Do You Know if Your Data is Safe?

Bryan Saggese Bs623

12/15

Info 4250 Surveillance & Privacy

Prof. Levy

Is Your Data is Safe?

In today's information society, most Americans are constantly connected to the internet. Whether citizens are texting, tweeting, or playing angry birds, they are connected to the internet more than ever before. According to The World Bank, approximately 84.2% of the population are users of the internet. With that said, how often do we stop and think about who is able to see the actions we make online and the texts we send each other? Evidence provided by databreaches.net proves that several companies and websites that we reveal so much of our personal information to have experienced data breaches over the past 10 years. In other words, some of your sensitive data including email addresses, passwords, and credit card information may be in the hands of hackers and dark web surfers(some of the biggest breaches on the web involve LinkedIn, Ebay, and Yahoo to name a few). Adding insult to injury, many of these data breaches are a result of company negligence. We must be conscious of these facts, i.e., no matter how private one views one's data, there is always a risk associated with the internet. We may also have to provoke data companies to consider information security more important, as information security must increase as fast as information collection appears to be. At the very least, we must be cognizant of this risk and approach the internet with caution.

It seems as though data breaches are not on the minds of many Americans. However, if Americans knew that all companies are at risk, would that be different? Just recently, Yahoo was the victim of the largest cyber attack in history. This past September, around 500 million accounts were seized by hackers who had access to information ranging from names and telephone numbers, to email addresses and answers to security questions. In the words of Yahoo

itself, “Yahoo believes that information associated with at least 500 million user accounts was stolen and the investigation has found no evidence that the state-sponsored actor is currently in Yahoo's network.” This points out one of the scariest ideas in the realm of cyber security, however, as Yahoo exemplified the fact that they were not certain if the threat still remained after the attack was known. It is alarming that it is often impossible to know if an attack has concluded. It also presents the idea that a good hacker may never go noticed. Yahoo’s lack of evidence does not necessarily provide grounds of evidence of the hacker’s departure. With that said, it is interesting to think that hackers may, in some cases, go undetected entirely. In these cases, their attacks may never be discovered, their victims may never be notified, and millions of dollars may be at risk. Even when these attacks are uncovered, how should one act if he/she is affected?

According to the NYS Information Security Breach and Notification Act, “State entities and persons or businesses conducting business in New York who own or license computerized data which includes private information must disclose any breach of the data to New York residents.” [1] While it is good news that businesses are lawfully required to notify their customers of data breaches, how should those notified act in response? As expected, there are different actions to be taken depending on what data an individual loses control over during a security breach. For obvious reasons, one of the most nerve-racking breaches occurs when customer credit card information is stolen. If one is notified that their credit card info has been breached, it is imperative that one cancels his/her credit card immediately or that he/she monitors all activity on the card and reports any suspicious activity. But what if something less obvious is stolen, like

---

[1] https://its.ny.gov/eiso/breach-notification

one's social security number? In this scenario, a hacker with malicious intent could open up new accounts in an unknown victim's name. This new account fraud is very difficult to detect because these new accounts will be opened with different addresses. One of the only ways one might prevent this type of fraud is by closely analyzing one's credit reports or implementing a credit freeze.[2] A few questions that are important to consider when dealing with these situations include should the companies that suffered the data breaches provide compensation to their customers for them to enact credit freezes? I would argue that customers are entitled to some sort of compensation in the event of a data breach. This may depend on the cause of the breach, however. If the breach was conceived in spite of relatively complex encryption, then there may be less fault places on the target. However, when large companies experience breaches as a result of security negligence or employee ignorance, I do believe customers deserve compensation.

