Undergraduate Thesis Prospectus

Redundancy and Distribution: Preventing a Single Point of Failure

(technical research project in Computer Science)

The Privacy Struggle: How Consumers Advocate for Change

(sociotechnical research project)

by

Uttam Rao

November 2, 2020

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.
Uttam Rao

Technical advisor: Aaron Bloomfield, Department of Computer Science

STS advisor: Peter Norton, Department of Engineering and Society

General Research Problem

How can the loss incurred from cyber breaches be reduced?

According to the World Economic Forum, other than environmental risks such as cataclysmic natural disasters, the cyber threat is the biggest risk the world faces (WEF, 2019). A successful cyberattack may cause millions of dollars in damage, but the impact extends far past the financial effects (Puranik, 2019). Most consumers readily trust their data to companies, exposing themselves to leaks of private information, or identity theft. Between 2017 and 2020, over 8 billion records were breached; many held sensitive data such as medical records or bank information (Puranik, 2019). In the Facebook-Cambridge Analytica Scandal, leaked consumer information was used to influence political processes (Confessore, 2018). Businesses that collect and store consumer data incur an average of $8.19 million in direct costs per breach, and suffer difficult-to-measure reputational damage (Puranik, 2019; Columbus, 2020). Governments store sensitive data about citizens and about national security. A cyberattack on a nation can damage critical infrastructure such as power stations and can even cause a disaster, such as emitting nuclear radiation. Even a decade ago, internet-connected computers faced an attack every 39 seconds on average (UMD, 2007). Now, cloud computing, automation, and 5G offer a larger surface for attackers to exploit (Wheeler et al., 2019; GAO, 2019). Because of the COVID-19 pandemic, social and economic dependence on the internet is greater than ever; hence cybersecurity is now more important than ever.

Redundancy and Distribution: Preventing a Single Point of Failure

How can data be distributed to prevent system breaches from becoming data breaches?

My technical research project is in the Computer Science department. It is also a capstone project. I intend to complete my technical report in the spring, so I have been instructed to list Aaron Bloomfield in the computer science department as my technical advisor. This will likely change in the spring. I plan to continue with this research problem and work individually, but the change in the CS capstone process allows for changing my focus or working with a partner in the spring.

There are a multitude of methods by which systems are currently compromised. Organization insiders, foreign state-sponsored attacks, hackers, configuration errors, and an increase in quantum computing efficiency can all cause system breaches and pose significant threats to data protection (Symanovich, 2020). If a system breach occurs, organizations are required to notify consumers if there is any possibility of data being compromised. The cost of notifications, remediations, non-compliance fines, and reputation damage poses a huge risk to organizations. The concept of safe harbor data protection, which assures that system breaches do not result in data breaches, is the holy grail in data protection (Burdon et al., 2010).

There are no widely implemented methods to provide safe harbor data protection. There are many effective techniques to protect a system and prevent a security breach. However, if a system is breached, there is no way to guarantee that data is protected. There are also various methods to react to a system or data breach and minimize the damage (Splunk, 2020). The current best in class data protection methods are various forms of encryption such as AES and RSA (NIST, 2018). These are still susceptible to insider threats, re-encryption attacks like ransomware, and quantum attacks. Multiple startups have come up with innovative ways to implement distributed safe harbor protection and have patents pending, but they still do not have market share (SplitByte, 2020; Myota, 2020). These methods are based on the innovative secret

sharing technique that Shamir introduced in 1979, but at the time lacked the scalability infrastructure that makes it feasible and relatively inexpensive today (Shamir, 1979).

I plan to research how redundancy and distribution over multiple locations in addition to existing forms of encryption can prevent a single point of failure. More specifically, I aim to research methods for utilizing Shamir's secret sharing on the cloud, where randomization and distribution on top of encryption will prevent any data from being compromised even if multiple (but not all) locations are breached. In contrast to the preventive and reactive methods discussed previously, this will be proactive data protection. I will research and review existing academic literature and the methods used by various startups and established companies in the industry thoroughly. I will also reach out to the leadership of these startups, with some of whom I already have secondary connections through my work experience. Since I will do my technical project in the spring, the details of what I will have at the end of my project are still to be decided. The extent of my project may just be a literature review, but I hope to also have a simple working demo of Shamir's secret sharing on the cloud which will show it is possible to have safe harbor data protection inexpensively.

The Privacy Struggle: How Consumers Advocate for Change

How do consumers who care about data privacy organize to advocate for interests?

