A RIGHT TO PRIVACY: THE INTERSECTION OF CYBERSECURITY AND POLICY IN PROTECTING CONSUMER DATA

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Jason Tufano

August 2, 2021

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.

ADVISOR
Catherine D. Baritaud, Department of Engineering and Society

DATA TECHNOLOGY ADVANCEMENTS THREATEN CONSUMER RIGHTS

With software and the internet collectively serving as a cornerstone of modern life, discussion of their flaws is critical in protecting the rights of the general public. One human right that the digital world has evolved is the right to privacy. The prevalence of data collection requires software engineers to consider both how they collect data, and how they keep it secure. The Cambridge Analytica-Facebook scandal illuminated issues of digital privacy, when in 2018 the public discovered that Cambridge Analytica had used the Facebook platform to harvest citizens' data. Cambridge Analytica managed to "download the sensitive personal information of 50 million Facebook users after only getting questionable authorization from 270,000 people" (Duck Duck Go, 2018, para. 1). This scandal brought privacy to the forefront of discussion, with a survey of 1,153 Americans showing that 64% were more concerned about online privacy after the incident than they were before (Duck Duck Go, 2018, para. 9).

To safeguard sensitive consumer data, software engineers have a responsibility to make secure products. To this end, the technical capstone of this portfolio analyzes the preparedness of University of Virginia (UVA) computer science engineers to deal with cybersecurity threats. Although not all computer scientists will need to deal with the specifics of cybersecurity, all software must be secure, and thus to be a responsible software engineer requires at least a cursory level of cybersecurity knowledge. Despite this, software data leaks are common occurrences. For example, in 2019, journalists Flitter and Weise reported that a hacker obtained "140,000 Social Security numbers and 80,000 bank account numbers" from Capital One (para. 7). Evaluating gaps in the UVA cybersecurity curriculum is not going to revolutionize software security in the industry, but it is a small step toward the ideal of impregnable software defenses.

Product security alone is insufficient in protecting digital privacy; social factors must be considered as well. Despite a general understanding of the importance of user privacy, major tech corporations like Google and Facebook appear to value potential data applications over potential ethical concerns of data collection. Thus, engineers need to consider more than their technical work to fully protect consumer data. This Science, Technology, and Society (STS) research paper explores the state of privacy in California using Actor-Network Theory (ANT) to reveal important non-technical factors embedded in digital data collection. A discussion of ANT would be incomplete without acknowledging the work of Michel Callon, Bruno Latour, and John Law, who have, through various articles, developed and refined the framework. Darryl Cressman (2009) succinctly summarized the usefulness of ANT as follows: "ANT studies associations between heterogeneous actors … these associations, in turn, can be used to describe how networks come to be larger and more influential than others, how they come to be more durable through enrolling both social and material actors, and where power comes from and how it is exerted" (p. 4). This paper will compare the associations of actors in the California data privacy network to associations in the national US network, to determine the key elements of strong privacy legislation.

In coupling the technical and social aspects of privacy, this portfolio intends to promote one of the fundamental responsibilities the National Society of Professional Engineers (2019) identifies in their code of ethics: to "hold paramount the safety, health, and welfare of the public" (p. 1). While a right to privacy may seem inconsequential in terms of the safety of the public, when improperly used and handled, personal data can be used against an individual, threatening their ability to live autonomously. This threat to autonomy alone is enough to warrant consideration from engineers. While this paper will not likely be a turning point for digital privacy, it does aim to promote responsibility and encourage awareness of consumer rights in software engineers.

PRIVACY IN PERIL: THE IMPORTANCE OF GIVING CONSUMERS A VOICE IN TECHNOLOGICAL DISCUSSION

CURRENT UNITED STATES DATA PRIVACY FALLS SHORT

The lack of privacy legislation in the US has resulted in the dominance of data scouring software. One of the primary data collection tools used by tech companies is social media. Social media products thrive on consumer data, creating profit by delivering personalized advertisements to users. Social media is a particularly devious data collection tool due to users developing a reliance on the platforms. In 2021, communications researcher Yu pointed out that "despite the deleterious effects of sharing information gathered from online government surveillance, people continue to use social media to share personal information" (p. 67). Consumers should not be blamed for this behavior, however; as business and technology researchers Zhu and Chen (2015) concluded, "each type of social media service is able to address a unique set of human needs," which explains why people are reluctant to stop using the platforms even in the face of privacy concerns (p. 339). With data collection software satisfying users' social needs, protecting privacy should not be solely a consumer responsibility. Software engineers and regulators must both take action to ensure that software products protect user rights.

