Data: The Ultimate Destination

Data has never truly had its own place in the world until social media had begun to take the world by storm. Twenty years ago people didn’t have to worry about where their data might be or who had access to that. They only cared about check fraud and identity theft which were both relatively easy to deal with. Presently there are few people whose lives are not somehow accessible on the internet by anyone with a keyboard. Data in the past has only lived in filing cabinets, but now it flows freely through the digital world into the hands of, well, who knows.

The digital frontier lays in the palms of our hands whether it is a mobile device, laptop, tablet, or iPad. A person can setup all of their mail to be paperless and receive all of their important documents, reminders, or social greetings on a multitude of devices. Our data is being sent all over the world. The virtual world spectrum includes everything from banking to saying hello to a friend or family member that is on the other side of the world via video messaging services. Since 2001 banks are required by federal law to give new customers a copy of the privacy statement. If the bank is going to share any of user’s data with any other companies it will be stated in the privacy statement. They will sell or share a customer’s data to strategically market products to each individual. The bank however should provide an option to the customer to opt-out of this sharing of personal data.

Banks along with any other company on the internet are able to track what websites a user visits the most by viewing the browsing habits through the computers browser cookies. A browser cookie is a piece of data sent from a website that gets stored in the user’s computer. Whenever the user goes back onto the internet and reloads that website, the cookie is sent back to the website notifying the company of the activity. Third party tracking cookies are used mostly to hoard continuing records of users browsing histories. Cookies were originally designed to store data for users doing online shopping so the items in the shopping cart would not disappear. They are also able to store a user’s personal data such as login data, passwords, form content, credit card data, or even their address.

This is vital data that user’s certainly do not want getting into the hands of anyone with malicious intent. Encryption is a rather useful tool that websites use to safely transmit user data for safe-keeping. If encryption is enabled on a website there are a few things to look for at the top of the browser like a key icon, lock icon, and https to be part of the web address field. This is verifying that the data the user is typing into the form is going to be encrypted for storage. The digital thieves are consistently evolving to the new standards that are setup and implemented therefor leaving data potentially vulnerable at any given point in time. This is why it is good practice to consistently be changing the user password for vital online accounts that you do not want anyone gaining access to. A password should not be made simple like “johnsmith” or “ilovepizza”. The password should be made up of 8 or more characters and be letters and numbers combined. In some cases it is good practice to incorporate characters (\*, ^, %, etc.) into the password.

Data kept on bank servers is safeguarded against an everyday hacker. More experienced hackers are capable of something else known as a botnet. These experienced hackers will gain remote control of high speed servers to form a group of botnets which will at their command begin an attack against the server of a bank or large corporation. The hacker can infect any type of computer they want using email spam, pop-up spam, bit torrents, or any other type of source that will allow the malicious software to quickly implant itself into the system.

Customers do not have full control of what happens to all of their data. They are allowed to limit what banks can share with other companies but not stop them completely. Banks are share data such as social security number, employment data, account balances, transaction history, credit data, assets, and even investment experience. A bank can share consumer information for a multitude of reasons. They share customer data with service providers to offer new services and products and/or with joint marketing companies. Data regarding transaction history, experiences, and credit can be shared with the banks affiliates’. Customer’s credit card accounts can also be shared with non-affiliates to market directly to the customer. On the website of every bank there is a consumer privacy notice that tells customers exactly what data is shared with what kind of companies. Banks will not come right out in the open and tell the consumers the names of the companies that they are working with and instead just generalize them by calling them affiliates which could really mean any company in the world.

The way personal data on social media websites is shared is very different from how banks share data. “We do privacy access checks literally tens of billions of times each day to ensure we’re enforcing that only the people you want see your content”(Mark Zuckerberg, [www.consumerreports.org](http://www.consumerreports.org)). Facebook is the largest social media site in the world and consumers are right to question the safety of their personal data. People are generally concerned with what actually happens to their data once it is posted online even with the safeguards Facebook puts in place. Facebook however collects massive amounts of data from users. If a user visits a page that is not a Facebook page and this page happens to have a “like” button on it Facebook collects the user’s data. Even if the user does not click the button, is not logged in, or even have an account. A Facebook user could have all of their privacy restrictions set to the highest standards and that wouldn’t even matter. If a user’s friend is using the Facebook app they can enable third-party access to user information without the user’s knowledge of them ever doing so. All of those restrictions the user put in place now mean nothing. The restrictions themselves are essentially a safety blanket for users. To make them feel better about the privacy of their data when in reality it is simple for other companies that are non-affiliates of the Facebook Corporation to gather user data without the user’s consent.

The collection of data pertaining to user activity is what helps drive profits for Facebook and the companies they share user information with. They examine every click that is made by users. Every time a user “likes” a page, makes comments about something there is a market for or can be sold to them somehow, the data is combined and examined. They take this collected data and fill advertisement space with things they think the user will be interested in based off of the collected data. The overall goal of Facebook is “making the world more open and connected” (Mark Zuckerberg). They want all of their users to share as much information as possible in order to feed their data mining operation.

