

2021

Era of Accelerating Digital Convergence: Security, Surveillance, Data, Privacy, Big Tech, and Politics

John Taschner

Follow this and additional works at: <https://digitalcommons.wcl.american.edu/auilr>



Part of the [International Law Commons](#), and the [Internet Law Commons](#)

Recommended Citation

Taschner, John (2021) "Era of Accelerating Digital Convergence: Security, Surveillance, Data, Privacy, Big Tech, and Politics," *American University International Law Review*: Vol. 36: Iss. 4, Article 2.

Available at: <https://digitalcommons.wcl.american.edu/auilr/vol36/iss4/2>

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University International Law Review by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.

ERA OF ACCELERATING DIGITAL CONVERGENCE: SECURITY, SURVEILLANCE, DATA, PRIVACY, BIG TECH, AND POLITICS

JOHN TASCHNER *

I. INTRODUCTION	774
II. UNITED STATES HISTORY WITH DATA SURVEILLANCE PRACTICES	783
A) DATA SURVEILLANCE UNDER PRESIDENT GEORGE W. BUSH'S ADMINISTRATION	784
B) DATA SURVEILLANCE UNDER PRESIDENT BARACK OBAMA'S ADMINISTRATION	787
C) DATA SURVEILLANCE UNDER PRESIDENT DONALD TRUMP'S ADMINISTRATION	792
D) DATA SURVEILLANCE UNDER PRESIDENT JOSEPH BIDEN'S ADMINISTRATION	794
E) UNITED STATES LAW ENFORCEMENT AGAINST CYBER WARFARE	797
III. GLOBAL LEGISLATION ON PRIVACY AND DATA COLLECTION	801
A) AMERICAN LEGISLATIVE BACKGROUND ON PRIVACY CONCERNS	802
B) GLOBAL LEGISLATION ON PRIVACY	806
IV. ONLINE SECURITY AND SURVEILLANCE HAPPENING MORE FREQUENTLY AND WITH GREATER INTENSITY	810
A) INTERNET SURVEILLANCE REACHES ARE INFRINGING ON CONSTITUTIONAL RIGHTS	810
B) SOCIAL MEDIA: THE MODERN WEAPON	814

* John Taschner, New York University. The author thanks Sherwet Witherington, Ruslan Klafehn, Mohammed Caudhry, Grace Kim, William Wetter, Daniel Atchue, and David Goad for their legal scholarship and invaluable contributions.

V. THE AGE OF SURVEILLANCE CAPITALISM AND MODERN TECHNOLOGY HERE TO STAY	817
A) AMAZON'S ROLE IN THE MARKETPLACE DURING COVID-19	818
B) THE LURKING DANGERS OF THE CYBERSPACE	820
C) ARE THERE LIMITS TO INCREASING INNOVATION?	822
VI. LANDMARK LEGISLATION HAPPENING FOR CYBERSPACE THAT WILL LIMIT REACH	824
A) TECH TITANS FACING SCRUTINY OVER GROWING MONOPOLIZATION OF THE INTERNET MARKETS	825
B) RELATIONSHIP BETWEEN BIG TECH AND U.S FEDERAL GOVERNMENT	827
VII. CONCLUSIONS	828
A) THE POLITICS OF TECHNOLOGY	829
B) EXTENT OF DATA COLLECTIONS INTERNATIONALLY AND DOMESTICALLY	833
C) RECOMMENDATIONS FOR PRIVATE LIVING IN A PUBLIC WORLD	837

I. INTRODUCTION

Thirty-two percent of surveyed tech executives said that defining a national cybersecurity protocol should be the top priority for the Biden administration and Congress.¹ While the benefits that technology offers the world have linked people closer than what was ever thought feasible, the potential for leaks, cyberterrorism, lack of privacy, and security issues are rapidly expanding at an unstoppable rate.² As

1. Riley de León, *50% Of U.S. Tech Execs Say State-Sponsored Cyber Warfare Their Biggest Threat: CNBC Survey*, CNBC (Dec. 17, 2020, 10:15 AM), <https://www.cnbc.com/2020/12/17/50percent-of-tech-execs-say-cyber-warfare-biggest-threat-cnbc-survey.html>.

2. See Camino Kavanagh, *New Tech, New Threats, and New Governance Challenges: An Opportunity to Craft Smarter Responses?*, 1–2 (2019) (unpublished manuscript) (on file with Carnegie Endowment for International Peace) (explaining technological advances have a disruptive nature creating cyber vulnerabilities).

personal privacy takes a back seat to collective convenience, cybersecurity and the continuously expanding role of major tech companies in the world are rapidly becoming some of the largest and most important topics facing modern society.³

With constantly increasing advances in technological capabilities, the new power players of the world are shifting away from individual countries towards tech giants like Facebook, Twitter, and Amazon.⁴ This relatively untapped power is seemingly limitless, and yet to be proven as either a definitively positive or negative change in history. There are quite literally billions of users on social media websites, which demonstrates the extensively interconnected nature of the modern human race.⁵ Despite this, it has also been increasingly found that “institutions have largely failed to address these technologies’ cybersecurity risks, [a]nd that is in large part because they have failed to address—and have even exacerbated—the moral hazard inherent in making and selling connected technologies.”⁶

These technologies have major risks to the cybersecurity of the nation, but effective monitoring continuously eludes the majority of big tech companies.⁷ There is no such thing as an “innocent search” anymore.⁸ Every search and posting down to the individual keystrokes

3. See *id.* (discussing the ways technology has outpaced expectations and the rapid nature of the industry calls for expedited response).

4. See *id.* (describing the need for governments to act while acknowledging the complex nature of cross-border solutions to global companies).

5. See generally *Global Social Media Stats*, DATAREPORTAL, <https://datareportal.com/social-media-users> (last visited Mar. 12, 2021) (citing data for billions of users worldwide).

6. Jeffrey L. Vagle, *Cybersecurity and Moral Hazard*, 23 STAN. TECH. L. REV. 71, 71 (2020) (“Yet our institutions have largely failed because they have failed to address—and have even exacerbated—the moral hazard inherent in making and selling technologies.”).

7. See Tom Huddleston Jr., *Bill Gates: ‘Government Needs to Get Involved’ to Regulate Big Tech Companies*, CNBC (Oct. 17, 2019), <https://www.cnbc.com/2019/10/17/bill-gates-government-needs-to-regulate-big-tech-companies.html> (discussing how the largest tech companies remain unregulated despite the need for government involvement, according to Bill Gates).

8. See generally Aliza Vigderman & Gabe Turner, *The Data Big Tech Companies Have on You*, SECURITY.ORG (Oct. 27, 2020), <https://www.security.org/resources/data-tech-companies-have/> (highlighting all the big data collected on individuals by Facebook, Google, Amazon, and others).

are tracked and saved, often without users' awareness.⁹ This is arguably the most significant public and private issue of our time. We have always made weapons, but now the issue of online presences becoming weaponized and privacy breaches require the use of new tactics and strategy.¹⁰

The revelations by Edward Snowden regarding the surveillance practices of the National Security Agency (NSA) revealed the depth to the NSA's domestic collection programs in 2013.¹¹ On many occasions, it has been suspected that wholesale surveillance of phone, email, text messages, and other forms of digital communication began under the Bush administration in the post-9/11 world.¹² From call detail records alone, the NSA can learn who you called, when you called, how frequently you called, how long you spoke, what device you used, your location when you made the call, the device used by the person you called, and the location of the person you called.¹³ In 2013, a copy of a secret Foreign Intelligence Surveillance Court (FISA) order approving NSA collection of three months' worth of Verizon call detail records was leaked to *The Guardian*, which then proceeded to publish it.¹⁴ The court order did not allow the NSA to know the content of the communication between the callers, it would be a "convenient first step towards the attainment of a warrant for that

9. See *id.* (showing big tech companies track and collect data when individuals conduct searches or engage with adverts).

10. See Bruce Schneier, *Cyberconflicts and National Security*, UN CHRON., <https://www.un.org/en/chronicle/article/cyberconflicts-and-national-security> (last visited Mar. 12, 2021) (discussing the need for cyberdefense responses to the ever-growing cyberwarfare problems).

11. See Raphael Satter, *U.S. Court: Massive Surveillance Program Exposed by Snowden Was Illegal*, REUTERS (Sept. 2, 2020), <https://www.reuters.com/article/us-usa-nsa-spying/u-s-court-mass-surveillance-program-exposed-by-snowden-was-illegal-idUSKBN25T3CK> (identifying the depth of the surveillance by the NSA and its illegality).

12. See Dan Tynan, *Why Is the NSA Spying on Us?*, COMPUTERWORLD (June 6, 2013), <https://www.computerworld.com/article/2711359/why-is-the-nsa-spying-on-us-.html> (discussing the unabated NSA surveillance program started by former President George W. Bush).

13. *Id.* ("It can learn who you called, when you called, how often and how long you spoke.").

