Problems regarding the Invasion of Privacy on the Internet in Japan

Makoto Sakai, Bunkyo University, Japan

The European Conference on Media & Mass Communication 2014
Official Conference Proceedings

Abstract
According to Ulrich Beck, in a society steeped in risks and uncertainty, the existing political system becomes the malfunction, and technology is tinged with political characteristics. Consequently, a new type of democracy that controls risks and uncertainty through technological means becomes needed. This tendency is remarkable in the present information society. This thesis will show three necessary regulations in the present information society in Japan based on sociological studies, after dividing examples of invasion of privacy on the Web into the following three types. Type 1 is related to the problem where social networking service (SNS) platform companies overlook the invasion of privacy. Type 2 refers to the problem that legal regulations cannot keep up with freedom of speech. Type 3 includes the problem of low information literacy of the users. Recently, these problems are increasing in Japan. Personal information related with crime, for both offenders and victims, are shared on SNS, through which other users may disseminate and copy such information to other Web sites. To prevent such invasion of privacy, new human rights should be established, such as the right to be forgotten on the web, and legal regulations should be enacted to cover SNS platform companies.

iafor
The International Academic Forum
www.iafor.org

Introduction

According to Ulrich Beck, in a society steeped in risks and uncertainty, the existing political system can malfunction and technology can become tinged with political characteristics. Information technology is politically neutral in general and tends to be thought of as not involving bias, but neutral opinions do not exist regarding the personalization of search information on the web.

Cass R. Sunstein states that there is a tendency for information on the web to go to extremes: people are now sensing the risk of going beyond their familiar information environment. Yet, there is also a tendency to shut down any information that criticizes these familiar information environments. In this way, not only the real world, but also the public sphere, narrows within the web community, causing a necessity to conserve the more intimate sphere of family and friends. For example, Eli Pariser points out that information on the web is filtered according to individuals' interests, so the fact that people are not as careful enhances social risks.

Since vast amounts of information are now appearing on the web, the demand for filtered information is increasing and people are accepting personalized information by choice. By organizing information through filters such as "recommended by a friend" and "enriched preference," social networking services (SNSs) such as Facebook have become popular. It can be said that communication via SNSs promotes the "You Loop," meaning that it involves recommended information based on the analysis of historical data on the user and the personalization of his/her web environment. However, we should remember that these information environments are obtained in order to provide vast amounts of personal information free of charge; thus, there is the potential for exposure to social risks, including invasion of privacy, when using SNSs such as Facebook.

Facebook originated as Facemash.com, a ranking system of the photos of female students at Harvard University. Mark Zuckerberg, the founder of Facebook, created a system that showed users two such photos—gathered through illegal access to Harvard computer servers—and asked the users to choose which female student was more beautiful. Zuckerberg then analyzed the data to create a ranking system of the appearance of Harvard's female students. Zuckerberg's blog even discussed a plan to allow users to vote by mixing photos of female students and animals. Thus, if we keep Facebook's origins in mind, it is easy to see that the company has never dealt decently with personal information. This now leaves the personal data of one billion people at risk.

One such risk occurred in mid-August of 2012. A female university student from Tokyo, who had traveled there on an internship to teach Japanese, was raped and killed by a group of men with whom she had shared a taxi in Bucharest, Romania. In Japan today, it is important for college students to participate in internships abroad, so this incident was widely reported and attracted people's attention. However, the reputational damage of this crime has not been a problem at all. After the incident, personal information that the victim had published on Twitter and Facebook was copied over and over on the web, and spread alongside writing that slandered the victim. Some detailed information, including photos of the victim, her name, the name of her university, her affiliation, and the names and photographs of her friends were

leaked from Facebook. Some of this information has still not been erased from the web, even though time has passed since the incident.

Problems such as this are increasing in Japan. Personal information related to crimes, regarding both offenders and victims, are shared on SNSs, through which other users may copy and disseminate such information to other websites. Even though Japan has delayed legislation on the protection of personal information, as have other developing countries, detailed personal information should not be allowed to be exposed such that honor is damaged. Yet, no one receives punishment for such action, creating a state of lawlessness. In order to prevent invasions of privacy like this one, not only is a legal responsibility imposed on the person who defames a victim, but Facebook, which perpetuates the risk of personal information outflow, should also be held responsible. A new type of regulation that controls risks and uncertainty and prevents invasion of privacy through technological means is needed on the web.

This thesis will introduce three suggested regulations for Japan's present information society based on prior sociological studies. It divides examples of privacy invasion on the web into three types: Type 1 relates to the problem of SNSs overlooking privacy invasion; Type 2 relates to the problem of legal regulations' inability to keep up with freedom of speech; and Type 3 relates to the problem of users' low information literacy. All three of these problems are currently increasing in importance in Japan.