“In Europe, companies must notify consumers before collecting their data, and people have the right to obtain and correct copies of their information. The European Commission recently proposed even tighter rules that would require explicit “opt-in” consent before data were gathered and let you order that your data be permanently deleted—a provision known as the “right to be forgotten” ([www.consumerreports.org](http://www.consumerreports.org)). These laws make it more difficult for websites operating in Europe to share information about users and could be the very reason none are as profitable as American websites. The laws in the United States of America are almost nonexistent in comparison to the laws of Europe. The United States government only has strong laws that protect citizens’ rights, health, and finances. This is why there is such a difference between what happens with user data in banking and social media. Facebook does have a section in the settings where a user can “download your information” to see the personal file that Facebook keeps which may or may not include the full amount of data they have stored for each user.

User data stored in Facebook thus far has many loophole that it can jump through into the hands of third-parties. Applications and games that are within Facebook for users to play with are dangerous when it comes to the privacy of user data. “Whenever you run one, it gets your public information, such as your name, gender, and profile photo, as well as your list of friends even if you haven’t made that list public. And if you give the app certain permissions, it can peer deeper into your data and even see information that your friends share with you, unless they have specifically forbidden sharing with apps in their own privacy settings”([www.consumerreports.org](http://www.consumerreports.org)). Also, if a Facebook user posts replies to a wall that is publicly available then anyone can find this information online using whatever tools they have at their disposal. The same can be said for any other kind of data such as pictures or picture comments. All data that is made publicly available is at risk of being audited by government agencies (IRS, FBI, and local), prospective employers, and current employers. They can all use the public data to check if a person is breaking the law, posting sexually unfavorable material, or even making racist remarks. Companies can use this data to reprimand employees or even terminate their employment. Criminals can try to use this information that the user has made publicly available to gain access to vital information and potentially use it to damage ones reputation or for identity theft which is a whole other topic on its own.

There is also this popular mobile application called “Snapchat”. The application allows in theory a user to take a photo or video and send it to any person that is their friend within the application. The sender is able to set a time of 10 seconds or less for the receiver to view the file and then it is supposed to be gone forever. It is a great concept but in reality data is never really gone is it. The idea behind the data, in this case video or picture, being gone forever is nothing more than a magicians trick in this case. “Forensic researcher, Richard Hickman, has discovered that Snapchat photos on Android phones are merely hidden, not deleted, and are still available for retrieval with the right forensic software” ([www.theguardian.com](http://www.theguardian.com)). Metadata is very difficult for any technology expert to remove from a device. Since the metadata from Snapchat is metadata we can conclude that it doesn’t in fact disappear like a magic trick and is physically somewhere on the device. Forensic toolkits that allow someone to go into the device are easily found with a little bit of effort searching the internet. It does get easier than that for users of Snapchat though. Other developers have found the exploit that reveals this illusory tactic and have made other applications available to save the pictures or videos without ever notifying the sending party.

Data and where it goes is often a mystery because the laws of the land are having such a hard time keeping up with the ever evolving world of technology. It’s only when big gaps in security are made public by security experts or hackers that companies continue to raise the security ceiling. There is never an impossible moment for data to be accessed by a third-party whether it is lawful or with malicious intent. In the United States a consumers data is safer because there are laws in place that strongly safeguard a persons or institutions finances. The same cannot be said for social media or mobile applications. In order for these companies to thrive they have to share and or sell user data to any company that wants to use user data for their own gain.

There is no such thing as safety of personal data if it is electronically shared. The luxury of technology has taken away privacy of any person that uses anything powered by electricity today. Everything from phones, cars, televisions, laptops, credit cards, and the list keeps going, will send user data pertaining to that item and the activities associated with it to any company with money. It does not matter if there are privacy settings in place because there are always limits as to what a user can block from being shared or there are simply too many loopholes in the system that basically negate every setting the user puts in place to safeguard their information. Data that users may not want shared with anyone or any company will never be private. Once it’s out there, it’s there forever unless laws change in the future.

Works Cited

1. Marie Wallace, IBM, What happens when big data meets social media (<http://www.simply-communicate.com/news/top-tips/what-happens-when-big-data-meets-social-media>)
2. FDIC, Safe Internet Banking (<http://www.fdic.gov/bank/individual/online/protect.html>)
3. Bank of America, U.S. Consumer Privacy Notice, (<https://www.bankofamerica.com/privacy/consumer-privacy-notice.go>)
4. June 2012, Consumer Reports Magazine, Facebook & your privacy (<http://www.consumerreports.org/cro/magazine/2012/06/facebook-your-privacy/index.htm>)
5. Mark Zuckerberg, December 2009 <https://www.facebook.com/notes/facebook/an-open-letter-from-facebook-founder-mark-zuckerberg/190423927130>
6. Nicole Perlroth, January 2014,NYTIMES.com, (<http://bits.blogs.nytimes.com/2014/01/02/snapchat-breach-exposes-weak-security/?_php=true&_type=blogs&_r=0>)
7. Snapchat’s expired snaps are not deleted, just hidden, theguardian.com (<http://www.theguardian.com/media-network/partner-zone-infosecurity/snapchat-photos-not-deleted-hidden>)