14. See Satter, *supra* note 11 (describing the findings of the Court, considering information published first by the Guardian newspaper).

information.”¹⁵

The extension of the national intelligence collections practices beyond simply foreign targets to include United States citizens seemingly goes beyond the claims that digital surveillance is necessary to detect and avoid external terrorist attacks (such as those like 9/11) from occurring again. Glenn Greenwald went as far to describe it as “the U.S. Surveillance State.”¹⁶ In this state, we are constantly being monitored and each byte of data is carefully stored and monetized for profit.¹⁷

These data points are not always used against us, and many Americans are blissfully unaware of the extent that tracking takes place.¹⁸ During the coronavirus pandemic, many individuals made the switch to online shopping or delivery as a way to avoid the risk of contracting the virus by going into crowded stores.¹⁹ These purchases were collected, tracked, and monitored, then pushed through algorithms to bombard consumers with products they would be more likely to buy based off of their purchasing histories.²⁰ Data tracking not only took place in a commercial setting, but also through

15. Tynan, *supra* note 12 (“While the court order doesn’t allow Verizon to reveal personally identifying information, it wouldn’t be hard to get.”).

16. Richard J. Kilroy Jr., *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State*. By Glenn Greenwald, New York, NY: Metropolitan Books, 2014, 9 J. STRATEGIC SEC. 99, 99 (2016) (arguing Greenwald was angered by the high levels of surveillance in the United States).

17. See generally Charlie Warzel & Ash Ngu, Opinion, *Google’s 4,000-Word Privacy Policy is a Secret History of the Internet*, N.Y. TIMES (July 10, 2019), <https://www.nytimes.com/interactive/2019/07/10/opinion/google-privacy-policy.html> (discussing the profiteering of personal data for targeted adverts).

18. See generally Vigderman & Turner, *supra* note 8 (discussing how people could understand the terms but they are too long to adequately review for full terms and understanding).

19. See generally *COVID-19 Has Changed Online Shopping Forever, Survey Shows*, UNCTAD (Oct. 8, 2020), <https://unctad.org/news/covid-19-has-changed-online-shopping-forever-survey-shows> (showing levels of increased online shopping).

20. See Brian X. Chen, *Are Targeted Ads Stalking You? Here’s How to Make Them Stop*, N.Y. TIMES (Aug. 15, 2018), <https://www.nytimes.com/2018/08/15/technology/personaltech/stop-targeted-stalker-ads.html> (explaining how targeted ads are created and how the advertisements are persistent).

communication.²¹ As more people took to their homes for work, communications took a sharp turn towards digital mediums.²² Platforms like Zoom were used for work-from-home situations, but also as time went on—for personal conversations as well.²³ However, this collision of security/privacy and convenience is the underbelly of the issues with national security and data collection.

This wide-scale collection violates the rights to privacy as originally written in the U.S. Constitution and has been the source of numerous hearings and government committees in recent years.²⁴ Torn between the obvious need to protect the country from acts of foreign terrorist attacks, protecting the rights of individual citizens as guaranteed by constitutional law, policing companies who may be less than forthcoming in the extent and manner in which they collect data, and allowing innovation and independence in the market, there is no easily implementable solution to the problems created by data mining.²⁵

Questions on privacy during the time of COVID-19 have been especially impacted as traditional in-person presence has moved to virtual learning in schools and remote work for various fields of business.²⁶ Completely unprecedented has been the necessary move to virtual trials in the legal sector, as courts have had to face radical changes in order to allow some semblance of the 6th amendment

21. See Dacia Green, *Big Brother is Listening to You: Digital Eavesdropping in the Advertising Industry*, 16 DUKE L. & TECH. REV. 352, 356–58, (2018) (explaining that voice assistant technology has recorded private communications, even while inactive).

22. See Heather Kelly, *The Most Maddening Part About Working from Home: Video Conferences*, WASH. POST (Mar. 16, 2020), <https://www.washingtonpost.com/technology/2020/03/16/remote-work-video-conference-coronavirus/> (discussing how the pandemic created a surge in usage of digital and video platforms).

23. See *id.* (explaining that Zoom and others expanded beyond professional use).

24. See *US: End Bulk Data Collection Program*, HUM. RTS. WATCH (Mar. 5, 2020), <https://www.hrw.org/news/2020/03/05/us-end-bulk-data-collection-program> (reflecting the legislative efforts to understand and regulate data collection).

25. Kavanagh, *supra* note 2, at 1–2 (explaining the complex nature of technological development).

26. See Alvaro Puig, *Settlement Requires Zoom to Better Secure Your Personal Information*, FED. TRADE COMM'N [FTC] (Nov. 9, 2020), <https://www.consumer.ftc.gov/blog/2020/11/settlement-requires-zoom-better-secure-your-personal-information> (requiring Zoom to create stronger privacy protections for users of the program).

during COVID-19.²⁷ In the early days of the pandemic, courthouses were simply closed altogether.²⁸ However, as the coronavirus continued to sweep throughout the country and infection and death rates continued to climb even after the initial plateau, it became abundantly clear that coronavirus was going to be a marathon, not a sprint.²⁹ As such, virtual trials began being more heavily explored and considered as a feasible alternative during the pandemic.³⁰ I will discuss this more extensively later on, as the holding of virtual trials through platforms like Zoom or other online software opens the doors to hacking or lack of confidentiality like never before.³¹

Lastly, the United States is unlike any other system of government in terms of the levels of encouraged free expression from its people.³² The First Amendment is one of the most fundamental of all protections, guaranteeing the right to free speech.³³ In the months

27. See generally U.S. CONST., amend. VI. (granting individuals who have been charged with a crime the right to a speedy trial); Jason Tashea, *The Legal and Technical Danger in Moving Criminal Courts Online*, BROOKINGS (Aug. 6, 2020), <https://www.brookings.edu/techstream/the-legal-and-technical-danger-in-moving-criminal-courts-online/> (warning of the possible constitutional violations that occur when conducting trials online).

28. See generally Bruce M. Wexler & Yar R. Chaikovsky, *U.S. Court Closings, Restrictions, and Re-Openings Due to COVID-19*, PAUL HASTINGS (Mar. 12, 2021), <https://www.paulhastings.com/insights/practice-area-articles/u-s-court-closings-restrictions-and-re-openings-due-to-covid-19> (showing the closings and changes to the courts around the country).

29. See Video, Audio, Photos & Rush Transcript: Amid Ongoing COVID-19 Pandemic, Governor Cuomo Issues Executive Order Moving New York Presidential Primary Election to June 23rd, (Mar. 28, 2020), <https://www.governor.ny.gov/news/video-audio-photos-rush-transcript-amid-ongoing-covid-19-pandemic-governor-cuomo-issues> [hereinafter *Cuomo Issues Executive Order Amid Pandemic*].

30. See Alan Feuer et al., *Coughing Lawyers. Uneasy Jurors. Can Courts Work Under Coronavirus?*, N.Y. TIMES (Mar. 20, 2020), <https://www.nytimes.com/2020/03/20/nyregion/coronavirus-new-york-courts.html> (creating a new normalcy of expanding virtual trials due to the ongoing pandemic).

31. See *infra* Section IV.A; U.S. Attorney's Office, *Federal, State, and Local Law Enforcement Warn Against Teleconferencing Hacking During Coronavirus Pandemic*, DEP'T OF JUST., (April 3, 2020) (explaining the phenomenon of zoom bombing and the potential risks of hacking on all virtual platforms).

32. See *Freedom of Speech: Historical Background*, CONST. ANNOTATED, https://constitution.congress.gov/browse/essay/amdt1_2_1/ (last visited Mar. 12, 2021).

33. See U.S. CONST., amend. I.

leading up to and during the 2020 Presidential Election, various social media platforms began “fact checking” several postings from political figures and taking them down, flagging them, or hiding them altogether as they alleged that they contained potentially untrue or exaggerated information.³⁴ This was particularly problematic for President Donald Trump and his supporters, as they declared that big tech companies were deliberately silencing conservatives on media platforms.³⁵ This was interpreted as a violation of first amendment rights, which guarantee the right to freedom of speech.³⁶

The problems with the collection of Internet data are multi-faceted and extremely complex. The convergence of national security needs, sovereign rights to regulate, and protection of civil rights all come together to create a deeply problematic issue with no clear resolution. In this article, I discuss these aspects of the modern Internet-dominated era.³⁷ National security must always be understood not only as a defensive priority, but also as an offensive priority. It is no longer enough to be able to defend against attacks; rather, the country must be able to move quickly and effectively on the offense as well.³⁸ The Senate Subcommittee on Communications, Technology, Innovation, and the Internet has jurisdiction over the legislation, congressional action, and other matters relating to communications.³⁹ This

34. Catherine Sanz & Catherine Thorbecke, *What Social Media Giants Are Doing to Counter Misinformation this Election*, ABC NEWS (Oct. 18, 2020), <https://abcnews.go.com/Technology/social-media-giants-counter-misinformation-election/story?id=73563997> (discussing the efforts to curb the spread of misinformation).

35. Sarah Kopit, *Why Big Tech and Conservatives are Clashing on Free Speech*, BLOOMBERG (Jan. 12, 2021), <https://www.bloomberg.com/news/articles/2021-01-12/why-big-tech-u-s-conservatives-battle-over-speech-quicktake> (“Trump . . . charged that Twitter had coordinated with rivals . . . to silence him.”).

