Harvard Model Congress
Boston 2024

DATA PRIVACY

By Sharon Tang

INTRODUCTION

As the world becomes more reliant on the internet and **big tech**, more consumer data is stored online. This has created an environment of high risk for compromised data relating to bank information, social security numbers, consumer preferences, and other personal information. In fact, in 2022 alone, over 422 million individuals were impacted by online data compromises such as data leakage, exposure, and breaches ("Annual", 2005).

Big Tech *– the most dominant companies in the tech industry, including Google, Apple, and Microsoft.*

Data privacy is a crucial issue. Although significant advancements have been made in the past decade, much work is still necessary. There are still major problems in the healthcare, consumer goods, and political sphere. These problems have been worsened by the increase in social media usage fostered by the pandemic and the rise of generative AI.

This issue is one that should be addressed by the Senate Homeland Security Committee, as it threatens the existence of American citizens at home and abroad. Thus, this briefing seeks to explore the different facets of this complex issue and the possible avenues of legislation that Congress may pursue to protect US consumers and businesses from modern data privacy concerns.

EXPLANATION OF THE ISSUE

Historical Development

The origins of data privacy are rooted in healthcare and finance, where patient and client data has historically been securely stored prior to the rise of the internet (Holdren, 2014). This data was protected by acts like the Health Insurance Portability and Accountability Act of 1996 (HIPAA) which guaranteed doctor-patient confidentiality ("Health", 2022).

The rise of the internet in the 1990s and 2000s led to the federal government pushing for data privacy legislation on a broader scale. The **Children's Online Privacy Protection Act of 1998** (COPPA) aimed to protect the identities of children under 13 ("Children's", 2013).

Also in the 90s and 2000s, some of the first social media apps took form: Six Degrees was founded in 1997, Friendster in 2001, and Myspace in 2003 ("The Evolution", n.d.). They were followed by larger social media apps like Facebook in 2004 and Twitter in 2006 ("The Evolution", n.d.). Slowly, people began to share their lives and personal information online through these social media applications on a large scale.

In contemporary times, at least seven in ten Americans use a form of social media, making it a core facet of daily life ("Social", 2021). The difference between pre-internet data and current data is the sheer scope of it. Big tech collects all forms of consumer data, from phone numbers, messages, searches, addresses, passwords, and payment information (Vigderman, 2023).

Scope of the Problem

Currently, data privacy has a wide array of short-term and long-term problems. Such problems include the rise of data breaches, government surveillance, social media, health data privacy, international data transfers and emerging technologies like generative AI.

Data Breaches and Privacy

As discussed earlier, big tech has risen in influence and scope over the last twenty years. Significantly, this rise has led to a rise in data breaches, both in severity and frequency. These cybercriminals target both consumer and business information, stealing from the government and large corporations.

The largest modern data breach occurred to social media corporation Yahoo!, when a team of Russian hackers pulled over three billion users' data (Chin, 2023). Similarly, Microsoft suffered a data breach on its Microsoft Exchange servers, impacting over 60 thousand companies (Chin, 2023). Social media applications like Facebook and LinkedIn have also suffered from these data breaches, like the Facebook-Cambridge Analytica controversy revealed in 2018 (Chin, 2023). In the 2010a, Cambridge Analytica illegally stole and sold the data of over fifty million Facebook accounts through a loophole on a third-party quiz application that was linked with Facebook (Chin, 2023).

At least seven in ten Americans use a form of social media.

The issue with data breaches is that they are extremely hard to prevent. Cybercriminals successfully attack weak points in data and come from all parts of the globe.

Surveillance and Government Access to Data

Tech companies are allowed to collect large sums of valuable individual data when determined valuable to the justice department. There has been a debate between national security and individual privacy. What information should be disclosed to officials in a trial and non-trial setting? Of course, sharing more information would help streamline the justice department, helping put more guilty people behind bars. However, many worry that giving the government too much information could transition the United States to a **surveillance state**.

Surveillance State *– an country where the government undertakes in pervasive surveillance of many of its citizens.*

Currently, authorities can access basic user data like IP addresses, account names, and billing information by issuing a **subpoena** (Nicas, 2021). Authorities have also partnered with tech conglomerates Microsoft and Apple to access phone records and texts, although Apple claims it only fulfills 44 percent of the requests while Microsoft fulfills around 50 percent (Nicas, 202). On the other hand, companies like Meta and Google report to fulfill close to 80 percent of authorities' requests (Nicas, 202).

