Syracuse University

SURFACE

School of Information Studies - Post-doc and Student Scholarship

School of Information Studies (iSchool)

2018

Reading Reflection Privacy and Security

Paul Sujith Rayi
Syracuse University, parayi@syr.edu

Follow this and additional works at: https://surface.syr.edu/ischoolstudents

 Part of the Privacy Law Commons, Science and Technology Policy Commons, Science and Technology Studies Commons, and the Securities Law Commons

Recommended Citation

Rayi, Paul Sujith, "Reading Reflection Privacy and Security" (2018). *School of Information Studies - Post-doc and Student Scholarship*. 9.
https://surface.syr.edu/ischoolstudents/9

This Other is brought to you for free and open access by the School of Information Studies (iSchool) at SURFACE. It has been accepted for inclusion in School of Information Studies - Post-doc and Student Scholarship by an authorized administrator of SURFACE. For more information, please contact surface@syr.edu.

Reading Reflection Privacy and Security

Privacy is a very important factor to be considered no matter what you do in life. Whether you are a doctor, professor, engineer, teacher, worker, it does not matter when it comes to protecting the privacy of your data. We generate tons of data everyday through our actions such as texting someone via phone, calling and speaking to anyone through phone, sending and receiving emails, making purchases at the grocery store, and paying our credit card bills etc. But we don't really think about whether our data being collected through internet and phone is sold to someone else, or recorded somewhere else without our knowledge etc. Part of the reason behind this is that we are so busy and engrossed in our individual lives, that we don't care about thinking about these things. And then something suddenly happens, and we hear in the news that a company like Facebook has sold our information to third parties for their data analysis, we get angry and we don't know what to do. Many cases such as these have happened, and many law suits have been filed. What about the end results of these activities, are we getting protected by new laws that govern how an organization can use our data? Well not really, and nothing has moved forward so far as the laws are concerned. There are government regulations in place which protect people's privacy as to the data being collected, but they are very complex and easy for companies to circumvent and get the profits they want by leveraging our data in an unethical way. So, who is to blame? The companies or the Government or are we fools for them to use our data like this because we are not concerned, and as long as we get what we need in life, we are okay with it. This is a very intriguing question as it involves a lot of dimensional overlapping of various laws and activities of our lives.

Security is like the other side of the same coin if we have privacy on one side. Especially after various terrorist attacks which happened in many countries and which are continuing to happen in many countries, governments do not want to take any chances when it comes to national security. Governments have sometimes gone to an extreme level to conduct surveillance activities on many citizens without probable cause or evidence. Looking at the mass shootings happening very frequently especially in the United States and nothing is being done by the government to curb it, I sometimes wonder that the government is giving very high priority towards external threat which is good, but at the same time it is completely neglecting the turmoil happening due to domestic gun violence in the country. Thanks to free DNA databases where people deposit their DNA data, law enforcement officers are able to catch criminals such as rapists and murderers who have committed the crimes 30 years ago, through family genealogy trees. This indicates to us that when new technology is invented, we can adopt it to enhance various security measures. Privacy and security need to be balanced out if we want to live a safe life and enjoy our liberties. And it is not an easy task for anyone to figure out how we can do that. The potentially intensifying antagonism between privacy and security warrants a vigorous debate (Dinev, Hart, & Mullen, 2008). Many people can have different views about privacy and security. Some say that if there is nothing to hide for a person, then there is no need to be private about what one does in life. Some take privacy very seriously and say that government has no right to put a tab on me and record all the phone calls that I make, or the google searches that I do. Sometimes a lot depends on the cultural factors of how one has been bought up and the community in which he/she lives. People from China know that the government collects all their data and they are not mindful or concerned about it because they are bought up in an atmosphere where the government has the final word in every issue and protests are not allowed to happen.

Whereas people from the United States, who are bought up in an individualistic atmosphere are very much concerned about their privacy and do not want government or anyone to breach their personal space and have the right to protest and challenge the government on various issues.

After the revelation of Facebook selling data to a British company which marketed ads to target people and influence them in the voting process, everyone started looking at companies with suspicion. Mr. Mark Zuckerberg the CEO of Facebook was called on to the senate floor to testify before members of congress. But, can events such as these bring any change, I hardly doubt. It is often difficult to change government rules, even when there is consensus in the agency and policy community that such change is appropriate (Daley, Irving, 1997). One of the reasons behind this is complex bureaucracy of government institutions. Trustworthiness on companies and the way they use data has not deteriorated the business e-commerce companies are generating. The growth of business to consumer electronic commerce seems to be non-stoppable (Belanger, Hiller, & Smith, 2002). With this light of things, I propose self-regulation to be an ideal solution to protecting privacy of customers. One reason for this being, we have seen government regulation efforts failing time and time again. The inflexibility of government rules suggests that rules passed today may create substantial compliance costs, because rules will not adapt smoothly enough to changing market and technical realities (Daley, Irving, 1997). Hence, it is better for companies to come together in an industry and form an association or body that regulates how they handle customer data. Regular communication of policies created by this body to customers is essential to build customer trust and loyalty. Customers must be contacted, and surveys must be taken before framing any policy as this takes into consideration the customer's point of view before making decisions. This enhances the company's goodwill in the eyes of the customer. Members of industry may also find it in their collective self-interest to promulgate and enforce regulations (Daley, Irving, 1997).