In an attempt to determine the role of regulators, this paper analyzes the state of data privacy in the US using Actor-Network Theory to compare the network in California to the national network. Solving issues of consumer privacy will require collaboration between engineers, tech companies, and regulatory entities; this paper does not intend to provide a full guide for how to achieve this collaboration. Rather, the goal is to identify key differences between California's actor-network and the United States' actor-network to understand where more attention may be needed when crafting national data privacy regulations. As shown in Figure 1 below, the United States network is complex, with many different actors who have varying levels of influence on data collection regulations. One important association to note is the weak connection between consumers and the US government, as consumers are only able to vote on representatives for the federal government, leaving little room for influence outside of these elections. The weak connection between state governments and data collection regulations, as well as the lack of connection between the US government and the regulations, represents the failure to protect privacy in the current system.

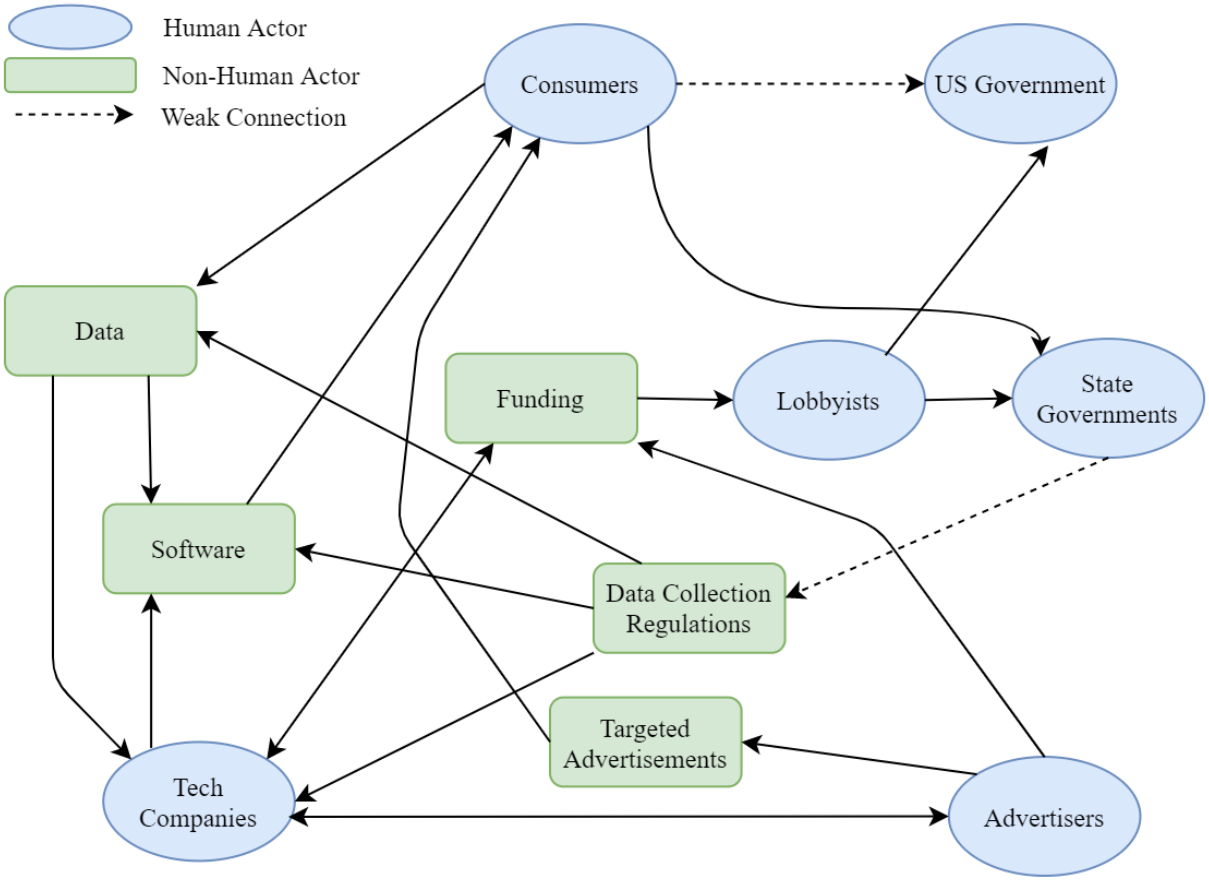

Figure 1: Actor Network Model of Current US Data Collection Regulation. This figure depicts the current state of affairs for digital privacy in the US. The missing link between the federal government and data collection regulations is a notable cause for concern. (Tufano, 2021a).