However, there is also data that is inaccessible to authorities, known as end-to-end encryption. This is when the data is only available to the sender and the recipient, therefore blocking company access to unencrypted data. The issue arises when law enforcement officials attempt to hack into phones to bypass the encryptions and gain access to the data.

Social Media

Subpoena*– a written piece issued by a court, to compel testimony by a witness or production of evidence under a penalty for failure.*

The fight between big social media apps like Tiktok and the US government has been at the forefront of many current conversations around technology and privacy. This is due to the concern that social media companies sell American user data to other companies and/or countries' governments. There is also the concern that social media can push propaganda and fake news via another government, internet trolls, or extreme political groups.

Congress has written many pieces of legislation on this topic, including the Deterring America's Technological Adversaries (DATA) Act proposed by Rep. Michael T. McCaul (R-Texas) and the Restricting the Emergency of Security Threats that Risk Information and Communications Technology (RESTRICT) Act proposed by Sen. Mark Warner (D-Va.) (Davis, 2023). However, this has drawn criticism, as some say that the bills were written out of xenophobic and anti-Chinese sentiments.

Twitter was also recently in the news after being acquired by billionaire and CEO of SpaceX and Tesla Elon Musk. Musk made sweeping changes after taking over the company, including mass layoffs and a hasty revamp of the platform's services, which has led to an undermining of the company's previous commitment to data protection (Zahn, 2023).

Health Data Privacy

The new norm is to have health records digitized, and many hospitals are making patient records available from a computer or mobile phone. Protecting and keeping patient data confidential from prying parties like in-laws, employers, or even the government is critical to health data privacy. The legislative basis for health data privacy is HIPPA, which limits what information hospitals and health professionals can share ("AMA", 2023). However, many online platforms storing health data are not restricted like hospitals, making them more prone to data leakage and risk. While large-scale research on disease analysis on medical records and genomic information could lead to better and faster treatment, it could also lead to inappropriate disqualification for insurance or jobs (Holdren, 2014).

With the repeal of the Supreme Court decision Roe v. Wade, the issue of data privacy has become more pressing. In Nebraska, the prosecutors in an illegal abortion case used private Facebook data in their case, gained through a subpoena (Cox, 2022). In response to the judicial utilization of menstrual data, healthcare apps like Flo, a period tracker mobile app, have rolled out "anonymous mode," which allows users to use the application without identifying information like names and email addresses (Pifer, 2022).

Emerging Technologies

Open AI's ChatGPT 4 and ChatGPT 5 are two forms of generative AI.
LogoWiki

Generative AI like ChatGPT has grown in popularity, with 100 million users and 1.8 billion site visits. Instead of detecting patterns or following orders, generative AI is designed to produce new content. All AI models take in large amounts of data, much of it being private information; once that data is fed in, it is hard to take it out. This becomes an issue when data is deleted or hacked into. Creating solutions to pre-empt the consequences of this emerging field is necessary (Korner, 2023).

Congressional Action

The Deterring America's Technological Adversaries (DATA) Act was introduced to the 118th Congress by Rep. Michael T. McCaul (R-TX), requiring federal action towards protecting sensitive personal data of US individuals, especially in relation to China (HR 1153). Similarly, the Restricting the Emergency of Security Threats that Risk Information and Communications Technology (RESTRICT) Act helps "identity and mitigate foreign threats to information and communications technology products and services (e.g., social media applications) (S 686). These acts were created as protective responses to social media collecting private information.

The Online Privacy Act of 2023 was proposed by Rep. Anna Eshoo (D-CA) to provide better guidelines related to the

privacy of personal information (HR 2701). Likewise, the Setting an American Framework to Ensure Data Access, Transparency, and Accountability Act (SAFE DATA Act) proposed by Sen. Roger Wicker (R-MS) "establishes various requirements relating to the collection of consumer data, data transparency and security, and corporate accountability, including limiting the amount of data a covered entity may collect" (S 2499).

Congress has taken a deep interest in data privacy for the last couple of years, creating many bills and laws. However, problems still arise from the changing landscape of this issue, as the online world continues to expand and evolve.

