictive data protection concerns.

Types of Privacy

Clarke (1997) used a human-centered approach to classify privacy into 4 major categories: privacy of the person; privacy of personal behavior, privacy of personal data; and privacy of personal communication.

- ***Privacy of the person:*** often referred to as bodily privacy is related to the integrity of a person's body. It include protections against physical intrusions, medical treatment, and compulsory provision of samples of body fluids and tissues, and submission to biometric measurement (Friedewald et al, 2013).
- ***Privacy of personal behavior*****:** is related to the protection against disclosure of such sensitive personal matters as religious practices, sexual practices/orientation, and political activities or leanings.
- ***Privacy of personal communication****:* relates to restrictions on monitoring of individual communications either on phone, email, virtual communications, or face-to-face.
- ***Privacy of personal data****:* this relates to protection of data and remains a major area of concern on digital privacy.

Friedewald and colleagues (2013) extended Clarke's categories of privacy by including: privacy of thoughts and feelings; privacy of location and space; and privacy of association.

- ***Privacy of location and space*** implies that individuals have the right to their private spaces (home, car and offices) and the freedom to move about in public and semi-public spaces without being identified, tracked or monitored.
- ***Privacy of thoughts and feelings*** implies that individuals are right to think whatever they like and have the freedom not to share their thoughts and feelings or have it revealed.
- ***Privacy of association*** implies that individuals have the freedom to associate with whomever or whatever group they wish without being monitored.

Kaspar (2005) provides an invasion-based typology on privacy. These she listed as *extraction-based* privacy invasion, *observation-based* privacy invasion, and *intrusion-based* privacy invasion. The extraction-based invasion involves a calculated drive at getting something or information from an individual. Observation-based privacy invasion involves actively monitoring or tracking an individual, while intrusion-based invasion concern uninvited presence or interference in an individual's life.

1. Due to the growth in information communication technology (ICT), privacy of personal communication and privacy of personal data have become intertwined and now both commonly referred to as ***information privacy***.

Information Privacy and Information Communication Technology

Though privacy concerns have been articulated since the beginning of large scale computing (e.g David and Fano, 1965), the issues and threats of privacy have never been more pronounced than in this age of high connectedness, explosion of data, and advances in ICT. A Forrester research (Ferrara et al, 2014)

reports privacy remains one of the most salient issues in information security especially with the growth of the internet and internet related technologies.

Online Privacy

Internet or online privacy focuses on the rights of individual over their personal data with respect to its collection and dissemination online. This includes the data storage, repurposing, provisioning to third parties, and display on the internet. Online privacy continues to pose a challenge due to cultural and political differences. For instance, while the European Union (EU) sees protection of personal data as a human right, the United States considers it in terms of consumer protection. Figure 1 shows a heat map of regulations governing privacy and data protection by countries. The complicated nature of online privacy has also raised a growing debate among policy makers and security experts (CNN, 2013).