36. See *id.* (detailing reactions from Trump and other conservatives who were banned from Twitter).

37. See *infra* Section V. See generally National Conference of State Legislatures, *Cybersecurity Legislation 2020*, LEXISNEXIS (Apr. 1, 2021), <https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2020.aspx> (detailing the various legislative acts created across multiple states addressing cybersecurity, and regulation).

38. See Kavanagh, *supra* note 2, at 8 (arguing governments and regulators should engage proactively with the growing capabilities of technology).

39. See *Communications, Media, and Broadband*, U.S. SENATE COMM. ON COM., SCI., & TRANSP., <https://www.commerce.senate.gov/communications-media->

Committee, chaired by Senator John Thune and with Senator Brian Schatz as a Ranking Member, will certainly be involved in the government response to the digital communications that are rapidly taking over the world.⁴⁰

I will also highlight the moral obligations involved in technology that have been largely overlooked by Big Tech.⁴¹ Whereas traditional addictions have correlated primarily to substances—nicotine, opioids, alcohol, or tobacco—newer studies suggest there are highly addictive elements of the Internet and particularly social media.⁴² I argue that there must be some level of accountability for companies that take deliberate action steps towards making their consumers drawn towards their products in an unhealthy manner.⁴³ While they are certainly permitted to market their product in certain styles, just as with any other company/product, technology and social media companies must not be able to tap into troves of users' personal data without permission in order to make their products irresistibly addictive to their customers.⁴⁴

Next, I will discuss the 2020 Presidential Election as a means of showing the power and influence that big tech has on American policies and defense.⁴⁵ Try as the government may to harness and/or

and-broadband-subcommittee (last visited Mar. 12, 2021).

40. See Lamar Johnson, *Senate Democrats Name Leadership on Cyber Committees*, MERITALK (Feb. 5, 2021), <https://www.meritalk.com/articles/senate-democrats-leadership-cyber-committees/> (stating the roles of the Senators on the cyber committee).

41. See *infra* Section V; Emanuel Moss & Jacob Metcalf, *The Ethical Dilemma at the Heart of Big Tech Companies*, HARV. BUS. REV. (2019) (discussing the constant ethical dilemmas faced by tech organizations).

42. See Sherri Gordon, *Excessive Social Media Use Comparable to Drug Addiction*, VERYWELL MIND (July 17, 2019), <https://www.verywellmind.com/excessive-social-media-use-4690882>.

43. See *infra* Section VII.A; *Don't Trust Big Tech, Hold Them Accountable*, PUB. CITIZEN, <https://www.citizen.org/article/techhearingaccountability/> (arguing for regulation and accountability for major tech companies).

44. See Ken Mueller, *Do the Right Thing: Social Media and the New Accountability*, ARCOMPANY (Mar. 5, 2014), <https://arcompany.co/do-the-right-thing-social-media-and-the-new-accountability/> (expressing the desire for integrity from tech companies with user data).

45. See *infra* Section II; Joan Donovan & Amed Khan, *Opinion, Big Tech was Allowed to Spread Misinformation Unchecked. Will Biden Hold Them Accountable?*, GUARDIAN (Jan. 27, 2021),

curtail the rapidly expanding power of Big Tech, if a technology company disseminates a certain message, there are hundreds of millions of people who are going to side with it. The United States has arrived at a place in time where there is a strong demand to not have the government regulate you, but also to protect the ability to guarantee national security while encouraging continual growth and innovation, and in a way that only portrays the “truth.”⁴⁶ There is no greater place that each of these complex issues met than the 2020 Election.⁴⁷ This time in history has created a type of “Never Never Land” and will continue to evolve, as will the colossally huge issues with controlling terrorism, the rights to privacy, structuring defense, and modern society.⁴⁸

In closing, I will make recommendations as to how we can navigate this enormously difficult period in such a way to ensure both collective safety as a nation battling daily cybersecurity leaks and attacks from foreign influences and as a country that prides itself on its ability to speak freely without censorship or fear of retribution from an authoritative party.⁴⁹ Much of the way modern warfare takes place is no longer on battlefields with heavy artillery, but rather online through hacks and leaks.⁵⁰ This occurs on the national scale but also impacts

<https://www.theguardian.com/technology/commentisfree/2021/jan/27/qanon-facebook-google-twitter-misinformation-big-tech> (addressing the issue of misinformation and the role it played in the 2020 presidential election).

46. See Jay Stanley, *Eight Problems with “Big Data”*, ACLU (Apr. 25, 2012), <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/eight-problems-big-data>.

47. Kopit, *supra* note 35 (stating that the Twitter bans propelled the argument between conservatives and social media platforms).

48. John Herrman, *We’re Stuck with the Tech Giants. But They’re Stuck with Each Other*, N.Y. TIMES MAG. (Nov. 13, 2019), <https://www.nytimes.com/interactive/2019/11/13/magazine/internet-platform.html> (discussing the magnitude of the internet and advanced technologies).

49. See *infra* Section VII; Ahiza Garcia-Hodges, *Big Tech has Big Power over Online Speech. Should it be Reined In?*, CNBC (Jan. 21, 2021), <https://www.nbcnews.com/tech/tech-news/big-tech-has-big-power-over-online-speech-should-it-n1255164> (discussing the delicate balancing act between American interests, security, and the need for regulation).

50. Amit Sharma, *Cyber Wars: A Paradigm Shift from Means to Ends*, 34 STRATEGIC ANALYSIS 62, 62 (2010) (discussing the shift in warfare to reflect the change in technological advances).

individual users.⁵¹ People may not always recognize how extensively they are being tracked and their data is being used, but this is all the more reason to discuss the need for their protection as fundamental American freedoms. Yet, these must be weighed against the critical need for national security. There may not be the perfect one-size-fits-all solution, but I will describe the direction taken by the federal law and modern circumstances to propose resolute measures that can be implemented to attempt to protect all parties while still encouraging technological progress.⁵²

II. UNITED STATES HISTORY WITH DATA SURVEILLANCE PRACTICES

The attacks on the World Trade Center by Al-Qaeda on September 11th, 2001 forever altered the American landscape. Changes spurred by the death of nearly 3,000 innocent Americans are visible in the way airports operate security policies and in the Aviation and Transportation Security Act (ATSA), which eventually led to the Transportation Security Administration (TSA).⁵³ Out of concern for the national security of the United States, the president at the time, George W. Bush, gave the green light to his administration to secretly carry out widescale surveillance actions.⁵⁴ Known as the President's Surveillance Program (PSP), secret wiretapping and surveillance were carried out as part of the war on terrorism, but the program would later become controversial as questions of it violating American principles emerged.⁵⁵

51. *See id.* (describing the impact of cyberwarfare on the individuals not just governments).

52. *See infra* Section VI.A; Garcia-Hodges, *supra* note 49 (describing the need for accountability within reason as not to hinder progress and security).

53. *See* Alycia B. Taylor & Sara Steedman, *The Evolution of Airline Security Since 9/11*, INT'L FOUND. PROT. OFFICERS (2003), <https://www.ifpo.org/resource-links/articles-and-reports/protection-of-specific-environments/the-evolution-of-airline-security-since-911/> (explaining the creation of TSA); Michael Smith, *September 11 and the Transportation Security Administration*, NAT'L MUSEUM OF AM. HIST., (Sept. 1, 2011), <https://americanhistory.si.edu/blog/2011/09/september-11-and-the-transportation-security-administration.html> (describing the development of the TSA as an organization).

54. OFF. OF INSPECTORS GEN., REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM, at 4, REPORT NO. 2009-0013-A (2009) [hereinafter OIG REPORT].

55. Tracey Maclin, *The Bush Administration's Terrorist Surveillance Program*

A) DATA SURVEILLANCE UNDER PRESIDENT GEORGE W. BUSH'S ADMINISTRATION

In the aftermath of 9/11, President Bush immediately took action to prevent a similar event from ever occurring again.⁵⁶ In Title III of the Foreign Intelligence Surveillance Act Amendments Act of 2008 (FISA Amendments Act), the President's Surveillance Program was defined as "the intelligence activity involving communications that was authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, including the program referred to by the President in a radio address on December 17, 2005 (commonly known as the Terrorist Surveillance Program)."⁵⁷ This program involved several agencies: the National Security Agency (NSA), Federal Bureau of Investigation (FBI), Central Intelligence Agency (CIA), and the Office of the Director of National Intelligence (ODNI) National Counterterrorism Center.⁵⁸ Many of the specific actions taken by the PSP remain classified information, but in December 2005 President Bush acknowledged that these activities included the interception, without a court order, of certain international communications when there was a "reasonable basis to conclude that one party to the communication is a member of al-Qa'ida, affiliated with al-Qa'ida, or a member of an organization affiliated with al-Qa'ida."⁵⁹ This program needed to be renewed every

and the Fourth Amendment's Warrant Requirement: Lessons from Justice Powell and the Keith Case, 41 U.C. DAVIS L. REV. 1259, 1263 (2008); see *Surveillance Under the USA/Patriot Act*, ACLU, <https://www.aclu.org/other/surveillance-under-usapatriot-act> (arguing that surveillance constitutes a search and that the Patriot Act violates the 4th Amendment by bypassing the warrant requirement for searches).