Other Policy Action

A major piece of state legislation passed relating to data privacy is the California Consumer Privacy Act, passed in 2018 and amended in 2020. This act gives California residents additional rights over their personal information and imposes restrictions and obligations for businesses that handle their data ("California", 2023). Many consider this to be a good starting point for creating more comprehensive federal legislation.

President Joe Biden also implemented a variety of executive orders regarding data privacy. In March 2022, President Biden signed an executive order to implement the European Union-US Data Privacy Framework in response to the EU's new privacy laws ("President", 2022). This executive order adds further safeguards for US signal intelligence activities and new regulations for the US regarding EU's new privacy laws.

IDEOLOGICAL VIEWPOINTS

Conservative View

Although Conservatives generally believe in the free market and allowing business to make their own decisions, individual privacy and national security highlight core tenets of the conservative platform (Laslo, 2023). Conservatives will likely prioritize individual and family privacy issues while remaining passive in the market and business relations. Regarding national security, Conservatives are also more likely to believe in the benefits of increasing aggression abroad, especially toward China, and using data distribution to assist law enforcement (Laslo, 2023).

The Conservative stance on big tech also tends to correlate with how young a senator is. Older Senators tend to value anti-regulation and the free market, while younger Senators tend to lean toward regulation to protect individual rights (Laslo, 2023).

President Joe Biden

Liberal View

Liberals also believe it is necessary to pass bills increasing data privacy for US citizens. The Liberal platform is also interested in passing antitrust laws in the tech industry, as "big tech" has a much higher market share in their industry than typically (Laslo, 2023). They are also less likely to want to use data in national security and healthcare cases due to prioritization of protecting individuals' rights.

AREAS OF DEBATE

General Data Protection Regulation *– the new EU data protection law targeting consumers.*

Solutions for the current data privacy issue are multi-faceted. Important areas of debate that can arise while discussing the implications of data privacy and attitudes towards big tech and rising technologies can include strengthening individual privacy laws, increasing the purview of domestic regulating agencies, breaking up big tech companies, promoting public education, and promoting state legislation.

Strengthening Individual Privacy Laws

The most common solution proposed regarding data privacy is strengthening individual privacy laws. There are many ways to do this, including increasing people's rights to be informed, increasing erasure, and bettering access; having more explicit consent laws; and streamlining procedures for data breaches (Wolford, n.d.). A lot of officials are looking towards the European Union's new data protection law, **General Data Protection Regulation** (GDPR), as a framework for implementing privacy regulations at a national scale as well (Wolford, n.d.).

Data protection is important because it allows individuals to be more informed and prevents business malpractice. In addition, increasing individual privacy laws is a necessary foundation for other potential solutions. It also streamlines the process when a business or individual breaks the law, as there is a clear metric on what the courts should do. The drawback of adding these privacy laws is that it makes it more difficult for businesses to operate efficiently.

Political Perspectives on this Solution

Both Conservatives and Liberals agree that some form of individual privacy law is necessary. However, they have some disagreement on how strict these laws should be. When weighing individual privacy and business practices, Conservatives generally are in support of prioritizing business operation over individual privacy, while Liberals are in support of helping individuals over protecting the free market.

Strengthening Regulating Agencies

Currently, a few regulatory agencies oversee enforcing privacy regulations, investigating data breaches, and holding companies accountable for data handling practices. One of these organizations is the Federal Trade Commission (FTC). This agency helps prevent unfair and predatory business practices and informs consumers on how to avoid scams and fraud ("Federal", n.d.). Giving these agencies more power and jurisdiction would give them more flexibility to tackle the modernizing data privacy landscape. It will also help hold companies more accountable, whether that be a financial institution, tech company, or small business.

The drawback to this solution is that once you give an agency more power, it is hard to reign that back in if necessary. In addition, giving an agency more leeway will require the federal government to give them more funding.

In 2021, the five biggest technology companies made more than $1.4 trillion in revenue, on par with Brazil's total GDP.

Political Perspectives on this Solution

Conservatives generally are against strengthening regulating agencies as a core tenet of conservative ideology is minimizing government intervention. Conservatives believe that educating individuals on how to protect themselves is a fairer practice than weighting the government with the responsibility.

Liberals generally believe in expanding government agencies as it provides direct support to their constituents. They also believe that expanding the agency will give it more flexibility to achieve its goals.