DYNAMIC DATA COLLECTION PRACTICES REQUIRE IMMEDIATE RESPONSE

The landscape of digital privacy is constantly changing, as tech companies continue to refine practices for collecting and analyzing consumer data. Although privacy legislation is already overdue, further delays threaten to leave consumer privacy vulnerable in the face of novel threats. One example of such a threat is Google's upcoming Federated Learning of Cohorts (FLOC) model. The FLOC model plans to change how consumer data is used by eliminating the need for tracking cookies across websites; instead, tracking will be done by the browser, which will determine a "cohort" of individuals who will likely be receptive to similar advertisements (De Vynck, 2021, p. 19). Google intends to implement this new model by 2022, leaving little time for federal privacy regulations to have any impact on its implementation. Privacy concerns that are not inherent with the development of technology are more unpredictable, but still demonstrate an urgent need for legislation. For example, the Covid-19 pandemic forced many people to increase the time they spend online, which in turn increased data collection. As social science researcher Kampmark (2020) concluded, "one enduring legacy of the novel coronavirus is the incremental development of surveillance technologies … giving birth to what amounts to the pandemic surveillance state" (p. 59). These threats, in addition to the unpredictability of future data collection practices, require immediate legislative response; maintaining the status quo will result in consumer privacy continuing to suffer.

The issue then does not concern whether or when legislation is needed, but instead what governing body should create the legislation. Though some may argue that privacy should be handled by the states, according to the International Association of Privacy Professionals (2021), only three states have passed privacy legislation, with only four other states having a bill in committee (p. 1). This leaves 43 states with no legislation, leaving many consumers defenseless.

With the majority of states failing to regulate data collection, a federal law is needed to guarantee privacy for all Americans. Unfortunately, as journalists Kang and McCabe (2021) concluded, bills that seek to weaken the power of Big Tech "face fierce opposition from technology companies," who use extensive lobbying to prevent such bills from being passed (p. 1). Finding a way to draft privacy legislation in the face of this opposition will be difficult, but an examination of the California privacy laws and how they came to be may shed light on a strategy for doing so.

RESOURCES FOR STRENGTHING UNITED STATES PRIVACY LEGISLATION

The US has a clear resource when it comes to forging a national privacy law: the California Privacy Rights Act (CPRA). The act is the second of two privacy acts passed in California, the first being the California Consumer Privacy Act (CCPA) in 2018. An understanding of why the CPRA is a useful model first requires an understanding of what it does. The CPRA expands upon the regulations of the CCPA, which delineated four main consumer rights: the right to know what data is collected and how it is used, the right to deletion of personal data, the right to opt-out of the sale of personal data, and the right to non-discrimination for exercising CCPA rights (State of California Department of Justice, n.d., para. 1). These protections are in line with those outlined in the European Union's General Data Protection Regulation (GDPR), which revolutionized data collection in Europe when it was implemented in 2018. As public policy researchers Radia and Khurana (2018) noted, two important stipulations of the GDPR are the right of portability, which "requires companies to export user data on request," and the right of erasure, which "requires companies to delete a person's data at his or her request" (p. 2). These two rights correspond to the "right to know" and the "right to delete", respectively.

The CPRA has many nuanced changes from the CCPA, but there are two major differences of note. First, the CPRA defines a concept called “sensitive personal information.” As legal workers Rosen, Madigan, and Markos (2021) concluded, this new classification “captures a broad scope of consumer data that goes beyond ‘personal information’”, including social security numbers, geolocations, and contents of communication not intended for the business (p. 30). The inclusion of an explicit description of sensitive personal information that consumers can know is safe may help foster an atmosphere of trust that is sorely needed in the industry. Second, the CPRA creates a new California Privacy Protection Agency, which the Electronic Privacy Information Center (EPIC) (n.d.) noted is “a major step forward in protecting the privacy of California residents” (para. 18). Examining the impacts of these changes on the California actor-network will shed light on the key role they play in protecting digital privacy.

The California actor-network, as seen in Figure 2 below, unsurprisingly bears many similarities to the national network. There are two notable differences: first, the inclusion of the California Privacy Protection Agency, which forms stronger connections between consumers, the government, and data collection regulations, and second, the ballot initiative system that connects consumers and activist groups to the government. The privacy protection agency creates communication options for consumers, tech companies, and legislators to provide input on data collection regulations. This agency reduces the pressure on legislators to be fully informed on the details of data privacy, and also allows consumers to better voice their opinions. The other difference, the ballot initiative system, is not a result of the CPRA, but rather the means by which it was created. In California, citizens can propose legislation, which can then be voted on during elections, provided the proposal gains enough signatures from registered voters.

The ballot initiative system was used for both the CCPA and the CPRA, allowing the activist group Californians for Consumer Privacy to directly propose legislation for citizens to vote on.