What some do not realize is that a surprising amount of breaches are caused by employee ignorance and lack of computer security. For example, in 2012, the government of Texas was responsible for accidentally leaking the social security numbers of 3.5 million people. In some cases this information was paired with dates of birth and drivers license numbers. In 2013, Scripps, a journalism company, discovered that TerraCom and Yourtel, two phone service providers, were housing sensitive information such as whether or not customers were enrolled in government assistance programs on public servers. More recently, personal details of over half a million Red Cross blood donors were accidentally published. This incident included contact information, drug use history, as well as whether or not the donor had taken part in any at risk

---

[2] https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice#data breach what to do

sexual behavior such as sex work or gay male sex. [3] Red Cross went on to explain that this information was published as a result of files being left unsecured and unprotected.[4] In these cases of information breach, victims deserve compensation, as these leaks could have easily been avoided had companies taken cyber security more seriously. For starters, employees should be educated on cyber security practices regardless of their position in a company. It is analogous to high school shop classes. All students entering the shop area must go through a safety course which highlights dangers of tools not everyone will use. This ensures that accidents are avoided when students use a tool they thought they would never have to use, perhaps during an emergency. In this way, companies could ensure that all employees are aware of how to handle sensitive data regardless of their current position in the company. As a result, if an employee is faced with handling pertinent data momentarily, he/she will be able to act securely.

Internal error aside, phishing and malware are two of the most common ways hackers gain access to valuable information. Phishing usually entails someone or something posing as a trusted entity and prompting users for personal information. The most common form of phishing is done via email and may involve sending an email designed to look exactly like one's trusted financial institution. The email may request that a user login and perform some action; however, once a user enters his/her username and password, his/her account has been compromised. It may be long before a user even notices any suspicious activity on his/her account; thus, it is imperative that emails be thoroughly inspected before any information is given online. In addition, malware involves software used with malicious intent. POS, or point of sale malware,

---

[3] http://mashable.com/2016/10/27/australia-biggest-ever-data-breach-red-cross/#nbUzlFbJkmqk

[4] https://docs.google.com/spreadsheets/d/1Je-YUdnhjQJO_13r8iTeRxpU2pBKuV6RVRHoYCgiMfg/edit#gid=3

is the most worrisome, as this is placed on technology that handles credit card transactions. Hackers may exploit a security flaw on a company network and set up malware on the connection customers make with company databases during credit card transactions. This would effectively allow hackers to intercept all incoming credit card information. Transactions are usually hidden from outsiders; however, if hackers are able to infiltrate into company networks, they will be able to see sensitive information which must be visible momentarily in order for a transaction to process.[5] Credit card information can then be sold on the dark web for anywhere from $1 to $100 depending on the robustness, or completeness, of the information offered. While this is all terrifying, I do not suggest simply avoiding all online technologies. I do, however, acknowledge that being aware of the ubiquity of data in tandem with the potential for data breaches may lead to a sort of panoptic mental state of mind.

Michel Foucault's idea of panopticism, as described in "Discipline and Punish", entails internalizing a certain fear to such an extent that one refrains from actions, even in the absence of direct supervision, that would present the chance of undesired consequences. [6] This applies to the analysis of data breaches because those who are aware of the implications surrounding loss of sensitive data may internalize the fear of a hacking event. Because we often cannot detect breaches as they are happening, the fear may become paramount, i.e., breaches are not necessarily associated with any flags, so they could be happening at any time. My laptop might be compromised as I write this very essay, and I could have no idea. In response, individuals may be very selective with the companies they trust. Some may exclusively use temporary email

---

[5] https://www.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks

[6] Foucault, "Discipline and Punish"

addresses and refuse to input credit card information online. As we have observed directly in class, some people cover their webcam when they are not using it. While seemingly simple, such an action demonstrates the panoptic power of the internet. Just as hackers may gain access to thousands of credit cards or social security numbers, they may be responsible for a quite literal application of the panoptic metaphor. In other words, not only may hackers observe digital footprints we leave online, they have the potential to literally watch us at our desk and observe the physical footprints we leave in our bedroom. Moreover, with the right computer script, hackers could take the passwords obtained from a data breach and apply these intrusive behaviors across millions of desktops simultaneously.