Breaking Up Big Tech

In 2021, the five biggest technology companies made more than $1.4 trillion in revenue, on par with Brazil's total GDP (Ang, 2022). Amazon accounts for over 40 percent of all e-commerce sales in the US, while Google consists of over 90 percent of all internet searches (Rainey, 2019).

The existence and regulation of big corporations is not new to the United States' history. The Sherman Antitrust Act of 1890 and the Clayton Antitrust Act of 1914 helped lay the groundwork for preventing monopolies and trusts (Rainey, 2019).

The reason for breaking up large tech companies, like breaking Meta's conglomerate into the smaller companies of Facebook, Instagram, and WhatsApp, is to help increase competition and innovation in the industry. Many large companies that have attempted to merge have been blocked by these antitrust laws, like the AT&T/T-Mobile merger in 2011 (O'Brien, n.d.). Other companies have been pushed to break up like Standard Oil (Reese, 2019)

On the other hand, many of these tech companies are only effective due to their **economies of scale** (Niyazov, 2020). Hence, breaking up would reduce these companies' effectiveness.

Political Perspectives on this Solution

People across political party affiliation support breaking up big tech, with people with more extreme left or right views being more vocal (Stewart, 2019).

Conservatives generally believe that big tech should be broken up due to the inherent bias present on many of these businesses' social media platforms (Stewart, 2019). By limiting the power of big tech, it will create an environment where people can more easily formulate their opinions.

Liberals generally believe big tech should be broken up due to their data collection policies and their large market share.

Promoting Education

The Senate can also encourage education programs for the public on data privacy, including their risks, rights, and best practices. These programs can include public awareness campaigns, school curricula, and free online materials. It could also be tailored towards helping businesses teach their employees best practices (Sander, 2022). Through highlighting education, the general population can become better equipped to solve the crisis.

There are not that many drawbacks to this solution, but a major criticism is that promoting education alone will not solve this issue. This solution should be paired with other ideas to create a comprehensive approach to addressing the crisis.

Political Perspectives on this Solution

Conservatives and Liberals both believe in educating the population and providing better data privacy resources. Conservatives believe that this is a cost-efficient way to reach a large audience without increasing the size of government, while Liberals believe it is a good starting point in making sure the general population is cognizant of the risks of data privacy.

Empowering State Legislation

Opinions on how to tackle data privacy vary greatly on a state level, and as such, many different state bills have passed tackling the subject. As discussed, prior, California has enacted stricter state laws through its **California Consumer Privacy Act** ((“California”, 2023). Four other states, Colorado, Connecticut, Utah, and Virginia have enacted similar consumer data privacy laws that give consumers rights over their personal information and impose restrictions and obligations for businesses that handle their data (“State”, 2022). Some variations of this law also require websites from businesses or online services to post a privacy policy listing the types of personal information collected (“State”, 2022).

The benefit of empowering state legislation is that these laws can be much more specific, tailored to the issues faced by residents in that state. This eliminates the criticism of privacy laws being too general. The drawback to this solution is that it pushes the problem to another group of authorities who also may not take the necessary education or know the proper actions to prevent the crisis.

Political Perspectives on this Solution

Conservatives support this position because many conservatives believe in decreasing the federal government's role. Although Conservatives believe the data privacy issue is a pressing one that needs attention, many also believe that the states can deal with this issue in a detailed manner.

Liberals oppose shifting efforts to states because states have varying preparedness to tackle data privacy problems and reducing strict federal regulations can lead to businesses taking advantage of the state-wide system.

BUDGETARY CONSIDERATIONS

In 2023, the Department of Homeland Security was allocated 101 billion dollars by the Biden-Harris administration to conduct its total yearly programs (Mayorkas, 2023). This number is expected to rise to 103 billion in 2024, a 1.5 percent increase (Mayorkas, 2023). This allocation includes all 17 of the department's subsidiaries.

CONCLUSION

In its upcoming session, the Senate Committee on Homeland Security will be tasked with addressing the contemporary data privacy crisis. Developing comprehensive policy solutions that allow for a fair system for consumers and businesses is essential. Should the government continue to take anti-trust action against social media giants like Meta, Twitter, and Tiktok? What data should be available to authorities when they request it? How should Congress tackle emerging technologies?

