Cody Scholl

Julie M. Henderson

CSCI 325

15 October 2018

# The Data You Actually Care About

Data, the essence of our being we use to show our personas online, has become worth diamonds in our consumer market today. Websites and companies nowadays have their user's data stored in a database, waiting to be pulled when the user clicks the remember me button on the sign in page or telling the user if their information they've typed to sign in is correct. Usernames, passwords, how many times user's frequent the site, are all catalogued into the database and companies will pay millions to get a dying business's information. This has become widespread across most platforms in the website and software industry, and companies love to know what the target audience is all about. As a prospect in the field of software development and writing programs to fit a consumer's needs and desires, I would likely have direct access to such sensitive information. But is it ethical for companies to keep such sensitive information such as phone numbers, emails, credit card numbers, social security numbers, names, contacts, and locations readily available? The ethical dilemma is what if all this information is broken into in a data breach and taken for malicious acts or identity theft?

Data breaches aren't at the top of most threatening list and this is for good reason. Companies pay big bucks to make sure their websites and software products are as safe as possible and for the most part, they truly are locked and secured. But occasionally it happens to the best of the best, take Facebook for instance. The social media giant's data breach was nothing

but massive and had nearly 14 million user's information stolen such as "…religion, gender, relationship status, birthdate… and location" (John). Additionally, "15 million users had just their names and contact information stolen" (John). Now thinking about these things, they don't seem to harmful other than maybe location, but experts say otherwise. Experts state, "Accessing your private communications and posts by itself is pretty invasive, but that information could also be used to crack account security questions or to scam you and your friends." (John). It becomes increasingly serious when the information taken is from a reputable place, like a bank or hospital. Hospital data breaks have residual effects like, "… financial and reputational harm…" (Knudson). It seems ridiculous, but you'd be surprised what people can get away with using someone else's online persona. As the bible states, "The good person out of the good treasure of his heart produces good, and the evil person out of his evil treasure produces evil, for out of the abundance of the heart his mouth speaks." (Luke 6:45 NIV). Not everyone is out to get and use your information for evil but the evil person out of his evil treasure produces evil and that can't be avoided as God intended it.

There are multiple ways to handle or limit this dilemma without companies losing their consumer base. First off, make companies and websites have a mandatory level or grade of protection on all their platforms. This will allow users to feel safe while typing in sensitive information and mostly likely limit the number of sketchy websites that can come up when you are browsing the web. Another one is to limit the amount of information a website or application can take, who wants to give out credit card information for a free trial? If we limit the amount of information the businesses and websites take, we can limit the amount is lost if something were to happen. Of course, there is always the option of hiring people to break into the companies and then tell them how to fix it or to just fix it themselves. This would allow companies to have a

growing protection on their data and security rather than a stagnant and possibly outdated level of protection.

I feel like I'm not ready to face these challenges as I'm still learning to build the software and programs, let alone protect them from someone trying to break them. Getting the program to run perfectly is arguably harder and the auto grader is a more difficult foe than anyone trying to breach the program. It would have to be something developed over time in the industry and alone on personal projects, like making something just to see if I could break into it. Learning the methods of entering so you can learn how to stop them, reverse engineering at it's finest. To get prepared I could sit through lectures and seminars about software and website protection, maybe get a hands-on approach from a course or lab. Even asking veterans in the field of data protecting would be beneficial and could shed some insight in the data breach dilemma in another light. Another interesting way would be to ask people who have broken into huge companies in return for like amnesty to see how they think and how they would approach stealing data. Something that could be experimental would be to hire the data stealers to defend it, that way they know what typical ways to breach and in return, block them from getting in.

Data is becoming more valuable by the second, but the more valuable things become, the more we must protect it. The ethical question is, should companies keep sensitive information? I think yes, but only to a certain extent, like a username and password, maybe a birthday for like sales or something. It must also be protected to a mandated level and companies should be punished for not meeting that level and fined if they are broken into, that will keep companies compliant of keeping their security of data up to date. For the ethical dilemma of data breaching, it should be respected and prepared for with responsibility and persistence.

# Work Cited

John, Allen St. “Here's What Makes the Facebook Data Breach so Harmful.” *Consumer Reports*, 12 Oct. 2018, www.consumerreports.org/digital-security/what-makes-the-facebook-data-breach-so-harmful/.

Knudson, Julie. “Data Breach: What's at Stake for Hospitals.” *Radiology Today*, Radiology Today Magazine Vol. 16 No. 2 P. 18, Feb. 2015, www.radiologytoday.net/archive/rt0215p18.shtml.

*New International Version*. Biblica, 2011. *BibleGateway.com*, https://www.biblica.com/bible/niv/luke/6/