Type 1: Privacy Invasion

WikiLeaks founder Julian Assange said in an interview with Russia Today that "Facebook in particular is the most appalling spying machine that has ever been invented." It is telling that even Assange, who has leaked sensitive information all over the world, sees Facebook's collecting of personal information as an "appalling spy machine." Yet, in recent years, Facebook has become more than a "spy machine": it has gathered not only personal data but also human data, including biological information such as face fingerprints. In China, a phenomenon called the "human flesh search" exists, in which people search for personal information, such as business addresses, names, and phone numbers, on the web. It would seem that Facebook has already become the world's largest "human flesh search" company.

According to the Associated Press, the number of Facebook users per month reached 1.28 billion in March of 2014. Even when false and overlap accounts—which are estimated at slightly less than 10% of the total—are taken into consideration, Facebook has about one billion active users—a figure close to that of the population of China and India. Moreover, Facebook is unlike other companies, such as Twitter, in that it requires users to create accounts using their real names; thus, the accuracy of the personal information found on Facebook is much higher than that of any other SNS. Facebook collects 70 types of personal information data, including credit card numbers, dates of birth, education history, facial recognition data, hometowns, last known locations, IP addresses, phone numbers, photos, political and religious views, search histories, work histories, and so on. Facebook can also analyze characteristic search words from all users' written text, thereby gathering not only the aforementioned 70 items, but also information such as sexual preference, medical history, discrimination, and evasion of the law. Thus, it is possible to analyze a variety of tendencies depending on the individual setting.

In the world of marketing, the demand for gathering such personal information is quite high. A huge company called Acxiom has already covered about 95% or more of U.S. households and retains the personal information of about 500 million people around the world. Since Facebook has already attracted many more users than Acxiom, it is not an exaggeration to say that Facebook has become the world's largest personal information company. Acxiom has the ability to earn profits by selling personal information data to private companies and government agencies. If Facebook joins this market and sells its gathered personal information, it will earn even more profits than Acxiom. It is said that the IT industry has faced many vicissitudes; therefore, companies in financial crisis will certainly be tempted to sell personal information to other companies to earn enough money to recoup losses.

Facebook has been under scrutiny by the U.S. Federal Trade Commission regarding the issue of the handling of personal information, and has been advised to discard its archive of personal data, in violation of E.U. law, by an information protection institution in Germany. In this desperate situation, Facebook has tried to regain its former glory by focusing on the enclosure of the user and the protection of further personal information. Facebook's motto was, "We're making the world more open and connected." However, the space on the web that Facebook manages is currently transforming into a "closed space" for the extraction of users' personal information. On the Facebook site, users are like livestock—given bait, enclosed within a fence, and sometimes deprived of resources. Users give up their personal data in exchange for the free use of the SNS system. Even though people join Facebook on the recommendation of their friends in order to expand their circles of friends and rekindle old friendships, personal data that appears to be visible to "friends only" could be collected and resold to third parties. It can thus be said that Facebook is quite a risky system in which to live one's private life. If they violate our privacy, should we continue to use SNS services on the web?

For these reasons, I believe that legal restrictions to anonymize personal information and to restrict the usage period of data should be required.

Type 2: Legal Regulations and Freedom of Speech

Privacy rules on the web are determined by the laws of the nations in which web servers are located, so Facebook can legally offer their services from countries that have loose privacy regulations. Of course, since SNSs are offered at no charge to the user, even though they are risky systems, there is a certain amount of freedom in their use. Yet, SNSs like Facebook have a structure in which the default settings make personal information outflow likely; thus, if users are not literate enough about those settings, it is difficult to stem the leakage of personal information. There are no problems if SNS communication is functioning smoothly, but if a communication problem occurs even once, it is possible for malicious users to expose personal information on the web. As William H. Davidow pointed out, over-connected relationships on the web incur excess positive feedback, so such relationships have extreme tendencies, such as failure leading to further failure and success to further success. Thus, if one has a problem with a friend on the web, there is a tendency for miscommunication to create further miscommunication.

SNSs often have unnecessary communication functions that sometimes enhance social risk. For example, Facebook has built a system that detects and analyzes the "face fingerprint" from the photographs that users upload. This system analyzes the human faces in each photo, and if friends' face fingerprints are found, their names are displayed near their faces. For example, if one uploads a group photo from an alumni reunion, one can see the names of all of the alumni in the photo. This makes it convenient for one to look for a friend whose name one cannot remember; however, this system also encourages over-connection among alumni who do not get along with each other. In addition, if Facebook connects friends' relationship metadata with the names on the group photo, it is possible to display their relationship status and dating history. Facebook users can choose whether their names are displayed when pictures of them are uploaded by other people; however, whether displayed or not, Facebook has still gathered and analyzed the face fingerprints of such pictures, which could pose some risks.