In preparation for the conference, delegates should read through this briefing and continue to be updated on current events and policy proposals from all sides of the aisle, as this briefing is in no way comprehensive of all the issues occurring in this expansive topic. Additionally, in the time passed since the publishing of this briefing, more information is likely to be available about this issue. While drafting legislation, delegates should consider various factors such as social implications, fiscal limitations, and feasibility, as well as if their policies align with the views of their constituents. Delegates are

encouraged to develop creative and multi-faceted solutions and should conduct independent research in addition to reading this briefing.

GUIDE TO FURTHER RESEARCH

The Department of Homeland Security was allocated 101 billion dollars.

This briefing offers a synopsis of the situation of the current data privacy issue, but it is no way comprehensive of all the historic implications and possible solutions. To gain a full understanding of the situation, it is essential for delegates to expand upon this research further through outside supplemental research. Additionally, the situation is rapidly changing; because of that, delegates should keep up to date on new developments in the weeks prior to the conference.

When doing research, adhere to reputable news sources such as *Wall Street Journal* or *Politico*. Also keep up to date with government resources such as congress.gov for a comprehensive list of introduced bills relating to data privacy. Overall, it is crucial to use this briefing as a launching pad for your own research.

GLOSSARY

Big Tech – the most dominant companies in the tech industry, including Google, Apple, and Microsoft.

California Consumer Privacy Act – act gives California residents additional rights over their personal information and imposes restrictions and obligations for businesses that handle their data.

Children's Online Privacy Protection Act of 1998 – an act passed by Congress aimed to protect the identities of children under 13.

Economies of Scale – as businesses get larger and increase production, they are able to reap specific benefits.

General Data Protection Regulation – the new EU data protection law targeting consumers.

Subpoena – a written piece issued by a court, to compel testimony by a witness or production of evidence under a penalty for failure.

Surveillance State – an country where the government undertakes in pervasive surveillance of many of its citizens.

BIBLIOGRAPHY

"AMA health data privacy framework." *AMA*. 2023. https://www.ama-assn.org/delivering-care/patient-support-advocacy/ama-health-data-privacy-framework.

Ang, Carmen. "How Do Big Tech Giants Make Their Billions?" *Visual Capitalist*. 25 April 2022. Web. https://www.visualcapitalist.com/how-big-tech-makes-their-billions-2022/.

"Annual number of data compromises and individuals impacted in the United States from 2005 to 2022." *Statistica*. 2022. Web. https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

"California Consumer Privacy Act (CCPA)." *California Attorney General*. 10 May 2023. https://oag.ca.gov/privacy/ccpa.

"Children's Online Privacy Protection Rule." *National Archives*. https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-312.

Chin, Kyle. "Biggest Data Breaches in US History." *UpGuard*. 28 May 2023. Web. https://www.upguard.com/blog/biggest-data-breaches-us.

Cox, David. "How overturning Roe v Wade has eroded privacy of personal data." *BMJ*. 26 August 2022. https://doi.org/10.1136/bmj.o2075.

Davis, Darreonna. "Government TikTok Bans: Exploring the Global Impact." *Forbes*. 6 June 2023. Web. https://www.forbes.com/sites/darreonnadavis/2023/06/06/government-tiktok-bans-exploring-the-global-impact/?sh=61f1e05570c0.

"Federal Trade Commision." *Usa.gov*. N.d. https://www.usa.gov/agencies/federal-trade-commission.

"Health Insurance Portability and Accountability Act of 1996 (HIPAA)." *Center for Disease Control and Prevention*. 27 June 2022. Web. https://www.cdc.gov/phlp/publications/topic/hipaa.html.

HR 1153. "DATA Act." *Congress.gov*. 28 February 2023. Web. https://www.congress.gov/bill/118th-congress/house-bill/1153?q=%7B%22search%22%3A%5B%22Deterring+Americas+Technological+Adversaries+%28DATA%29+Act%22%5D%7D&s=3&r=1.

HR 2701. "Online Privacy Act of 2023." *Congress.gov*. 19 April 2023. Web. https://www.congress.gov/bill/118th-congress/house-bill/2701/text?s=5&r=1&q=%7B%22search%22%3A%5B%22Online+Privacy+Act%22%5D%7D.

Holdren, John. "Report to the President. Big Data and Privacy: A Technological Perspective." *Executive Office of the President*. May 2014. Web. https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

Korner, Katherina. "Generative AI: Privacy and tech perspectives." *IAPP*. 28 March 2023. Web. https://iapp.org/news/a/generative-ai-privacy-and-tech-perspectives/.