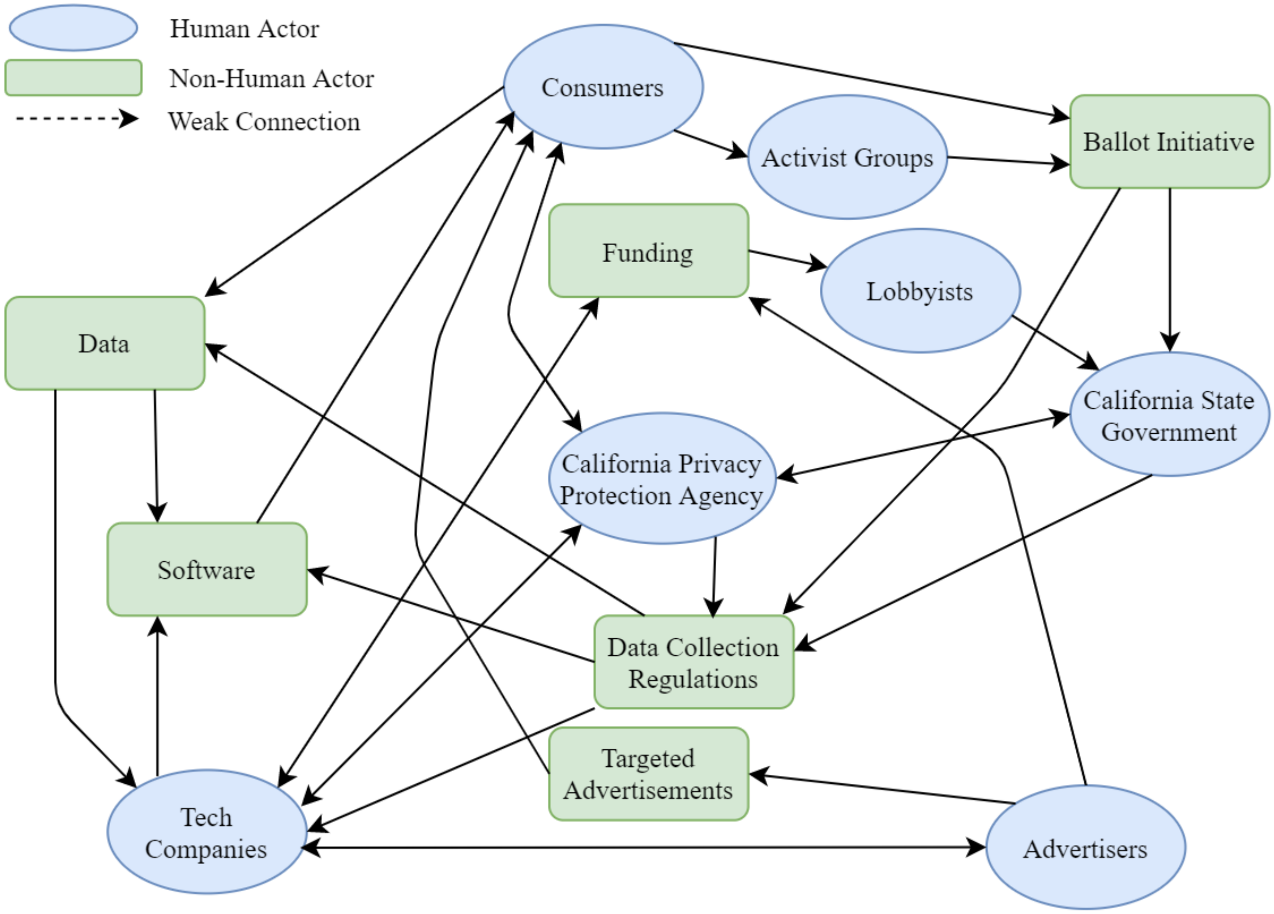

Figure 2. Actor network model of data collection regulation in California. This figure depicts the state of digital privacy in California after the passage of the CPRA. The new California Privacy Protection Agency and the ballot initiative program are key differences from the national network. (Tufano, 2021b).

THE VALUE OF A PUBLIC VOICE ON PRIVACY

The California actor-network model in Figure 2 demonstrates the importance of providing consumers with a platform to provide input on data collection regulations. The issue is then not one of determining what will help safeguard consumer privacy at a national level, but instead one of figuring out how consumers can provide input. Unfortunately, applying the ballot initiative system nationally requires restructuring the US governmental system. Making such a major change to the way the country is run is not a simple task. There is still hope for privacy, however; while consumers may struggle to have their voice heard at times, the need for data privacy regulations is clear, and the government may finally begin to make headway on this front. Karen Schuler (2021) of the International Association of Privacy Professionals cited the proposal of four data privacy acts in the Senate since 2019 as a reason to believe that Congress will pass privacy legislation in the near future (para. 2). If a law is passed, creating pathways for consumers to influence future data collection regulations will be critical in providing lasting protection of the right to privacy.