According to data from 2013, Facebook users upload about 350 million photos per day. Facebook therefore possesses a huge amount of face fingerprint data, and even if users stop using Facebook in the future, the company will retain this information. In June of 2012, Facebook acquired the Israeli company face.com at a value of 100 million USD. Face.com provided Facebook with the ability to analyze face fingerprints, and Facebook has been focusing on the analysis of photos and video ever since. In the future, if the secondary use of face fingerprint data on Facebook is not regulated, it is possible that personal information will be derived from photos taken on the street or video taken by surveillance cameras. When the technology associated with face fingerprinting can identify Facebook's one-billion-person information database with high accuracy, the "world's largest human flesh search system" will have reached completion. As a number of users have posted photos of their children on Facebook, we should strongly consider the risk of maintaining face fingerprints of these children into their adulthood. If Facebook were to go bankrupt, it could easily sell this personal data to a third party.

For these reasons, I believe that legal regulations should be created to limit the collection of biological information, such as face fingerprints, from videos and photos taken in public places.

Type 3: Low User Information Literacy

Of course, it is possible to reduce the risks of the outflow of personal information from SNSs if we can achieve information media literacy. It is helpful to use free services if users can change their default privacy settings in order to limit the exposure range of their personal information, and if they are careful about updating that information online. Yet, despite its privacy policy, Facebook—a private company—remains the world's largest human flesh search system, outpacing other SNSs. For example, Twitter does not collect personal information and has relatively simple operational rules. Personal data on Twitter is not necessarily tied to one's real name, so anonymity is higher than on Facebook and Twitter only promotes the secondary use of personal data that remains anonymous.

Lawrence Lessig pointed out that, even though web services are legitimate, it is necessary for IT companies to contribute the health of the democratic web

architecture. However, Facebook collects personal and biological information that is not related to the provision of their services. Facebook has been running ads based on the analysis of personal information, but they have not been open in explaining the criteria for the use of that information. Moreover, Facebook has changed its terms and conditions many times, even allowing them to be applied retroactively to past posts.

Despite these issues, I do not think that people in Japan are particularly interested in the risk of Facebook collecting their personal data. Since the "right to privacy" has not been specified in Japan's constitution, the consideration of privacy policies has weak roots there. In Japan, there is no diplomatic ability to request restrictions on global platform companies like Facebook in the U.S. Whatever Facebook's privacy policy may be, the site is hugely popular in Japan: users of Facebook now outnumber users of Mixi, which was the most popular SNS in Japan in 2011, and of Twitter, which was the most popular in 2012. It is important for Japanese people to accept the reality that Facebook has embarked on the analysis of one billion face fingerprints and has turned into the world's largest human flesh search company.

For these reasons, I believe that legal regulations should be created to distinguish between personal information that is analyzed because users have agreed with the terms and conditions and personal information that is analyzed only on condition of anonymity.

Conclusion

One private company should not be able to decide what personal information should or should not be analyzed. That should be determined by law in accordance with the social norms of individual countries. People have a right to be forgotten, thus, biological information, search histories, and comments posted on the web should have a finite usage period, and biological information and non-anonymous personal information should not be sold without users' consent. Just because Facebook provides a useful system for free, this does not give it the right to do business by using one billion people's biological and personal information unconditionally. There are many complex issues in the world that cannot be resolved merely by clicking "Like."

References

Ulrich Beck, Risk Society: Towards a New Modernity (London: SAGE, 1992).

Cass R. Sunstein, Republic.com 2.0 (Princeton, NJ: Princeton University Press, 2009).

Eli Pariser, The Filter Bubble: What The Internet Is Hiding From You (London: Penguin Press, 2011).

David Kirkpatrick, Facebook Effect: The Inside Story of the Company That Is Connecting the World (London: Virgin Publishing, 2011).

Russia Today, "WikiLeaks revelations only tip of iceberg – Assange," May 2, 2011.

Associated Press, "Number of active users at Facebook over the years," May 1, 2013.

"Facebook Privacy Policy: Feb.2, 2014," Facebook. http://www.facebook.com/help/405183566203254

William H. Davidow, Overconnected: The Promise and Threat of the Internet (Harrison, NY: Delphinium, 2012).

Cooper Smith, "Facebook Users Are Uploading 350 Million New Photos Each Day," Business Insider, September 18, 2013.

Lawrence Lessig, Code: And Other Laws of Cyberspace, Version 2.0, (Jackson, TN: Basic Books, 2006).