56. Gary L. Gregg II, *George W. Bush: Foreign Affairs*, UVA MILLER CTR., <https://millercenter.org/president/gwbush/foreign-affairs> (last visited Mar. 12, 2021).

57. See FISA Amendments Act of 2008, H.R. 6304, 110th Cong., § 301(a) (3).

58. OIG REPORT, *supra* note 54, at 1, n.1.

59. See Press Briefing, Alberto Gonzales, U.S. Attorney General, and General Michael Hayden, Principle Deputy Director for National Intelligence, *Briefing from the White House About NSA Authorization*, WHITE HOUSE: OFFICE OF PRESS SEC'Y (Dec. 19, 2005, 8:30 AM), <https://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051219-1.html> [hereinafter AG Gonzales Press Briefing] (clarifying the listening occurred only when someone was suspected of belonging to a terrorist organization).

45 days to remain active, a criteria met each time.⁶⁰

The Department of Justice (DOJ) Office of Legal Counsel (OLC) Deputy Assistant Attorney General John Yoo drafted the first series of legal memoranda supporting the program.⁶¹ To him, the ultimate test as to whether the government could engage in warrantless electronic surveillance activities was whether such conduct was consistent with the Fourth Amendment, rather than whether it met the standards of FISA.⁶² The Fourth Amendment states:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”⁶³

Yoo dismissed concerns about the Fourth Amendment in regard to PSP to the extent that the PSP’s authorizations applied to non-U.S. persons outside of the United States.⁶⁴ In regard to the aspects of the PSP that involved interception of the international communications of U.S. persons in the United States, “Yoo asserted that Fourth Amendment jurisprudence allowed for searches of persons crossing the border and that interceptions of communications into or out of the United States fell within the ‘border crossing exception.’”⁶⁵ He also later stated that the electronic surveillance occurring in “direct support of military operations” did not violate the constitutional rights that prohibit illegal searches and seizures and that the activity that took place under the PSP met the “reasonable” criteria in the Fourth Amendment and thus the lack of a warrant was acceptable.⁶⁶

However, in the unclassified report, the closing paragraph states: “the collection activities pursued under the PSP, and under FISA

60. See *The NSA Wiretapping Program*, 1 FOR THE RECORD 1, 7 (2007), <https://www.lawandsecurity.org/wp-content/uploads/2007/01/NSA-Wiretapping-Program.pdf> (explaining how the NSA program works, including the renewal process).

61. OIG REPORT, *supra* note 54, at 12–15.

62. *Id.*

63. See U.S. CONST., amend. IV.

64. OIG REPORT, *supra* note 54, at 15.

65. *Id.*

66. *Id.*

following the PSP's transition to that authority, involved unprecedented collection activities. We believe the retention and use by IC organizations of information collected under the PSP and FISA should be carefully monitored."⁶⁷ The secretive nature of the program led to many powerful government officials being left in the dark.⁶⁸ However, when analysis eventually reached higher-ups in the Department of Justice in late 2003 and early 2004, they were "convinced that the plan may have run afoul of the law, ignoring important Supreme Court rulings on executive-branch power."⁶⁹

The effectivity of the PSP was challenged, as reports interviewing intelligence officials found that they had trouble "citing specific instances where PSP reporting had directly contributed to counterterrorism successes" and the CIA "did not implement procedures to assess the usefulness of the product of the PSP, and did not routinely document whether particular PSP reporting had contributed to successful counterterrorism operations."⁷⁰ This report led Senator Russ Feingold, a Wisconsin Democrat sitting on the Senate Intelligence Committee, to conclude:

[The report] highlights just how outrageous and damaging the illegal warrantless wiretapping program really was. This report leaves no doubt that the warrantless wiretapping program was blatantly illegal and an unconstitutional assertion of executive power. I once again call on the Obama administration and its Justice Department to withdraw the flawed legal memoranda that justified the program and that remain in effect today.⁷¹

67. *Id.*

68. See Carrie Johnson & Ellen Nakashima, *Report: Wiretaps Risked a Crisis*, PHILA. INQUIRER (July 11, 2009), https://web.archive.org/web/20090713055716/http://www.philly.com/inquirer/front_page/20090711_Report_Wiretaps_risked_a_crisis.html (stating that the program was entrusted with only three DOJ lawyers).

69. *Id.*

70. See *Bush-Era Wiretap Program had Limited Results, Report Finds*, CNN (July 12, 2009), <https://www.cnn.com/2009/POLITICS/07/12/bush.wiretap/> (reflecting on the shortcomings of the program in countering terrorism).

71. *Id.*

B) DATA SURVEILLANCE UNDER PRESIDENT BARACK OBAMA'S ADMINISTRATION

Prior to his presidency, Barack Obama was a Senator from Illinois who opposed the Patriot Act.⁷² This act broadly expanded law enforcement's surveillance and investigative powers by giving sweeping search and surveillance privileges to domestic law enforcement and foreign intelligence agencies while eliminating the checks and balances system that was previously used by courts to ensure that those powers were not abused.⁷³ Obama argued that it was still possible to secure the United States against terrorist attacks and risks without trampling on individuals' civil liberties.⁷⁴ Some may incorrectly believe that Obama's surveillance practices simply matched the footsteps of the presidential administration before him, but it was under his administration that the revelations about the NSA were made in 2013 by Edward Snowden.⁷⁵

Edward Snowden was an IT systems expert working for the NSA when he made the choice to become a whistleblower by sharing thousands of top-secret documents about the United States intelligence agencies' surveillance of Americans with journalists from *The Guardian*, *The New York Times*, and *The Intercept*.⁷⁶ He provided proof to the journalists that the government was regularly tracking the

72. See Kara Brandeisky, *The Surveillance Reforms Obama Supported Before he was President*, PROPUBLICA (Aug. 7, 2013), <https://www.propublica.org/article/the-surveillance-reforms-obama-supported-before-he-was-president> (stating former senator Obama's opposition to the Patriot Act).

73. See *PATRIOT Act*, ELEC. FRONTIER FOUND. (July 13, 2020), [https://www.eff.org/issues/patriot-act#:~:text=The%20USA%20PATRIOT%20Act%20\(officially,the%20September%2011%2C%202001%20attacks](https://www.eff.org/issues/patriot-act#:~:text=The%20USA%20PATRIOT%20Act%20(officially,the%20September%2011%2C%202001%20attacks).

74. See *Senate Floor Statement - The PATRIOT Act*, BEST SPEECHES OF BARACK OBAMA THROUGH HIS 2009 INAUGURATION, <http://obamaspeeches.com/041-The-PATRIOT-Act-Obama-Speech.htm> (last visited Mar. 12, 2021).

75. See Julia Angwin et al., *New Snowden Documents Reveal Secret Memos Expanding Spying*, PROPUBLICA (June 4, 2015), <https://www.propublica.org/article/new-snowden-documents-reveal-secret-memos-expanding-spying> (arguing the program expanded under the Obama administration).

76. Hanna Kim, *The Resilient Foundation of Democracy: The Legal Deconstruction of the Washington Posts's Condemnation of Edward Snowden*, 93 IND. L.J. 533, 533 (2018).

calls of millions of Americans, unbeknownst to the citizens who were being spied on.⁷⁷ These 2013 revelations startled the American population, who suddenly began to recognize the complexities of the ambiguous levels of data and privacy security they possessed.⁷⁸

It was also under Obama's administration that an Internet worm named Stuxnet was released.⁷⁹ In David Sanger's book *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*, he confirms that both the United States and Israeli governments developed and deployed Stuxnet with the goal of breaking "Iranian nuclear centrifuge equipment by issuing specific commands to the industrial control hardware responsible for their spin rate . . . [thus] hop[ing] to set back the Iranian research program."⁸⁰ Although the program was first authorized by George W. Bush, it was Obama who continued the practice and ended up releasing the virus.⁸¹ This program was called "Olympic Games" as a code name and unpredictably disabled parts of the Natanz plant in Iran even as it told controllers that everything was normal; in 2010, Stuxnet escaped Natanz and, after being connected to the Internet, did what it was designed not to do: spread in public.⁸² The finger-pointing then began to assign blame for the fatal coding error.⁸³ In a briefing to the

77. *Id.*

78. See generally A.W. Geiger, *How Americans Have Viewed Government Surveillance and Privacy Since Snowden Leaks*, PEW RSCH. CTR. (June 4, 2018), <https://www.pewresearch.org/fact-tank/2018/06/04/how-americans-have-viewed-government-surveillance-and-privacy-since-snowden-leaks/> (providing survey results that demonstrate the degree to which Americans became aware of government surveillance and private data collection following the Snowden leaks).

79. See Paul Wagenseil, *Obama, Bush Behind Stuxnet Worm, Report Says*, NBC (June 1, 2012), <https://www.nbcnews.com/id/wbna47647550> (highlighting the program was not terminated under Obama rather the program was continued and expanded).

80. Nate Anderson, *Confirmed: US and Israel Created Stuxnet, Lost Control of It*, ARS TECHNICA (June 6, 2012), <https://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/>.

81. David E. Sanger, *Obama Order Sped Up Wave of Cyberattacks Against Iran*, N.Y. TIMES (June 1, 2012), <https://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html> (noting that a new variant of the worm had been deployed shortly before the summer of 2010, when it escaped Natanz).