Following California's example, instituting a data privacy agency at the national level would be perfect way to include consumers in decisions. Even Daniel Sepulveda (2018), a former employee of an advertising technology company, argued that responsible data collection practices must "place consumers at the centre of the digital ecosystem and to let them know and control who in the ecosystem gets access to their data" (p. 37). Additionally, the idea for a national Data Privacy Agency is not new. In 2019, Rotenberg and Fitzgerald, the president and policy director of EPIC, respectively, insisted that "the United States urgently needs a Data Protection Agency" (p. 2). The inclusion of a similar such agency in the CPRA indicates that it would be a key addition to a national privacy law. As shown in Figure 3 below, a federal Data Privacy Agency would act as a mediator between consumers, government legislators, and tech companies. This agency would not directly address the issue of consumers having generally weak influence over national laws, but it would help alleviate the burden of policy-makers to keep informed of the quickly advancing technologies involved with data privacy. In 2001, Peha argued that "to get more technologists involved in policy, institutional change may ultimately be required," and the creation of a Data Privacy Agency is a perfect example of such a change (p. 19).

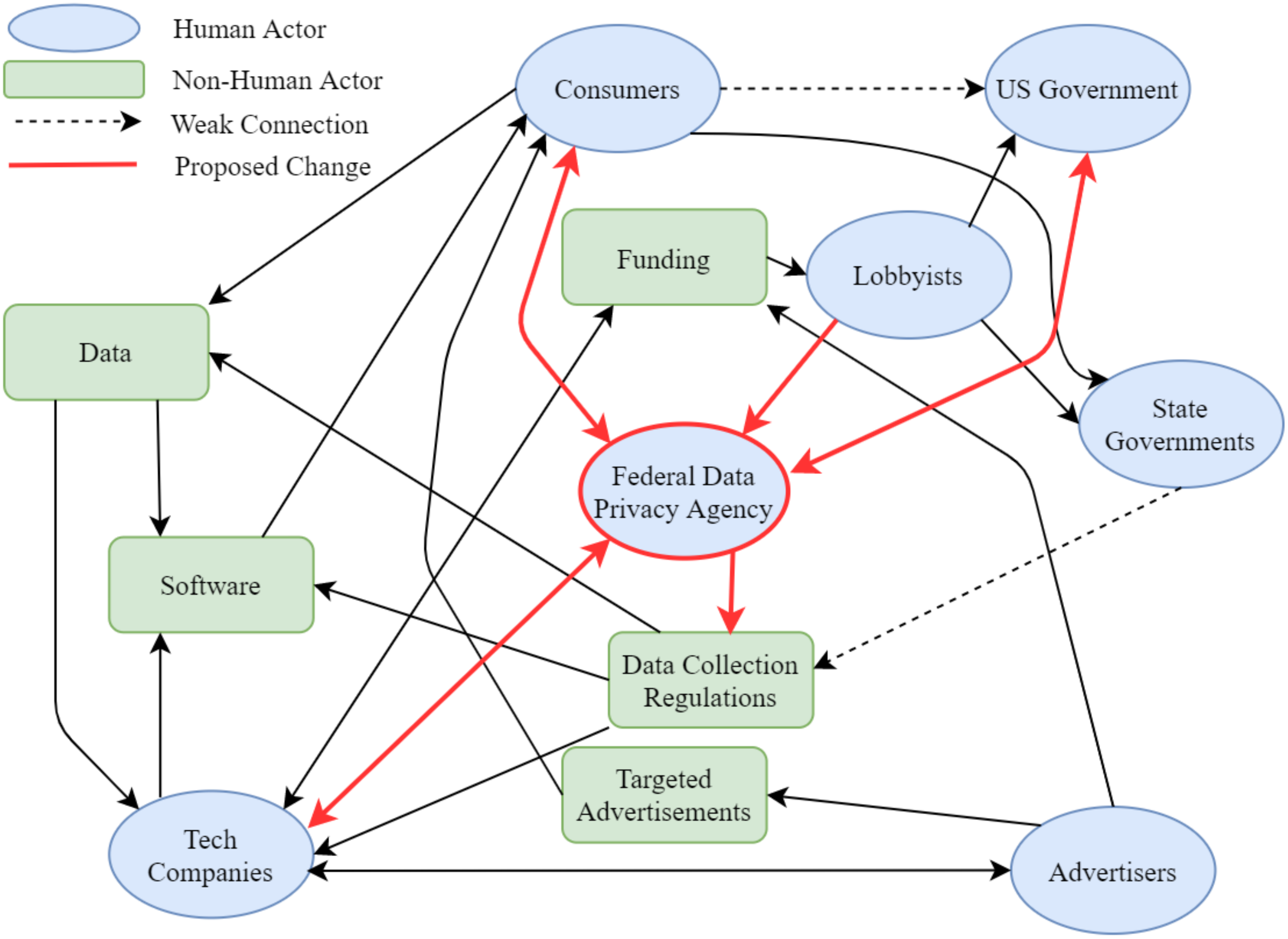

Figure 3. Actor network model of possible future US data collection regulation with Data Privacy Agency. This figure depicts a modified version of the actor network model shown in Figure 1. All of the changes in this model stem from the inclusion of a new federal Data Privacy Agency. (Tufano, 2021c).

HOPE FOR LASTING DIGITAL PRIVACY

Policy-makers have a difficult job when it comes to regulating rapidly changing technology. The wide breadth of issues legislators discuss makes it nigh-impossible to be adequately informed on every topic. In 2018, Spandana Singh, a policy analyst, discussed the failure of Congress to gain useful information from Facebook CEO Mark Zuckerberg when he testified about the Cambridge Analytica scandal, demonstrating the struggle of public officials to have sufficient knowledge of current technologies (para. 1). However, this does not remove the need for digital privacy legislation, nor does it excuse the lack of progress made towards such legislation. By creating stronger channels for citizens to provide input on privacy issues, the burden for lawmakers to be informed about data collection technologies is lessened. Users have a unique knowledge of how data collection interacts with their right to privacy that is critical in determining the path forward for regulations. By following California's example, a federal standard for consumer privacy can be set, and the creation of a federal agency would be the perfect way to prevent further glaring oversights in regulation.