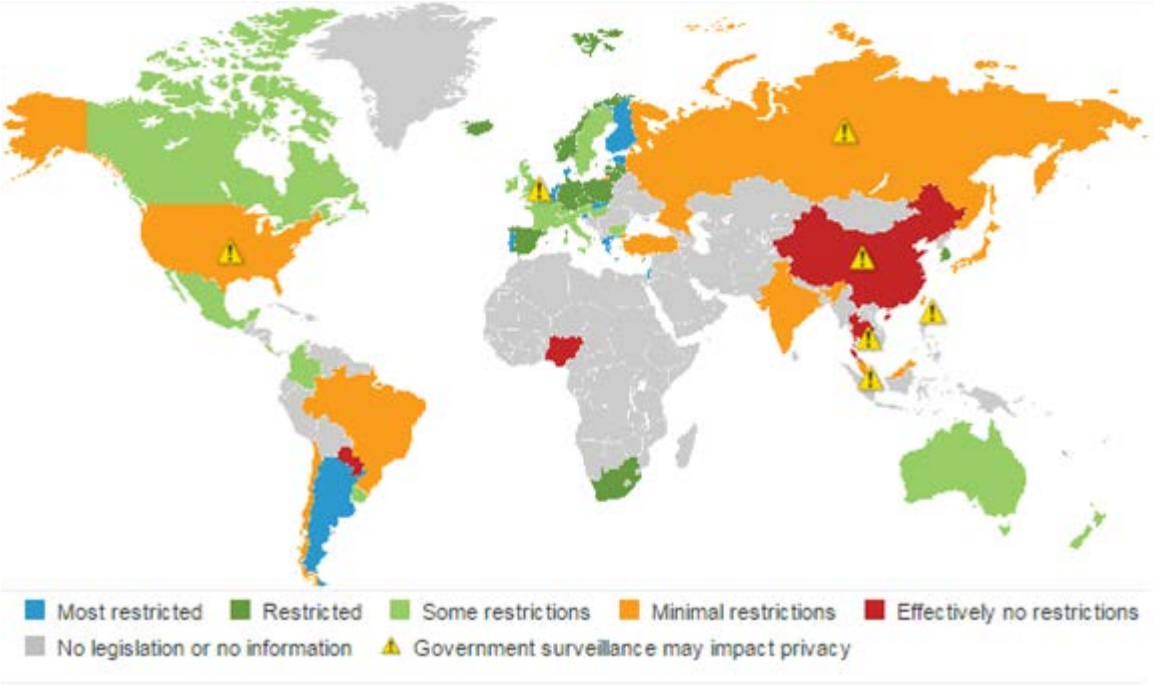

Figure 1. Heat map of privacy and data protection regulations by countries. (Adapted form http://heatmap.forrestertools.com/)

Online privacy related information can be broadly divided into two: personally identifiable information (PII) and non-personally identifiable information (non-PII).

PII refers to any information on an individual that can be used to trace or distinguish the individual's identity or information that is linked or linkable to such individual. Most PIIs are often categorized in many organizations' data protection policy as belonging to the very sensitive and restricted data category and as such require maximum protection with restricted access. Usually, data belonging to this category are often encrypted when stored, used in portable devices, removed from a secure location, or electronically transmitted. It includes such information as social security number, date and place of birth, passport number, biometric records, medical, educational, financial, and employment information.

Non-PII information include such information as a website visitor's online behavior which can be used to deduce more intrusive insights about an individual such as race, personality, sexual orientation, political and religious views. Most of the debate on online privacy is centered on this class of online privacy related information since such activities as government surveillance programs, and consumer online behavioral tracking belong to this category and there are reports that some of the tracking activities are done without the individual's consent (Traders, 2011).

Threats to Online Privacy

With more life related activities and tasks moving online, from online shopping and social networking to storing content in the cloud, individuals are generating more data which is rich in information. These information often tells more about an individual than the individual may realize posing threats to privacy. Similarly, the emergence of new technologies and evolving regulations on how data on individuals' online-life is treated also contributes in posing threats to online privacy. The following are the major threats of online privacy:

Proliferation of Cookies

Cookies are software agents that are used by online sites to track user browsing habits and personal data. According to a PCworld article (Riofrio, 2013), the number of cookies an individual gets from browsing a website in recent years have increased tremendously. Most of the cookies come from third parties linked with the website like ad servers, data brokers, and trackers. A major issue with cookies is that often times, the users have no idea of what is going on. For instance, they may have no knowledge of cookies, how much data these cookies are collecting, and how long these cookies sit on their machines.

Data in the cloud

While most people are happy to use cloud services and store data in the cloud, a key issue remains that data in the cloud is not subject to the same protections as data in a personal hard drive (Nguyen, 2013). In fact, most individuals who have data in the cloud do not know where (the location) their data is stored. And with major cloud storage providers having experienced some form of breach in the past (Lee, 2013; Reuters, 2016) and different countries having different data protection policies, the cloud remains a major threat to privacy.

Geolocation Tracking

Cellphones' GPS functionality provide easy location tracking and have turned cellphones into personal tracking devices. While law enforcement agencies can subpoena location tracking information for criminal purposes, employer-owned devices can now be used for employee monitoring. It has been noted that it is very difficult for users to prevent their geolocation data from being gathered (Riofrio, 2013).

Online Photo Tagging

Online photo posting and tagging is helping build large facial recognition databases most of which are in the hands of internet giants like Facebook and Google. Some of these photos are not just embarrassing, but are potentially incriminating to the individuals tagged. As of now, available facial recognition and tagging programs do not provide any opportunity for individuals to opt out before the data is collected.

While the internet giants maintain that the data is safe, there are no regulations on the sale of these data to third parties and how the third-parties use such data.

Legally Mandated Scanning

With the high spate of cybercrimes and acts of terrorism, countries have initiated online surveillance programs that scan individual online activities for revelatory signs of cybercrime or terrorism. Such programs include PRISM and MUSCULAR in the United States. While the argument for such surveillance practices remains that it is used in fighting crime and that data is scanned in aggregate (in order not to pinpoint individuals), the fact remains that individual information and online activities are monitored without the individual knowing or consenting to such surveillance.

Cost of Online Privacy

Privacy protection comes at a cost to both consumers and businesses. For instance businesses that deal with consumers pay the price when consumers react to a lack of privacy or a breach in their personal data. Similarly, consumers who are privacy sensitive may have to pay higher prices to ensure their privacy.

Cost to Businesses

Loss of Sales: the FTC estimates lost online sales due to privacy concerns to be as much as $18 billion (Gellman, 2002). There is evidence showing that consumers are dissuaded from buying when they perceive that an online business does not guarantee privacy and recent hacks on sites considered private.