82. Anderson, *supra* note 80.

83. *Id.*

president, Obama's vice-president, Joe Biden, reportedly stated, "it's got to be the Israelis, they went too far."⁸⁴ This type of cyber-attack was largely unprecedented around the world, and particularly in the United States, yet the extent to which cyberwarfare could take place had yet to be fully explored.⁸⁵

This worm was one of the first computer malware codes that was capable of causing destruction at a physical level.⁸⁶ Initially, it was not clear if a cyberattack on physical infrastructure was possible, but a dramatic meeting saw the pieces of a destroyed test centrifuge spread out on a conference table, at which point the United States gave the go-ahead to unleash the malware.⁸⁷ Although it was capable of physical destruction, it did not destroy every infected computer.⁸⁸ Rather, upon infection, it checked to see if the computer was "connected to specific models of programmable logic controllers (PLCs) manufactured by Siemens," then "alter[ed] the PLCs' programming, resulting in the centrifuges being spun too quickly and for too long, damaging or destroying the delicate equipment in the process."⁸⁹

By 2014, President Barack Obama promised to end the NSA's practice of collecting and storing bulk phone-call data; however, his administration continued to seek reauthorization every 90 days of the telephone metadata program.⁹⁰ In a plan submitted to Congress, the

84. *Id.*

85. See Sanger, *supra* note 81 ("Mr. Obama, according to participants in the many Situation Room meetings on Olympic Games, was acutely aware that with every attack he was pushing the United States into new territory, much as his predecessors had with the first use of atomic weapons in the 1940s, of intercontinental missiles in the 1950s and of drones in the past decade.").

86. See Josh Fruhlinger, *What is Stuxnet, Who Created It and How Does It Work?*, CSO (Aug. 22, 2017), <https://www.csoonline.com/article/3218104/what-is-stuxnet-who-created-it-and-how-does-it-work.html> (noting that Symantec described the Stuxnet code as more complex than anything it had previously seen).

87. *Id.*

88. *Id.*

89. *Id.*

90. Press Release, *Joint Statement from the ODNI and the U.S. DOJ on the Declassification of Renewal Collection Under Section 501 of the FISA*, OFF. DIR. NAT'L INTEL. (Dec. 8, 2014) (on file with the Office of the Director of National Intelligence) [hereinafter *Joint Statement*]; see Cody M. Poplin, *NSA Ends Bulk Collection of Telephony Metadata under Section 215*, LAWFARE (Nov. 30, 2015),

NSA would also be required to conduct searches of data at phone companies and would need to receive a warrant from a federal judge to conduct the search—a change from the Bush Administration's practices of warrantless wiretapping.⁹¹ However, it failed to fix the problem of unconstitutional National Security Letters, did not stop the bulk collection of data on Americans' digital communications, continued "backdoor" surveillance under Section 702 of the FISA Amendments Act, and failed to provide non-US persons with the same privacy protections as those afforded to US persons.⁹²

In 2017, a declassified FISA report that was marked "Top Secret" was published, in which it was noted that the NSA routinely violated Americans' Fourth Amendment rights and had abused intelligence tools to do so.⁹³ The report labeled the matter as a "very serious Fourth Amendment issue," cited an "institutional lack of candor" on the part of the administration, and criticized the NSA for having a "disregard" for the rules and showing "deficient" oversight.⁹⁴ Soon after, the NSA

<https://www.lawfareblog.com/nsa-ends-bulk-collection-telephony-metadata-under-section-215> (observing the end of the NSA's bulk collection of telephony metadata on November 29, 2015, pursuant to the USA Freedom Act).

91. Press Release, *Fact Sheet: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program*, WHITE HOUSE (Mar. 27, 2014), <https://obamawhitehouse.archives.gov/the-press-office/2014/03/27/fact-sheet-administration-s-proposal-ending-section-215-bulk-telephony-m>; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), <https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html> (discussing George W. Bush's 2002 presidential order for the NSA to surveil calls and emails without first obtaining warrants).

92. See Mark Rumold, *One Year Later, Obama Failing on Promise to Rein in NSA*, ELEC. FRONTIER FOUND. (Feb. 3, 2015), <https://www.eff.org/deeplinks/2015/02/one-year-later-obama-failing-promise-rein-nsa>.

93. See U.S. FOREIGN INTEL. SURVEILLANCE CT., [Serial No. Redacted], MEMORANDUM OPINION AND ORDER 1, 17, 63–64 (Apr. 26, 2017), [available at https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISF_Memo_Opin_Order_Apr_2017.pdf] (approving the NSA's new targeting and minimizing procedures for surveillance under Section 702, which were designed to avoid future violations of US persons' Fourth Amendment rights).

94. *Id.* at 17–19 (referencing an October 26, 2016, FISC hearing where the Court criticized the NSA for not disclosing at an earlier hearing that the NSA Inspector General and Office of Compliance for Operations had learned that NSA analysts violated the prohibition on queries using US-person identifiers run against upstream Internet data).

concluded “after a comprehensive review of mission needs, current technological constraints, United States person privacy interests, and certain difficulties in implementation, [they had] decided to stop some of [their] activities conducted under Section 702 [of the FISA Amendments Act].”⁹⁵

Obama’s actions may not have begun cyberwarfare or Internet surveillance, but his administration largely expanded pre-existing practices.⁹⁶ He took the country into a full-scale civilian and global surveillance period largely unknown until the Snowden whistleblowing scandal.⁹⁷ Although the government has since doubled down on such actions, Obama’s administration will still go down in history as one of the most influentially aggressive cyber administrations.⁹⁸ At this time, there were few rules to govern cyberattacks, which did not fall under the standards set forth by the Geneva Convention.⁹⁹

95. Press Release, *NSA Stops Certain Section 702 “Upstream” Activities*, NSA (Apr. 28, 2017), <https://www.nsa.gov/news-features/press-room/Article/1618699/nsa-stops-certain-section-702-upstream-activities/> [hereinafter *NSA Press Release 2017*] (changing surveillance collections from communications “about” foreign intelligence targets to only communications directly to or from those targets).

96. See Rumold, *supra* note 92 (enumerating four facets of the NSA surveillance program that Obama did not “rein in” during his presidency).

97. See Glenn Greenwald et al., *Edward Snowden: The Whistleblower Behind the NSA Surveillance Revelations*, *GUARDIAN* (June 11, 2013), <https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance> (describing Snowden’s public disclosure of the NSA bulk surveillance program as “one of the most significant leaks in US political history,” and the scope of the program as “all-consuming”).

98. See Joseph Marks, *Obama’s Cyber Legacy: He Did (Almost) Everything Right and it Still Turned Out Wrong*, *NEXTGOV* (Jan. 17, 2017), <https://www.nextgov.com/cybersecurity/2017/01/obamas-cyber-legacy-he-did-almost-everything-right-and-it-still-turned-out-wrong/134612/> (“The Obama administration made an unprecedented all-fronts effort to secure cyberspace.”).

99. The Geneva Conventions outline a set of rules of war, along with Additional Protocols. Their purpose is to: “provide minimum protections, standards of humane treatment, and fundamental guarantees of respect to individuals who become victims of armed conflicts.” It is broken up into several conventions and protocols: Convention I: “ensures humane treatment without discrimination founded on race, color, sex, religion or faith, birth or wealth, etc. To that end, the Convention prohibits torture, assaults upon personal dignity, and execution without judgment.” Convention II: “extended the protections described in the first Convention to shipwrecked soldiers and other naval forces”

C) DATA SURVEILLANCE UNDER PRESIDENT DONALD TRUMP'S ADMINISTRATION

Data surveillance practices were one of the defining issues of Donald Trump's presidency, tracing back to even before he was inaugurated in January 2017.¹⁰⁰ An investigative journalist dove into the Cambridge Analytica and Facebook relationship only to find evidence that Facebook had used their massive data storage ownership to disproportionately influence swing voters during the 2016 United States election and propel Donald Trump to the presidency through the application "thisisyourdigitallife."¹⁰¹ The application recorded results of a personality quiz and took data from the Facebook accounts of those that took the quiz as well the friends of the individuals who took the quiz.¹⁰² The gathered data was then sent through an algorithm that enabled psychological profiling based on Facebook interactions.¹⁰³ This in turn was used to push specific ads to certain people who could potentially be persuaded to vote for Donald Trump in the 2016 presidential election.¹⁰⁴

Convention III: "defined 'Prisoner of War' and accorded such prisoners proper and humane treatment as specified by the first Convention . . . Nations party to the Convention may not use torture to extract information from POWs."

Convention IV: "civilians are afforded the same protections from inhumane treatment and attack afforded to sick and wounded soldiers in the first Convention."

Protocol I: "new rules regarding the treatment of the diseased, cultural artifacts, and dangerous targets were produced."

Protocol II: "the fundamentals of 'humane treatment' were further clarified."

Protocol III: "add[ed] another emblem, the 'red crystal' to the list of emblems used to identify neutral humanitarian aid workers."