Laslo, Matt. "The Political Theater Behind the Bipartisan Data Privacy Push." *Wired*. 8 February 2023. Web. https://www.wired.com/story/sotu-privacy-congress-biden/.

Mayorkas, Alejandro. "FY 2024 Budget in Brief." *Department of Homeland Security*. 2023. Web. https://www.dhs.gov/sites/default/files/2023-03/DHS%20FY%202024%20BUDGET%20IN%20BRIEF%20%28BIB%29_Remediated.pdf.

Nicas, Jack. "What Data About You Can the Government Get From Big Tech?" *New York Times*. 14 June 2021. Web. https://www.nytimes.com/2021/06/14/technology/personal-data-apple-google-facebook.html.

Niyazov, Sukayl. "Don't Break Up Big Tech." *Medium*. 27 February 2020. Web. https://medium.com/swlh/dont-break-up-big-tech-fb17590f30f1.

O'Brien, Shauna. "5 Big Mergers and Their Battle with Antitrust Laws." *Dividend.com*. n.d. https://www.dividend.com/how-to-invest/5-major-antitrust-mergers/.

Pifer, Rebecca. "Period tracker Flo launches anonymous mode amid post-Roe privacy concerns." *Heathcare Dive*. 15 September 2022. https://www.healthcaredive.com/news/flo-anonymous-mode-period-tracker-app-abortion-roe/631926/.

"President Biden Signs Executive Order to Implement the European Union-U.S. Data Privacy Framework." *The White* House. 7 October 2022. Web. https://www.whitehouse.gov/briefing-room/statements-releases/2022/10/07/fact-sheet-president-biden-signs-executive-order-to-implement-the-european-union-u-s-data-privacy-framework/.

Rainey, Toria. "Is it Time to Break Up Big Tech?" *Questrom The BU Business Magazine*. 2019. Web. https://www.bu.edu/questrom-magazine/fall-2019/is-it-time-to-break-up-big-tech/.

Reese, Frederick. "15 companies the U.S. government tried to break up as monopolies." *Stacker*. 22 October 2019. https://stacker.com/business-economy/15-companies-us-government-tried-break-monopolies.

S 2499. "SAFE DATA Act." *Congress.gov*. *28 July 2021*. Web. https://www.congress.gov/bill/117th-congress/senate-bill/2499.

S 686. "RESTRICT Act." *Congress.gov*. 7 March 2023. Web. https://www.congress.gov/bill/118th-congress/senate-bill/686?q=%7B%22search%22%3A%5B%22Restricting+the+Emergency+of+Security+Threats+that+Risk+Information+and+Communications+Technology+%28RESTRICT%29+Act%22%5D%7D&s=4&r=1.

Sander, Alexa. "Here's Why Data Privacy in Schools Should be a Priority in Your District." 17 February 2022. Web. https://managedmethods.com/blog/data-privacy-in-schools/.

"Social Media Fact Sheet". *Pew Research Center*. 7 April 2021. Web. https://www.pewresearch.org/internet/fact-sheet/social-media/.

"State Law Related to Digital Privacy." *National Conference of State Legislatures*. 7 June 2022. https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy.

Stewart, Emily. "Poll: Two-thirds of Americans want to break up companies like Amazon and Google." *Vox*. 18 September 2019. Web. https://www.vox.com/policy-and-

politics/2019/9/18/20870938/break-up-big-tech-google-facebook-amazon-poll.

"The Evolution of Social Media: How Did It Begin, and Where Could It Go Next?" *Maryville Univeristy*. n.d. https://online.maryville.edu/blog/evolution-social-media/.

Vigderman, Aliza. " The Data Big Tech Companies Have On You." *Security.org*. 6 February 2023. Web. https://www.security.org/resources/data-tech-companies-have/.

Wolford, Ben. "What is GDPR, the EU's new data protection law?" n.d. https://gdpr.eu/what-is-gdpr/.

Zahn, Max. "Senators warn Twitter, Elon Musk over alleged 'disregard' for data privacy." *ABC News*. 5 June 2023. Web. https://abcnews.go.com/Business/senators-warn-twitter-elon-musk-alleged-disregard-data/story?id=99838319