The main limitation of this work is clear; it does not provide a clear path to actually creating data collection legislation. As such, future work to further promote the ideal of digital privacy may benefit from a focus on how national laws have been passed in the face of fierce opposition from lobbyists. The lobbyists should not be ignored, as they represent the interests of many companies, and therefore a significant portion of the economy; however, balancing the needs of corporations with the needs of the general public is critical in promoting general welfare. Studying former national laws that faced opposition may reveal a pathway for the passage digital privacy legislation. Another potentially impactful area to consider is the four data privacy acts that have been proposed in Congress since 2019 (Schuler, 2021, para. 2). An understanding of why these proposals never became laws may illuminate struggles that were not shown in this paper’s examination of the California privacy laws.

REFERENCES

Cressman, D. (2009). A brief overview of Actor-Network Theory: Punctualization, heterogeneous engineering & translation. *Center for Policy Research on Science and Technology*.

De Vynck, G. (2021, June 21). Google set to change how ads track people on the Internet. *The Washington Post*, p. 19.

Duck Duck Go. (2018, March 28). What U.S. adults think about Facebook after Cambridge Analytica. Retrieved from https://spreadprivacy.com/cambridge-analytica/

Electronic Privacy Information Center. (n.d.) *California's Proposition 24.* Retrieved from https://epic.org/state-policy/ca-prop24/

Flitter, E., & Weise, K. (2019, July 29). Capital One data breach compromises data of over 100 million. *The New York Times.* Retrieved from https://www.nytimes.com/

International Association of Privacy Professionals. (2021). *US State Privacy Legislation Tracker* [Table]. Retrieved from https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

Kampmark, B. (2020). The pandemic surveillance state: an enduring legacy of COVID-19. *Journal of Global Faultlines, 7*(1), 59-70. doi:10.13169/jglobfaul.7.1.0059

Kang, C., & McCabe, D. (2021, June 25). Tough road seen for bills that limit tech firms. *The New York Times*, p. 1.

National Society of Professional Engineers. (2019, July). *Code of ethics for engineers.* Retrieved from https://www.nspe.org/resources/ethics/code-ethics

Peha, J. M. (2001). Bridging the divide between technologists and policy-makers. *IEEE Spectrum, 38*(3), 15-19. doi:10.1109/6.908884

Radia, R., & Khurana, R. (2018, May 23). *European Union's General Data Protection Regulation and lessons for U.S. privacy policy.* Retrieved from Competitive Enterprise Institute website: https://cei.org/studies/european-unions-general-data-protection-regulation-and-lessons-for-u-s-privacy-policy/

Rosen, P. M., Madigan, K. J., & Markos, C. A. (2021, March). The California Privacy Rights Act: Understanding California's latest voter-approved consumer data privacy law and its impact on the CCPA. *Orange County Lawyer. 63*(3), 29-32.