100. See, e.g., Kate Brannelly, *Trump Campaign Pays Millions to Overseas Big Data Firm*, NBC (Nov. 4, 2016), <https://www.nbcnews.com/storyline/2016-election-day/trump-campaign-pays-millions-overseas-big-data-firm-n677321>

(discussing the voter targeting by the 2016 Trump campaign using data analysis by Cambridge Analytica); Michael Balsamo, *What's Known About Surveillance of Trump Campaign Aides*, AP (May 3, 2019), <https://apnews.com/article/f9b05595332242e9809f739d9a185177> (detailing the surveillance of Donald Trump's 2016 campaign staff).

101. See Ikhlal ur Rehman, *Facebook-Cambridge Analytica Data Harvesting: What You Need to Know*, 2019 LIBR. PHIL. & PRAC. 5–6 (explaining that, by using Cambridge Analytica, Donald Trump's 2016 campaign was able to secure the votes of an additional 77,000 people in Michigan, Wisconsin, and Pennsylvania).

102. *Id.* at 5.

103. *Id.* at 5–6.

104. *Id.* at 6.

During his administration, Trump staged a war against whistleblowers.¹⁰⁵ Whistleblowers have existed throughout American history and have a longstanding pattern of exposing the government or high-powered officials for acting in ways that are perceived as being outside of the law or morally inappropriate.¹⁰⁶ Government whistleblowers are increasingly being charged under laws like the Espionage Act despite not being spies, and are receiving treatment that may damage their reputations among the American public.¹⁰⁷ Whistleblowing has been encouraged by some as a means of boosting transparency and thus trust in public officials, or even by keeping track of the actions of our elected leaders.¹⁰⁸ Trump's time in office was filled with violations of long-standing norms of disclosure, including refusal to make income tax returns public and providing basic information about his whereabouts and activities.¹⁰⁹

Still, data surveillance practices became a challenge to his authority as information was discovered about suspicious financial transactions involving Trump's former attorney Michael Cohen, prominent attorney Michael Avenatti, and a journalist for the New Yorker, Ronan

105. See Micah Lee, *The Trump Administration is Using the Full Power of the U.S. Surveillance State Against Whistleblowers*, INTERCEPT (Aug. 4, 2019), <https://theintercept.com/2019/08/04/whistleblowers-surveillance-fbi-trump/> (examining the prosecution by the Trump administration of whistleblowers under the Espionage Act).

106. See, e.g., *The History Of Whistleblowing in America*, WHISTLEBLOWERS INT'L, <https://www.whistleblowersinternational.com/what-is-whistleblowing/history/> (last visited Apr. 20, 2021) ("Benjamin Franklin became one of the first American whistleblowers in 1773 when he exposed confidential letters showing that the royally appointed governor of Massachusetts had intentionally misled Parliament to promote a military buildup in the Colonies.").

107. See Lee, *supra* note 105 ("The [Espionage Act] is blind to the possibility that the public's interest in learning of government incompetence, corruption, or criminality might outweigh the government's interest in protecting a given secret . . . [i]t is blind to the difference between whistleblowers and spies.") (internal quotes omitted).

108. William H. Harwood, *Secrecy, Transparency and Government Whistleblowing*, 43 PHIL. & SOC. CRITICISM 164, 165–66 (2017) (quoting Abraham Lincoln, Thomas Jefferson, and James Madison to support the proposition that transparency is essential to democracy).

109. Glenn Greenwald, *In the Trump Era, Leaking and Whistleblowing Are More Urgent, and More Noble, Than Ever*, INTERCEPT (Nov. 14, 2016), <https://theintercept.com/2016/11/14/in-the-trump-era-leaking-and-whistleblowing-are-more-urgent-and-more-noble-than-ever/>.

Farrow.¹¹⁰ One of these transactions saw Cohen paying \$130,000 to an adult film actress in exchange for her silence about an alleged affair between herself and Trump.¹¹¹ However, Trump's Justice Department later indicted Internal Revenue Service (IRS) official John Fry for providing these details.¹¹² Regardless of whether the allegations were true or not, the Trump Administration sent a strong message through the indictment that they would not be accepting or encouraging of whistleblowers, and instead would pursue punitive measures.

D) DATA SURVEILLANCE UNDER PRESIDENT JOSEPH BIDEN'S ADMINISTRATION

A 2020 survey of technology executives found that 32 percent of its respondents said that defining a national cybersecurity protocol should be the top priority for President Joe Biden's administration and Congress.¹¹³ Phil Quade, chief information security officer for Fortinet, said "action by the incoming [Biden] administration—national leadership across policy, strategy, diplomacy, and operations—in consultation with the private sector, must complement private sector actions, to protect the nation's infrastructures, hard-earned economic advantages and personal privacy."¹¹⁴ He also wrote "our nation had a cybersecurity coordinator on the National Security Council during the Bush and Obama administrations—a post central to developing policy to defend against increasingly sophisticated digital attacks and the use of offensive cyber weapons."¹¹⁵ In 2018 that position was eliminated.¹¹⁶ At the time, national security adviser John R. Bolton said the post was no longer considered necessary because lower-level officials had already made cybersecurity issues a "core function" of the president's national security team.¹¹⁷ It is time for President-elect Biden to fill that position again.¹¹⁸

110. See Lee, *supra* note 105.

111. *Id.*

112. *Id.*

113. See de León, *supra* note 1.

114. *Id.*

115. *Id.*

116. See *id.*

117. *Id.*

118. *Id.*

In carving out his own policies and precedent to characterize his administration, Biden is likely to follow much of the same work that he conducted under the Obama administration. At the end of 2020, during the transition period between former President Donald Trump and Biden's inauguration, the United States was victim to a massive Russian cyberattack that included breaches of U.S. government computer systems at the departments of Treasury, Commerce and Homeland Security that may have lasted months before they were discovered.¹¹⁹ Biden is likely to come down hard against adversaries who engage in cyberattacks against the U.S., as he stated "a good defense isn't enough; We need to disrupt and deter our adversaries from undertaking significant cyberattacks in the first place."¹²⁰ Senate Minority Whip Dick Durbin agreed, calling the attacks "virtually a declaration of war by Russia on the United States, and we should take that seriously."¹²¹

Their resolute remarks align with the mission of the U.S. Army Cyber Command (ARCYBER), which is an organization that serves to "operate and defend Army networks and deliver cyberspace effects against adversaries to defend the nation."¹²² Their responsibilities include "continually monitoring cyber threats and keeping a 24-hour watch on the Army's global networks; modernizing networks and improving defensive cyberspace operations; bringing offensive and defensive cyber capabilities to combat malicious threats; and

119. See Jaclyn Diaz, *Russia Suspected in Major Cyberattack on U.S. Government Departments*, NPR (Dec. 14, 2020), <https://www.npr.org/2020/12/14/946163194/russia-suspected-in-months-long-cyber-attack-on-federal-agencies>.

120. See Christina Wilkie, *Joe Biden Warns He Will Be Tough on State Sponsors of Cyberattacks, as U.S. Suffers Massive Hack*, CNBC (Dec. 17, 2020), <https://www.cnbc.com/2020/12/17/biden-hints-at-a-tougher-stance-against-state-sponsors-of-cyberattacks.html> (quoting then-President-elect Biden's response to the SolarWinds attack).

121. See Yaron Steinbuch, *Sen. Dick Durbin Says Alleged Russian Hack 'Virtually a Declaration of War'*, N.Y. POST (Dec. 18, 2020), <https://nypost.com/2020/12/18/sen-dick-durbin-says-alleged-russian-hack-virtually-a-declaration-of-war/> (vowing, also, that "there will be a price to pay for [Russia's hack].").

122. See *About Army Cyber Command*, U.S. ARMY, <https://www.goarmy.com/army-cyber/about-army-cyber-command.html> (last updated July 31, 2019).

modernizing networks to provide resilient Army combat systems to meet challenges in any operational environment.”¹²³ Biden’s statement also included the promise: “We will do that by, among other things, imposing substantial costs on those responsible for such malicious attacks, including in coordination with our allies and partners. Our adversaries should know that, as President, I will not stand idly by in the face of cyber assaults on our nation.”¹²⁴

Due to the controversial nature of the 2020 election that resulted in a weeks-long delay of the transition process, concern grew over the susceptibility of the nation’s security.¹²⁵ By Trump and some members of the GOP refusing to accept a Biden victory, the United States was left without any universal agreement on national leadership.¹²⁶ The commander-in-chief is briefed on various topics that are critical to the welfare of the nation. Who is included in these briefings if there is a lack of consensus regarding who the commander-in-chief is? Biden was included in some briefings during the Obama administration, most notably during the Stuxnet worm when it was alleged that he was vocal about his disregard.¹²⁷ Although the Russian hack occurred prior to Biden’s official January 2021 inauguration, Biden noted that his incoming national security team was briefed on the attacks.¹²⁸ This marks a notable shift from the prior administration in its dealings with cybersecurity and Internet attacks.¹²⁹ Furthermore, the three lead

123. *Id.*

124. Wilkie, *supra* note 120 (outlining how to disrupt and deter cyber-attacks).

125. See Vivian Salama et al., *Lack of Transition Coordination and Pentagon Chaos Could Leave US Vulnerable to National Security Threats*, CNN (Nov. 14, 2020), <https://www.cnn.com/2020/11/12/politics/transition-pentagon-chaos-intelligence-national-security-threat> (noting that the Presidential transition is a period when adversaries have historically looked to escalate tensions with the US, thus worrying national security experts during the transition when senior-level personnel left the Department of Defense and the Trump administration blocked then-President-elect Biden from receiving classified briefings).