Right to be Forgotten act has revolutionized how people view privacy in Europe. A man can google search his name and look at his information on the net which is available for public view. If he finds out something which is no longer relevant or something which he deleted but it still appears on google search, he can order the source to delete that particular content and they have to comply according to the Right to be Forgotten Act. This act is applicable all over the European Union's jurisdiction. This Act came into existence when a person was denied housing based on something which he did long time ago in his life. The belief that only those considered to have perfect records can avoid discrimination is undesirable and increasingly untenable (Garcia-Murillo & MacInnes, 2018). Laws such as these will benefit the society but, we have to be careful when allowing people to delete whatever content they want about themselves. Also, allowing people to delete personal information fosters the idea, however accurate, that humans are vengeful by nature, and thus we need to protect ourselves from harm (Garcia-Murillo & MacInnes, 2018). Serious crimes such as murder and rape cannot be forgotten and must be held in the record of that person forever. As we go through lives, we understand the flaws that we ourselves have as human beings and must learn to forgive people for small mistakes they have done in the past and allow them to smoothly transition into normal societal life. We must accept the weaknesses of others, as well as the setbacks that occur in the real world, allowing for a culture of trust to emerge, a culture that relies on empathy and shows humility when judging others (Garcia-Murillo & MacInnes, 2018). In the United States we have the largest incarcerated population. Time and time again we have seen African-American men being subject to police brutality and people of color in general being discriminated against. Laws such as Right to be Forgotten can help imprisoned people for minor crimes get a second chance in life and help

them live a better life. This increases public trust in the system and governing bodies. There is evidence of positive changes that have occurred in society when previous anti-discrimination laws have been implemented (Garcia-Murillo & MacInnes, 2018).

Government surveillance has become one of the biggest concerns to be dealt with in the 21st century. Common people are not aware of what information is being collected on them by the government. Recent government initiatives to improve security following September 11th suggest that the information asymmetry between consumers and web retailers and third parties, including government agencies has increased (Dinev, Hart, & Mullen, 2008). After the Edward Snowden revelations, we can say that some aspects of how government collects information about its citizens has come out to the public. People have become more and more cautious about how they use internet and mobile applications. The perception that information-gathering and analysis may be occurring could result in behavior modification regarding Internet use (Dinev, Hart, & Mullen, 2008). Time and again we have seen terrorist attacks happening all around the world, this also brought fear in the minds of people, so they became more obliged to agree with some government surveillance if it is for national security. The statistically significant relationship between perceived need for government surveillance and willingness to disclose personal information suggests that users perceive security initiatives as important and tolerable (Dinev, Hart, & Mullen, 2008). In the Patriot Act the government was very nebulous as to what information is being collected and whose information is being collected. Government tried to surveil all the citizens data, irrespective of he/she being suspected of terrorism or not. People when they got to know about this, opposed it vehemently. They however overwhelmingly opposed the same kind of surveillance if it was aimed at ordinary Americans (Dinev, Hart, & Mullen, 2008).

There should be a balance between protection of privacy and data collection for security. It will be a huge task for governments and people to figure out how they do this. One possible solution that I propose is for government officials to sit down with interested parties and frame guidelines about the policies to be developed with regards to privacy and security. The interested parties must include companies, common people, not-for-profit organizations and other important agencies.

References

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: The role of privacy, security, and site attributes. *The Journal of Strategic Information Systems, 11*(3-4), 245-270.

Dinev, T., Hart, P., & Mullen, M. R. (2008). *Internet privacy concerns and beliefs about government surveillance – an empirical investigation*doi://doi.org/10.1016/j.jsis.2007.09.002

Garcia-Murillo, M., & MacInnes, I. (2018). *Così fan tutte: A better approach than the right to be forgotten* doi://doi-org.libezproxy2.syr.edu/10.1016/j.telpol.2017.12.003

Daley, M., Irving, L. (1997).

U.S. Department of Commerce: Prepared by National Telecommunications and Information Administration. Washington, D.C.