Rotenberg, M., & Fitzgerald, C. (2019, December). *Examining Legislative Proposals to Protect Consumer Data Privacy.* Retrieved from Electronic Privacy Information Center website: https://epic.org/testimony/congress/EPIC-SCOM-LegislativePrivacyProposals-Dec2019.pdf

Schuler, K. (2021, January 22). Federal data privacy regulation is on the way – that's a good thing. *International Association of Privacy Professionals.* Retrieved from https://iapp.org/

Sepulveda, D. (2018, October). Put consumers first. *Intermedia. 46*(3), 36-38. Retrieved from https://www.iicom.org/intermedia/

Singh, S. (2018, May 22). Why policy makers need technologists [Blog post]. Retrieved from https://www.newamerica.org/millennials/dm/why-policy-makers-need-technologists/

State of California Department of Justice. (n.d.) *California Consumer Privacy Act (CCPA).* Retrieved from https://oag.ca.gov/privacy/ccpa

Tufano, J. (2021a). *Actor network model of current US data collection regulation*. [Figure 1]. *STS Research Paper: A right to privacy: the intersection of cybersecurity and policy in protecting consumer data* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Tufano, J. (2021b). *Actor network model of data collection regulation in California.* [Figure 2]. *STS Research Paper: A right to privacy: the intersection of cybersecurity and policy in protecting consumer data* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Tufano, J. (2021c). *Actor network model of possible future US data collection regulation with Data Privacy Agency.* [Figure 3]. *STS Research Paper: A right to privacy: the intersection of cybersecurity and policy in protecting consumer data* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Yu, P. (2021). The emergence of surveillance culture: The relationships between Facebook privacy management, online government surveillance, and online political expression. *Journal of Broadcasting & Electronic Media, 65*(1), 66-87. doi:10.1080/08838151.2021.1897816

Zhu, Y., & Chen, H. (2015). Social media and human need satisfaction: Implications for social media marketing. *Business Horizons, 58*(3), 335-345. doi:10.1016/j.bushor.2015.01.006

BIBLIOGRAPHY

Association for Computing Machinery (2018). ACM Code of Ethics and Professional Conduct. Retrieved from https://www.acm.org/code-of-ethics

Barr v. AAPC (2020). Brief of amici curiae Electronic Privacy Information Center et al. in support of petitioners, Barr v. American Association of Political Consultants, Inc., United States Supreme Court No. 19-631.

Beck, J. (2018, June 7). People are changing the way they use social media. *The Atlantic.* Retrieved from https://www.theatlantic.com/

Belvaux, B. (2011, March). The development of social media: Proposal for a diffusion model incorporating network externalities in a competitive environment. *Recherche Et Applications En Marketing (English Version), 26*(3), 7-22. doi:10.1177/205157071102600301

Businesswire. (2019, April 4). IDC forecasts revenues for big data and business analytics solutions will reach $189.1 billion this year with double-digit annual growth through 2022 [Press release]. Retrieved from https://www.businesswire.com/news/home/20190404005662/en/IDC-Forecasts-Revenues-for-Big-Data-and-Business-Analytics-Solutions-Will-Reach-189.1-Billion-This-Year-with-Double-Digit-Annual-Growth-Through-2022

Cressman, D. (2009). A brief overview of Actor-Network Theory: Punctualization, heterogeneous engineering & translation. *Center for Policy Research on Science and Technology.*

De Vynck, G. (2021, June 21). Google set to change how ads track people on the Internet. *The Washington Post,* p. 19.

Electronic Frontier Foundation. (2020, March 19). Are your identification photos in a face recognition database? Retrieved from https://www.eff.org/press/releases/are-your-identification-photos-face-recognition-database

Electronic Privacy Information Center. (n.d.) *California's Proposition 24.* Retrieved from https://epic.org/state-policy/ca-prop24/

Fienberg, H. (2020, September 14). Insights Association joins TCPA challenge at the Supreme Court: Insights Association. Retrieved from https://www.insightsassociation.org/article/insights-association-joins-tcpa-challenge-supreme-court

Flitter, E., & Weise, K. (2019, July 29). Capital One data breach compromises data of over 100 million. *The New York Times.* Retrieved from https://www.nytimes.com/

Grosz, B. J., Grant, D. G., Vredenburgh, K., Behrends, J., Hu, L., Simmons, A., & Waldo, J. (2019). Embedded EthiCS: Integrating ethics across CS education. *Communications of the ACM, 62*(8), 54-61. doi:10.1145/3330794