Perhaps none of this could be said without the feeling of visibility that the internet creates. It is as if some of us are more visible online than we are face to face, as information we may not normally disclose in every conversation is available for viewing at any time; for example, one's relationship status or sexual orientation. This speaks volumes about the implications associated with data breaches. As Kevin Haggerty and Richard Ericsson point out in "The Surveillant Assemblage," internet users have a "data double," which is described by an individual's online activity. To clarify, imagine a web page with every piece of information about you that is available on the internet, including the somewhat involuntary data that is recorded about you by businesses. This is your data double. Some of the contents of the double are only accessible to you; however, in the event of a data breach, all of this information may be uncovered. Haggerty and Ericsson would argue that privacy is more of a negotiation where privacy is traded for products, better services, and deals.[7] So, is the risk associated with having

---

[7] Kevin Haggerty & Richard Ericson, "The Surveillant Assemblage"

so much data available online just a requirement to be accepted along with these products and better services, or is there a moral obligation for companies to act on behalf of their customers and invest more in protecting data doubles with the same effort one might protect human life? If that sounds irrational, is it rational to think that the data we input online may one day be so sensitive that such a question might be reasonable? Overall, as our data doubles continue to build our lives into the digital realm, the harm caused by data breaches increases.

The good news is that data breaches are not occurring more frequently as time progresses.[8] So, unlike global warming, there may be less pressure to act. According to Edwards et al, "In our case, as security practices have improved, attacks have become more sophisticated, possibly resulting in stasis for both attackers or defenders." In other words, hackers are advancing just as fast as security measures are. Edwards also points out that although the frequency and size of attacks are stagnant, the impact of attacks may not be. As I alluded, the amount of data collected is increasing and becoming more financially related. With the rise of applications such as Venmo, which allows lightning fast money transfers, data breaches are far more significant.

Consequently, the bad news is that data breaches are not occurring less frequently as time progress. Big data companies need data to make money, and more data means more money, and as a result, there are more opportunities for hackers to capitalize than ever before. On the bright side, information technology laws and regulations are relatively new and there is certainly room for change. We live in a crucial time period for big data, as the government has the potential to decide the future of data and smart tech industries for years to come. Currently, the United States

---

[8] http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_edwards.pdf

adheres to a notice and consent policy. This means companies may collect virtually every piece of data about a user provided he/she agrees to share such data with companies. While it may go without saying, this solves nearly nothing. How many people truly read the privacy consent forms they agree to before perusing a website or downloading an app? In fact, according to a Carnegie Melon study done by Aleecia M. McDonald and Lorrie Faith Cranor, it would take approximately one month of reading per year to read all of the the privacy policies the average person would encounter on the internet if they were to read eight hours per day.[9] So, while consent legally legitimizes nearly every aspect of data collection, most people are paying consent zero attention. Maybe we need to be smarter as consumers, but more realistically, maybe we need to be smarter as a democracy.

With "smart technology" invading every aspect of consumer life, perhaps we need to focus this "smart" power on privacy and look for a smarter solution. As Meg Leta Jones points out, "There is opportunity as we transition from a world without screens to flip notice and choice on its head and build a smart world on choice and notice…" [10] This would mean that users could outline what exactly what they allowed to be done with their data, and companies would have to adhere. While Jones was focused primarily on smart technology, this would revolutionize data collection entirely and place more of the responsibility on businesses. This relates to data breaches in the sense that information users are not aware were collected are often exposed during cyber attacks. A choice and notice policy would also ostensibly allow users to specify how long their data may be stored before it must be requested again. Allowing users to place

---

[9] http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf

[10] Meg Leta Jones, "Privacy Without Screens & The Internet of Other People's Things"

expiration dates on their data could be extremely helpful. For example, I created a MySpace account several years ago and then forgot it existed. A few years after I forgot about the site's existence, it was confirmed that almost 300 million accounts were compromised. According to haveibeeenpwned.com, which determines whether or not an email address has been compromised, my data was leaked in the MySpace attack. Had I been able to set an expiry date on my MySpace credentials, this may have been avoided. (I encourage you to keep haveibeeenpwned.com bookmarked if you have several different internet accounts.)

Another way we should consider improving cyber security, this time to combat data breaches more directly, would be to instantiate an encryption law requiring companies of certain sizes to maintain a certain level of encryption. It is simply unacceptable for a company to store customer data in plain text, especially considering many encryption tools are free and relatively simple to use. Still, basic level encryption is not enough. In the case of MySpace, hackers were able to gain access to unsalted, yet encrypted passwords. In the realm of cryptography, salt is a random string of characters added to passwords before they are hashed, or hidden, to make them much harder to crack. So, while Myspace passwords may have been encrypted, without the use of salt, common passwords appeared as the same string of encrypted characters. This meant hackers could identify several hundred thousand passwords by comparing hashed strings they calculated using their own hash functions. For example, hackers may have known "password1" was going to be used numerous times. After inputing the string "password1" into a hash function, hackers could see how that password would appear in the MySpace database, which would effectively identify which users had "password1" as their password. Adding randomized salt would mean repeated passwords would still have different hashes so that this method of hacking

would not be feasible; however, while this could have been prevented with salt, it may have also been prevented by Myspace users.