126. See Karen Yourish et al., *The 147 Republicans Who Voted to Overturn Election Results*, N.Y. TIMES (Jan. 7, 2021), <https://www.nytimes.com/interactive/2021/01/07/us/elections/elecelect-college-biden-objectors.html> (listing the 147 Republican Representatives and Senators who voted to sustain objections to Congress’s certification of electoral votes).

127. See Sanger, *supra* note 81 (quoting Biden fuming in the Stuxnet briefing that the Israelis “went too far”).

128. Wilkie, *supra* note 120.

129. *Id.*

agencies responsible for investigating attacks and protecting the U.S. from cyber threats—the FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the Office of the Director of National Intelligence—announced the formation of a joint command to respond to what they noted was a “significant and ongoing cybersecurity campaign” against the country.¹³⁰

E) UNITED STATES LAW ENFORCEMENT AGAINST CYBER WARFARE

The United States has several sectors devoted to the protection of the U.S. cyber realm. This includes several branches of the FBI, Department of Homeland Security, Office of the Director of National Intelligence, the CIA, and Senate Committees and Subcommittees. The number of cyber threats, security breaches, and necessary surveillance grows increasingly higher by year as technology advances, thus making it a top priority for national defense to be involved on both offensive and defensive levels.¹³¹

The FBI’s branch on Information Technology is composed of three divisions that work together to “mov[e] forward aggressively to build better and faster networks; innovative IT tools and applications for agents and other professionals; and automated systems that streamline our work and free up our time . . . to stop today’s high-tech criminals and terrorists”.¹³² September 11, 2001 underscored the need for a robust IT infrastructure that could “integrate and manage the FBI’s information across several computer systems to support its mission.” Then-Director Robert S. Muller, III listed “upgrad[ing] technology to successfully perform the FBI’s mission” as among his top 10 priorities for transforming the FBI.¹³³ He also stated in congressional testimony

130. *Id.*

131. See Jory Heckman, *Biden Makes Cybersecurity ‘Top Priority’ in National Security Guidance*, FED. NEWS NETWORK (Mar. 4, 2021), <https://federalnewsnetwork.com/cybersecurity/2021/03/biden-makes-cybersecurity-top-priority-in-national-security-guidance/> (stating that the Biden administration called cybersecurity a “top priority”).

132. See *Information Technology*, FBI, <https://www.fbi.gov/about/leadership-and-structure/information-technology> (last visited Apr. 2, 2021) [hereinafter *FBI Information Tech*].

133. *Id.*

that “technology is intertwined with the bureaucracy. We have a paper bureaucracy that has built up over 90 years. There are ways of doing things that are torturous—burdensome, if not torturous—let me just put it that way. And the technology is going to make a large difference in how we change as an organization.”¹³⁴ Since then, technology infrastructure has undergone significant changes, and is now a major resource for the FBI.¹³⁵

Another branch of the FBI that involves technology is the Science and Technology branch, which “deploys the FBI’s world-renowned applied science and operational technology resources to support investigative and intelligence activities . . . serves as the strategic leader of the FBI’s scientific, operational technology, and information sharing programs.”¹³⁶ It is this sector that is responsible for operational technology to “help keep the nation safe by providing sophisticated tools and techniques used across all FBI investigative programs,” which includes both electronic and technical surveillance.¹³⁷ Electronic surveillance is defined as “developing and deploying tools and techniques to perform lawfully authorized intercepts of wired and wireless telecommunications and data network communications” while technical surveillance is defined as “using technology and capabilities to covertly and lawfully surveil, track, or locate targets of interest in operational matters.”¹³⁸ It is important to note the addition of “lawfully” in these descriptions because of scandals like the Edward Snowden leak.¹³⁹ Unfortunately, the problem with much of the modern issues regarding surveillance and Internet security is that there are limited rules and regulations on what can and cannot happen.¹⁴⁰

134. *Id.*

135. *See id.* (listing the ways FBI technology has been modernized since 2003).

136. *Science and Technology Branch*, FBI, <https://www.fbi.gov/about/leadership-and-structure/science-and-technology-branch> (last visited Apr. 2, 2021) [hereinafter *FBI Science & Tech*].

137. *Id.*

138. *Id.*

139. *See Satter, supra* note 11 (reporting on the Ninth Circuit’s holding that the NSA’s mass surveillance program—exposed by Snowden—violated FISA).

140. *See* Manav Tanneeru, *Can the Law Keep Up With Technology?*, CNN (Nov. 17, 2009), <https://www.cnn.com/2009/TECH/11/17/law.technology/index.html> (“Internet-related cases are being watched closely because they confront new and unaddressed areas of American law.”).

Technology is advancing at a faster rate than laws can manage and keep up with, making it difficult to manage the relationship between individuals' right to privacy and the government's obligations to protect its citizens and the nation from both domestic and international cyberthreats.¹⁴¹

The FBI also relies heavily on the Operational Technology Division (OTD), whose mission and vision are to “deliver technology-based solutions that enable and enhance the FBI’s intelligence, national security, and law enforcement operations . . . to counter current and emerging threats through applied technology.”¹⁴² Their work rarely makes news headlines, but the department has been instrumental in averting terrorist plots, identifying adversaries involved in espionage activities, and helping convict a child pornography suspect.¹⁴³

Intelligence also plays a key role in the protection of American democracy. The United States’ system is a relatively new model of democracy, and a system that is still being tested daily. As such, it still faces various threats against it, particularly against the election process.¹⁴⁴ In a hearing by the Committee on Homeland Security called “Secure, Safe, and Auditable: Protecting the Integrity of the 2020 Elections,” it was said:

We must not forget the lessons of 2016 . . . Russian foreign interference campaign engaged in their hack and dump operations against one candidate and targeted election systems in all 50 states. We must continue to improve the security of election infrastructure and campaign organization and improve the public resilience to foreign influence campaigns.¹⁴⁵

141. See *id.* (stating that the development of law related to new technologies is about five years behind the development of the technologies themselves).

142. See *Operational Technology*, FBI, <https://www.fbi.gov/services/operational-technology> (last visited Apr. 2, 2021) [hereinafter *FBI OP. Tech*].

143. *Id.*

144. See *Election Security*, BRENNAN CTR., <https://www.brennancenter.org/issues/defend-our-elections/election-security> (last visited Apr. 2, 2021) (“[During the 2016 elections,] [h]ackers conducted ‘research and reconnaissance’ against election networks in all 50 states, breached at least one state registration database, attacked local election boards, and infected the computers at a voting technology company.”).

145. *Secure, Safe, and Auditable: Protecting the Integrity of the 2020 Elections*:

National security and law enforcement also must consider what our opponents are using to attack us. Our skills and tools cannot be anything less than what we are attempting to police or prevent, and if anything, we must have more.

The effectiveness of technology has yet to be fully understood but is a vital component to our national security.¹⁴⁶ Tech companies, particularly those that have troves of user data such as Facebook, Twitter, Google, or Amazon, have access to information that can be critical to national security,¹⁴⁷ thus complicating the issue, as the government attempts to rein in companies that are irreplaceable in value for protecting national security. Furthermore, legislation on privacy and data collection can be painstakingly slow as it must pass

Hearing Before the Subcomm. on Cybersec., Infrastructure Prot., & Innovation of the H. Comm. on Homeland Sec., 116th Cong. (2020) (on file with the subcommittee) (statement of Rep. Cedric Richmond, Chairman of the Cybersecurity, Infrastructure Protection, & Innovation Subcommittee). See generally *Secure, Safe, and Auditable: Protecting the Integrity of the 2020 Elections: Hearing Before the Subcomm. on Cybersec., Infrastructure Prot., & Innovation of the H. Comm. on Homeland Sec.*, 116th Cong. (2020), <https://homeland.house.gov/activities/hearings/secure-safe-and-auditable-protecting-the-integrity-of-the-2020-elections>.

146. See Jessica Leber, *Don't Panic, But Our Technology Now Defies Human Understanding*, FAST CO. (July 20, 2016), <https://www.fastcompany.com/3061952/dont-panic-but-our-technology-now-defies-human-understanding> (“[W]hat’s scary is not that [everyday consumers] don’t understand the systems and machinery that are at this point responsible for society’s function and our individual safety. It’s that even those who are supposed to understand them often don’t.”); Loren B. Thompson, *Why U.S. National Security Requires a Robust, Innovative Technology Sector*, LEXINGTON INST. 1, 4 (2020), <https://www.lexingtoninstitute.org/wp-content/uploads/2020/10/100820-why-u.s.-national-security-requires-a-robust-innovative-technology-sector-002.pdf> (noting the fungibility of technologies between civilian and military uses, such as smartphone processors being used in “smart weapons, battlefield communications, and military training devices,” and the ability of such technologies to confer an advantage).