Lost international opportunities: for businesses that do not have adequate privacy protection capabilities, they can lose opportunities in countries with very strict privacy laws. For instance, some European Union (EU) member countries restrict the export of personal data to countries that have insufficient privacy protections for data.

Legal costs: businesses may become subject to various private and public litigations as a result of their privacy policies and practices. Litigations can be expensive and may have both economic and social costs (e.g. brand erosion).

Cost to Consumers

Cost of privacy protection: it is estimated that a privacy sensitive family spends about $280 a year to guarantee privacy (Gellman, 2002) often against identity theft, telemarketing avoidance, internet privacy, and junk mail. Similarly, some online service providers like email service providers require consumers to pay if they do not want to receive junk mails or advertisements. This shows that for consumers, privacy has a dollar cost.

Cost of privacy breach or violation: consumers may incur cost due to privacy violations like higher credits cost in the case of identity theft, losses as a result fraud targeted at them using their private information, and embarrassment or loss of reputation from exposed data or online behavior (e.g. the Ashley Madison data breach).

References

- Casper, C. 2011. “Privacy Key Initiative Overview”, http://www.gartner.com/document/code/212289?ref=grbody&refval=2432315&latest=true
- CNN. 2013. “The Great Privacy Debate”. Retrieved from http://www.cnn.com/2013/06/06/opinion/roundup-privacy-opinion/
- David E. E. and Fano R. M. (1965). "Some Thoughts about the Social Implications of Accessible Computing. Proceedings 1965 Fall Joint Computer Conference
- Friedewald, M., Finn, R. and Wright, D. 2013. “Seven types of Privacy”, https://works.bepress.com/cgi/viewcontent.cgi?article=1070&context=michael_friedewald
- Gellman, R. 2002. “How The Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete”, https://epic.org/reports/dmfprivacy.html
- Gellman, R. 2002. “Privacy, Consumers, and Costs” Retrieved from https://epic.org/reports/dmfprivacy.html
- Kaspar, Debbie V.S. “The Evolution (or Devolution) of Privacy.” Sociological Forum 20 (2005): 69-92.
- Lee, A. 2013. “So Dropbox Can Be Hacked—What Else Is New?” Retrieved from http://readwrite.com/2013/08/28/dropbox-hacked-reverse-engineered-client#awesm=~oolQS7mbWMs95t
- Marsan, C. D. 2012. “15 Worst Internet Privacy Scandals of all Time”, http://www.networkworld.com/article/2185187/security/15-worst-internet-privacy-scandals-of-all-time.html
- Nguyen, P. 2013. “The 6 Biggest Online Privacy Threats You Should be Concerned With” Retrieved from http://blog.hotspotshield.com/2013/12/19/the-6-biggest-online-privacy-threats/
- Pepitone, J. 2011. “Facebook settles FTC charges over 2009 privacy breaches” Retrieved from http://money.cnn.com/2011/11/29/technology/facebook_settlement/index.htm
- Reuters. 2016. “Hundreds of Millions of Email Accounts Hacked and Traded Online, Says Expert”. Retrieved from http://www.nbcnews.com/tech/security/hundreds-millions-email-accounts-hacked-traded-online-says-expert-n568491
- Riofrio, M. 2013. “The 5 biggest online privacy threats of 2013” Retrieved from http://www.pcworld.com/article/2031908/the-5-biggest-online-privacy-threats-of-2013.html
- Roger Clarke, “Introduction to Dataveillance and Information Privacy, and Definitions of Terms”, Xamax Consultancy, Aug 1997. http://www.rogerclarke.com/DV/Intro.html
- Solove, D.J. 2002. "Conceptualizing Privacy," California Law Review, pp. 1087-1155.
- Stanford. 2013. “Privacy”. Retrieved from https://plato.stanford.edu/entries/privacy/
- Steel, E. and Fowler, G. A. 2010. “Facebook in Privacy Breach”, http://www.wsj.com/articles/SB10001424052702304772804575558484075236968
- Traders, A. 2011. “The Ethical Issues with 3rd Party Behavioral Tracking”. Retrieved from https://adexchanger.com/the-debate/3rd-party-behavioral-tracking/
- Vinton, K. 2015. “FTC Pursues Tech Company It Claims Violated Privacy Policy While Tracking 9 Million Phones”. Retrieved from http://www.forbes.com/sites/katevinton/2015/04/23/nomi-agrees-to-settle-with-ftc-after-allegedly-violating-its-privacy-policy-while-tracking-9-million-mobile-devices/#72bd2e26c38c

Acknowledgements

Development of this note is based upon work supported by the *National Science Foundation* under Grant No. 1418711.

Biography

Onochie Fan-Osuala is a PhD Candidate in information systems (IS) at the Muma College of Business, University of South Florida. He is interested in using analytics and experimental designs to solve problems bothering on the IS-operations, IS-marketing and IS-entrepreneurship interfaces. His work mostly explore these problems in online platforms and marketplaces.