In response to growing cyber threats, organizations have needed more robust privacy protections. Though consumers report that they value privacy, few read privacy policies before agreeing to them (Redman et al., 2020; Auxier et al., 2020a). Recently, however, a stream of data breaches, misuses, and scandals has caught people's attention (Kerry, 2019). Surveys have identified a growing group of consumers: 32 percent of respondents now report that they not

only care about data privacy but are also willing to act to protect it (Cisco, 2019). How members of this group, termed here *privacy actives,* organize and advocate for their interests bears implications both for company strategies and for public policy governing data privacy and ownership (Redman et al., 2020; CCP, 2020).

Private companies and public agencies collect private data. Private companies seek to balance short-term profits against the expense of averting longer-term privacy threats. A privacy scandal can wreak financial havoc on a company (BBC, 2020). Therefore Facebook, for example, has publicized a commitment "for the next decade ... to build much stronger privacy protections" for all consumers (Zuckerberg, 2020). It has also pledged to be accountable for data security and to comply with the law (Facebook, 2020). Data companies also spend millions to lobby against regulatory threats (Romm, 2020). Government agencies must comply with federal law and earn public trust. For example, the National Security Agency claims that it "strives to build public trust" by demonstrating that it can "uphold civil liberties and privacy values while also protecting America and its allies" (NSA, 2020).

Among consumers, *privacy actives* are willing to act to protect privacy. *Privacy actives* are represented by advocacies such as Common Sense Media. Jim Steyer, its CEO, has said that privacy "is complex stuff, and we need to make it very easy for consumers to understand what their rights are and how to exercise them" (Ng, 2019). On behalf of *privacy actives*, Steyer pressed California Governor Newsom to back the California Consumer Privacy Act of 2018 (Loizos, 2019). Other consumers favor control over their privacy but do not act to promote stricter privacy standards. Surveys indicate that the vast majority of them disapprove of some data companies' uses of personal data (PwC, 2020; Auxier et al. 2020b). Californians for Consumer Privacy (CCP) is an advocacy representing *privacy actives*. Its members include

presidential candidates and the CEOs of large companies. It sponsored "the California Consumer Privacy Act ballot referendum signed by 629,000 Californians" (CCP, 2020; California DOJ, 2020).

Researchers have studied the competition to set data privacy standards. Acquisti and Loewenstein (2013) found that while consumers report caring about their privacy, few act to protect it. Bennet (2008) credits civil society organizations for the development of privacy rights and argues that they are crucial to privacy advocacy. In a study of consumers, government agencies, companies, and advocacies, Hemphill (2019) concludes that industry self-regulation has advantages over public regulation. Examining the interest group struggle that culminated in CCPA in 2018, Alpert (2020) maintains that big tech is still insufficiently regulated. Hurwitz and Jaffer (2020) contend that privacy advocates' positions are often counterproductive in the long run.

References

Acquisti, A., John, L., & Loewenstein, G. (2013). What Is Privacy Worth? *The Journal of Legal Studies, 42*(2), 249-274. doi:10.1086/671754

Alpert, D. (2020). Beyond Request-and-Respond: Why Data Access Will Be Insufficient to Tame Big Tech. *Columbia Law Review, 120*(5), 1215-1254. doi:10.2307/26921064

Auxier et al. (2020a). Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, May 26). Americans' attitudes and experiences with privacy policies and laws. Pew Research Center. https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

Auxier et al. (2020b). Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2020, August 17). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center.

https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

BBC. (2020, January 29). Facebook: Privacy scandals take toll on profits. https://www.bbc.com/news/business-51304516#:~:text=Facebook has recorded its first,bn (£14.1bn).

Bennett, C. J. (2008). Privacy advocates, privacy advocacy and the surveillance society. *Routledge Handbook of Surveillance Studies,* 412-419. doi:10.4324/9780203814949.ch4_2_c

Burdon, M., Reid, J., & Low, R. (2010). Encryption safe harbours and data breach notification laws. *Computer Law & Security Review, 26*(5), 520-534. doi:10.1016/j.clsr.2010.07.002

Columbus, L. (2020, April 06). 2020 Roundup of Cybersecurity Forecasts and Market Estimates. *Forbes*. https://www.forbes.com/sites/louiscolumbus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/?sh=279f4448381d

Confessore, N. (2018, April 04). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. *The New York Times*. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

California DOJ (2020). State of California Department of Justice. (2020, July 20). California Consumer Privacy Act (CCPA). https://oag.ca.gov/privacy/ccpa

CCP (2020). Californians for Consumer Privacy. (2020, October 07). About Californians for Consumer Privacy & Yes on Prop 24. https://www.caprivacy.org/about-us/

Cisco Systems, Inc. (2019, November). *Consumer Privacy Survey* [Scholarly project]. In *Consumer Privacy Report - Cisco Cybersecurity Series Feb 2020*. https://www.cisco.com/c/dam/en/us/products/collateral/security/cybersecurity-series-2019-cps.pdf