Moreover, the battle of cyber security does not fall solely on the hands of businesses, as there is a lack of education surrounding online security for users as well. One alarming fact that continues to stare users in the face in the event of data breaches is that people are using elementary passwords that lend themselves to hacking (among the top five passwords revealed in the MySpace breach were “abc123” and “password1”). One tip to avoid online vulnerability would be to use long passwords, perhaps as long as twelve characters. Secondly, a commonly held belief is that arbitrary passwords such as “qehil2” provide strength, as they are seemingly random. However, most hackers crack passwords using brute force methods, meaning they try every possible combination until a match is found. That being said, the time it takes to crack a password while blindly guessing is proportional to the length of the password, not the complexity. Therefore, a long password that actually makes sense would not only benefit the user in the sense that it would be easier to remember, it would also be harder to crack.

With all of this in mind, it is clear that something can and should be done about the current state of cyber security. Furthermore, it seems as though education and awareness is the best place to start. As we educate the public concerning online security and preventative measures that can be taken to mitigate the effects of data breaches, people will become naturally conscious of the implications internet data and more informed when making security decisions on the internet. If people were more knowledgeable on the technology they use daily, there would be greater potential for corporate level changes as well. Lastly, education would presumably encourage more people to enter the cyber security sector which seems to be an

insatiable market at the moment. This would lead to a positive feedback loop possibly resulting in a society that is ultimately able to make smarter decisions online.

Works Cited

"Breach Notification." New York State Office of Information Technology Services. Enterprise Information Security Office, 17 Oct. 2016. Web. 5 Dec. 2016. <https://its.ny.gov/eiso/breach-notification>.

Cox, Orla. "Demystifying Point of Sale Malware and Attacks." Symantec Security Response. Symantec, 25 Nov. 2015. Web. 4 Dec. 2016. <https://www.symantec.com/connect/blogs/demystifying-point-sale-malware-and-attacks>.

Edwards, Benjamin, Steven Hofmeyr, and Stephanie Forrest. "Hype and Heavy Tails: A Closer Look at Data Breaches." (2015): n. pag. Web. <http://www.econinfosec.org/archive/weis2015/papers/WEIS_2015_edwards.pdf>.

Foucault, Michel. Panopticism. Harmondsworth: Penguin, 1979. Print.

Haggerty, Kevin, and Richard Ericson. "The Surveillant Assemblage." Haggerty - 2000 - The British Journal of Sociology - Wiley Online Library. N.p., 2000. Web. 5 Dec. 2016. <http://onlinelibrary.wiley.com/doi/10.1080/00071310020015280/abstract>.

Jones, Meg. "PRIVACY WITHOUT SCREENS & THE INTERNET OF OTHER PEOPLE'S THINGS." HeinOnline (n.d.): n. pag. Web.

Mandybur, Jerico. "Red Cross Leaks Personal Data of Half a Million People in Mass Breach." Mashable. N.p., 28 Oct. 2016. Web. 4 Dec. 2016. <http://mashable.com/2016/10/27/australia-biggest-ever-data-breach-red-cross/#nbUzlFbJkmqk>.

McDonald, Aleecia, and Lorrie Cranor. "The Cost of Reading Privacy Policies." A Journal of Law and Policy for the Information Society (2008): n. pag. Web. <http://lorrie.cranor.org/pubs/readingPolicyCost-authorDraft.pdf>.

"What to Do When You Receive a Data Breach Notice." What to Do When You Receive a Data Breach Notice | Privacy Rights Clearinghouse. Privacy Rights Clearinghouse, 26 Nov. 2016. Web. 5 Dec. 2016. <https://www.privacyrights.org/consumer-guides/what-do-when-you-receive-data-breach-notice#data breach what to do>.