Hinds, J., Williams, E. J., & Joinson, A. N. (2020). "It wouldn't happen to me": Privacy concerns and perspectives following the Cambridge Analytica scandal. *International Journal of Human-Computer Studies, 143,* Article 102498. doi:10.1016/j.ijhcs.2020.102498

Internet Association. (2018, June 28). Statement on the enactment of California privacy legislation. Retrieved from https://internetassociation.org/news/statement-enactment-california-privacy-legislation/

International Association of Privacy Professionals. (2021). *US State Privacy Legislation Tracker* [Table]. Retrieved from https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

Kampmark, B. (2020). The pandemic surveillance state: an enduring legacy of COVID-19. *Journal of Global Faultlines, 7*(1), 59-70. doi:10.13169/jglobfaul.7.1.0059

Kang, C., & McCabe, D. (2021, June 25). Tough road seen for bills that limit tech firms. *The New York Times*, p. 1.

National Society of Professional Engineers. (2019, July). *Code of ethics for engineers.* Retrieved from https://www.nspe.org/resources/ethics/code-ethics

McCallion, J. (2017, February 2). Data breach news: Most UK banks don't believe they can detect a data breach. *ITPro.* Retrieved from https://www.itpro.co.uk/

Peha, J. M. (2001). Bridging the divide between technologists and policy-makers. *IEEE Spectrum, 38*(3), 15-19. doi:10.1109/6.908884

Radia, R., & Khurana, R. (2018, May 23). *European Union's General Data Protection Regulation and lessons for U.S. privacy policy.* Retrieved from Competitive Enterprise Institute website: https://cei.org/studies/european-unions-general-data-protection-regulation-and-lessons-for-u-s-privacy-policy/

Rosen, P. M., Madigan, K. J., & Markos, C. A. (2021, March). The California Privacy Rights Act: Understanding California's latest voter-approved consumer data privacy law and its impact on the CCPA. *Orange County Lawyer. 63*(3), 29-32.

Rotenberg, M., & Fitzgerald, C. (2019, December). *Examining Legislative Proposals to Protect Consumer Data Privacy.* Retrieved from Electronic Privacy Information Center website: https://epic.org/testimony/congress/EPIC-SCOM-LegislativePrivacyProposals-Dec2019.pdf

Schuler, K. (2021, January 22). Federal data privacy regulation is on the way – that's a good thing. *International Association of Privacy Professionals.* Retrieved from https://iapp.org/

Sepulveda, D. (2018, October). Put consumers first. *Intermedia. 46*(3), 36-38. Retrieved from https://www.iicom.org/intermedia/

Singh, S. (2018, May 22). Why policy makers need technologists [Blog post]. Retrieved from https://www.newamerica.org/millennials/dm/why-policy-makers-need-technologists/

State of California Department of Justice. (n.d.) *California Consumer Privacy Act (CCPA).* Retrieved from https://oag.ca.gov/privacy/ccpa

Tufano, J. (2021a). *Actor network model of current US data collection regulation*. [Figure 1]. *STS Research Paper: A right to privacy: the intersection of cybersecurity and policy in protecting consumer data* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Tufano, J. (2021b). *Actor network model of data collection regulation in California.* [Figure 2]. *STS Research Paper: A right to privacy: the intersection of cybersecurity and policy in protecting consumer data* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Tufano, J. (2021c). *Actor network model of possible future US data collection regulation with Data Privacy Agency.* [Figure 3]. *STS Research Paper: A right to privacy: the intersection of cybersecurity and policy in protecting consumer data* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Vakil, S., & Higgs, J. (2019). It's about power: A call to rethink ethics and equity in computing education. *Computers & Applied Sciences Complete*, *62*(3), 31-33. doi:10.1145/3306617

Verizon. (2020). *Data breach investigations report*. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Villas-Boas, J. M. (2004). Consumer learning, brand loyalty, and competition. *Marketing Science, 23*(1), 134-145. doi:10.1287/mksc.1030.0044

Washington Post. (n.d.). Gerrit De Vynck. Retrieved from https://www.washingtonpost.com/people/gerrit-de-vynck/

Yu, P. (2021). The emergence of surveillance culture: The relationships between Facebook privacy management, online government surveillance, and online political expression. *Journal of Broadcasting & Electronic Media*, *65*(1), 66-87. doi:10.1080/08838151.2021.1897816

Zhu, Y., & Chen, H. (2015). Social media and human need satisfaction: Implications for social media marketing. *Business Horizons*, *58*(3), 335-345. doi:10.1016/j.bushor.2015.01.006

Zuckerberg, M. (2019, March 06). A privacy-focused vision for social networking. Retrieved from https://www.facebook.com/notes/mark-zuckerberg/a-privacy-focused-vision-for-social-networking/10156700570096634/