Facebook, Inc. (2020, October). General Data Protection Regulation. https://www.facebook.com/business/gdpr

GAO (2019). United States Government Accountability Office. (2019). *Cloud Computing Security Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed* (Rep.). doi:https://www.gao.gov/assets/710/703193.pdf

Hemphill, T. A. (2019). 'Techlash', responsible innovation, and the self-regulatory organization. *Journal of Responsible Innovation, 6*(2), 240-247. doi:10.1080/23299460.2019.1602817

Hurwitz, J., & Jaffer, J. (2020). Modern Privacy Advocacy: An Approach at War with Privacy Itself? *Pepperdine Law Review,* 955-964. https://digitalcommons.pepperdine.edu/plr/vol47/iss4/4.

Kerry, C. F. (2019, October 25). Why protecting privacy is a losing game today-and how to change the game. Brookings Institution. https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game/

Loizos, C. (2019, February 13). Jim Steyer runs the powerful nonprofit Common Sense Media; now he's using his influence to battle big tech. *TechCrunch*. https://techcrunch.com/2019/02/12/jim-steyer-runs-the-powerful-nonprofits-common-sense-media-and-hes-increasingly-using-his-influence-around-tech-consumption/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAAE5J7_P-bPQdFbVx7Kgm0e7GCMv9ssdb2jDZ7QN4CQNe9_s8yZptN5iGW-vcnQrWC-2h3u91Qk9oaWWTJv6d2lbhZi8rEAilPNbGLqJ6s6yDEh31xCdb6eqbma8lZlZcV2j-bjPj9OKqDi_LhuEqKb9W4fyJaaWZCRomcsn3FGrx
Contains direct quotes from Jim Steyer in an interview which are primary sources.

NSA (2020). National Security Agency. (2020, August). Civil Liberties and Privacy. https://www.nsa.gov/about/civil-liberties/

Myota Inc. (2020, October 19). Change the Data. Change the Rules. That's the magic of Myota. http://myota.io/

NIST (2018). National institute of Technology and Standards, & Swenson. (2018, December 11). NIST's Encryption Standard Has Minimum $250 Billion Economic Benefit, According to New Study. https://www.nist.gov/news-events/news/2018/09/nists-encryption-standard-has-minimum-250-billion-economic-benefit

Ng, A. (2019, May 01). Consumer advocates give Congress a different perspective on data privacy law. CNET. https://www.cnet.com/news/consumer-advocates-give-congress-a-different-perspective-on-data-privacy-law/

Puranik, M. (2019, December 02). Council Post: What Is the Cost of a Data Breach? *Forbes*. https://www.forbes.com/sites/forbestechcouncil/2019/12/02/what-is-the-cost-of-a-data-breach/?sh=39250a8a29e7

PwC (2020). PricewaterhouseCoopers. (2020, February 28). Consumers trust your tech even less than you think.

https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/trusted-tech.html

Redman, T. C., & Waitman, R. M. (2020, January 28). Do You Care About Privacy as Much as Your Customers Do? *Harvard Business Review*. https://hbr.org/2020/01/do-you-care-about-privacy-as-much-as-your-customers-do

Romm, T. (2020, January 22). Tech giants led by Amazon, Facebook and Google spent nearly half a billion on lobbying over the past decade, new data shows. *The Washington Post*. https://www.washingtonpost.com/technology/2020/01/22/amazon-facebook-google-lobbying-2019/

Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22*(11), 612-613. doi:10.1145/359168.359176

SplitByte Inc. (2020, October). Technology. https://splitbyte.com/technology/

Splunk Technology. (2020, October). Using Cyber Security Analysis to Detect, Analyze and Respond. https://www.splunk.com/en_us/cyber-security/security-analysis-response.html

Symanovich, S. (2020). What is a security breach? NortonLifeLock Inc. https://us.norton.com/internetsecurity-privacy-security-breach.html#:~:text=A security breach occurs when,organization's protected systems and data.

UMD (2007). A. James Clark School of Engineering. (2007, February 9). Study: Hackers Attack Every 39 Seconds. https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds

Wheeler, T., & Simpson, D. (2019, October 25). Why 5G requires new approaches to cybersecurity. Brookings Institution. https://www.brookings.edu/research/why-5g-requires-new-approaches-to-cybersecurity/

WEF (2019). World Economic Forum. *The Global Risks Report 2019* (14th ed., pp. 5-6, Rep.). Geneva. doi:http://www3.weforum.org/docs/WEF_Global_Risks_Report_2019.pdf

Zuckerberg, M. (2020, January 28). Starting the Decade by Giving You More Control Over Your Privacy. Facebook Inc. https://about.fb.com/news/2020/01/data-privacy-day-2020/