147. See Ganesh Sitaraman, *The National Security Case for Breaking Up Big Tech*, KNIGHT FIRST AMENDMENT INST. (Jan. 30, 2020), <https://knightcolumbia.org/content/the-national-security-case-for-breaking-up-big-tech> (highlighting that big American technology companies operating in China or seeking to do so will likely result in information being transferred to the Chinese government and “directly or indirectly furthering China’s emergent domestic surveillance capabilities, its military use of those technologies, and its spread of digital authoritarianism abroad as well”).

through numerous houses of government.¹⁴⁸ While this occurs, technology is still evolving, and the government is left scrambling behind attempting to police actions that have already taken place.¹⁴⁹

III. GLOBAL LEGISLATION ON PRIVACY AND DATA COLLECTION

Although the Internet is a relatively recent development to global society, countries around the world are still citing fundamental and basic laws to make decisions on how to best navigate this new reality.¹⁵⁰ At the time the U.S. Constitution was drafted in the 18th century, there was no reason to anticipate the evolution of technology to the extent of what it has become today; therefore, the document does not contain any clear direction for how to navigate technological privacy. Still, there are several critical amendments that do protect the rights of individuals from an overbearing reach of government powers, and these can and are applied to modern-day issues with Internet security in the United States.¹⁵¹ These are often limited to within

148. See, e.g., David Uberti, *States Push Internet Privacy Rules in Lieu of Federal Standards*, WSJ (Feb. 18, 2021), <https://www.wsj.com/articles/states-push-internet-privacy-rules-in-lieu-of-federal-standards-11613644200> (outlining the “mosaic” of state-level privacy laws that is slowly and unevenly developing in lieu of a unified national framework).

149. See Thompson, *supra* note 146, at 17–18 (“[B]ecause new applications for information technology are constantly proliferating and the options for compromising those technologies are so numerous, it is hard to keep up with the evolution of the threat. Thus, many of the advances that the military hopes to make using technologies like artificial intelligence, autonomous vehicles and big data are potentially at risk. The new technologies can not only be degraded, they can be subverted to pose a threat to their users.”).

150. See, e.g., David Fidler, *The Supreme Court Adapts Constitutional Law to Address Technological Change*, COUNCIL ON FOREIGN REL. (July 11, 2018), <https://www.cfr.org/blog/supreme-court-adapts-constitutional-law-address-technological-change> (discussing the Supreme Court’s decisions in *Dakota v. Wayfair, Inc.* and *Carpenter v. United States*, where the Court reinterpreted the Commerce Clause and Fourth Amendment to account for changes in the relationship between the government and the governed caused by digital technologies).

151. See Cameron F. Kerry & John B. Morris, Jr., *Framing a Privacy Right: Legislative Findings for Federal Privacy Legislation*, BROOKINGS (Dec. 8, 2020), <https://www.brookings.edu/research/framing-a-privacy-right-legislative-findings-for-federal-privacy-legislation/> (noting that the Constitution protects various privacy interests through the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments).

America's jurisdiction and do not necessarily apply beyond U.S. borders. This creates a unique split in power and questions emerge in regard to how to navigate a borderless Internet world in a physical world with rules defined by geographical borders.

A) AMERICAN LEGISLATIVE BACKGROUND ON PRIVACY CONCERNS

The Constitution is one of the foundational documents to the United States and is considered to be the supreme law of the land. The first ten amendments outline basic rights of citizens, and the First Amendment states:

Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.¹⁵²

This fundamental American right and privilege must be protected, but there are also additional circumstances now in which free speech can have serious repercussions. If people can speak freely in person or in writing, should it be any different on the Internet? And at what point is it considered harmful? Furthermore, if people do choose to speak their minds online, do they still have rights to privacy for what is said? The Constitution may not contain any express right to privacy, but the Bill of Rights does reflect a strong concern for protection of specific aspects of privacy.¹⁵³

More recent legislation pertaining to defense include Section 230 of the Communications Decency Act (CDA) of 1996. This act states, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."¹⁵⁴ More simply put, online intermediaries [including Internet Service Providers (ISPs) and virtually any online service that publishes third-party content] that

152. U.S. CONST. amend. I.

153. *The Right of Privacy*, EXPLORING CONST. CONFLICTS, <http://law2.umkc.edu/faculty/projects/ftrials/conlaw/rightofprivacy.html> (last visited Apr. 2, 2021).

154. See Communications Decency Act [CDA], 47 U.S.C. § 230(c)(1).

host or republish speech are protected against a range of laws that could be otherwise used to hold them responsible for the words and actions of others.¹⁵⁵ This is a vitally important right, as the sheer size of user-generated websites like Facebook or YouTube makes it impossible for the platforms to prevent objectionable content from emerging on their sites. CDA 230 creates broad protections that allow continued innovation and the protection of the First Amendment freedom of speech.¹⁵⁶

However, CDA 230 was brought to the forefront of the nation's attention at the end of 2020 when President Donald Trump threatened to veto an annual military funding bill unless Congress agreed to repeal Section 230.¹⁵⁷ This is part of the \$740 billion National Defense Authorization Act, a huge chunk of the federal budget. He tweeted out:

Section 230, which is a liability shielding gift from the U.S. to 'Big Tech' (the only companies in America that have it – corporate welfare!), is a serious threat to our National Security & Election Integrity. Our Country can never be safe & secure if we allow it to stand. Therefore, if the very dangerous & unfair Section 230 is not completely terminated as part of the National Defense Authorization Act (NDAA), I will be forced to unequivocally VETO the Bill when sent to the very beautiful Resolute desk.¹⁵⁸

President Trump's refusal to sign a major military bill underscores the importance of Section 230, as his proposed "trade" implies that he considered the two comparable in terms of significance.¹⁵⁹

155. *Section 230 of the Communications Decency Act*, ELEC. FRONTIER FOUND., <https://www EFF.org/issues/cda230> (last visited Mar. 15, 2021).

156. *See id.* (mentioning that Facebook has more than 1 billion users and YouTube users upload 100 hours of video per minute).

157. Ross A. Lincoln, *Trump Threatens to Veto Defense Bill in Apparent Tantrum Over Mean Things Said About Him on Twitter*, MSN: THE WRAP (Dec. 2, 2020), <https://www.msn.com/en-us/tv/news/trump-threatens-to-veto-defense-bill-in-apparent-tantrum-over-mean-things-said-about-him-on-twitter/ar-BB1by9D3?ocid=msedgdhp>.

158. Melissa Quinn, *Trump Threatens to Veto Defense Bill Over Social Media Shield Law*, CBS NEWS (Dec. 2, 2020), <https://www.msn.com/en-us/news/politics/trump-threatens-to-veto-defense-bill-over-social-media-shield-law/ar-BB1byPvX?ocid=msedgdhp>.

159. *See id.* (hinting that opposition to Trump's stance on the defense bill is coming from House and Senate leaders).

These protections afforded through Section 230 are unique to American law, as most other countries do not have similar statutes.¹⁶⁰ These nations may still have high levels of Internet access, but most of the prominent online services are based in America, which makes the country one of the leaders in the battle to protect controversial speech and free expression.¹⁶¹

Even still, other sectors of the government are continuing to rally behind the idea of placing limitations on technology. In October 2020, the United States Department of Commerce's Bureau of Industry and Security ("BIS") published long-awaited controls on six categories of "emerging technologies."¹⁶² These new controls mean that companies will now almost always require authorization from the BIS to provide certain items to most jurisdictions that are outside of the United States or even to share important technical knowledge about said items with foreign national employees under BIS's "deemed exports" controls.¹⁶³ For foreign investors in U.S. businesses, they should also be aware of the ways these newly implemented controls will affect the abilities of the Committee on Foreign Investment in the United States (CFIUS) to review, block, or impose mitigation measures on investments in American businesses that are dealing in these new controlled technologies.¹⁶⁴

The advance notice of proposed rulemaking (ANPRM) did not specifically provide concrete examples of what would fall under the umbrella of "emerging technologies." However, the BIS did give a list that is currently subject to limited controls considered "emerging" and thus subject to new, broader controls:

(1) biotechnology

160. See, e.g., Mark MacCarthy, *In France, What's Illegal Offline Is Now Illegal Online*, FORBES (May 18, 2020), <https://www.forbes.com/sites/washingtonbytes/2020/05/18/in-france-whats-illegal-offline-is-now-illegal-online/?sh=7f554f538b5a> (detailing the protections for online content in France).

161. See *id.* (pointing out the difference in protection in France compared to the US).

162. Implementation of Certain New Controls on Emerging Technologies, 85 Fed. Reg. 62583 (Oct. 5, 2020) (to be codified at 15 C.F.R. pts. 740, 772, 774).

163. See *id.* at 62586 (outlining licensing requirements for export, re-export or transfer of items).

164. *Id.*

- (2) artificial intelligence and machine learning
- (3) position, navigation, and timing (PNT) technology
- (4) microprocessor technology
- (5) advanced computing technology
- (6) data analytics technology
- (7) quantum information and sensing technology
- (8) logistics technology
- (9) additive manufacturing
- (10) robotics
- (11) brain-computer interfaces
- (12) hypersonics
- (13) advanced materials
- (14) advanced surveillance technologies.¹⁶⁵

However, these attempts to control technology are often done with national security in mind: the ANPRM suggested that technologies be considered “essential to the national security of the United States” if they have “potential conventional weapons, intelligence collection, weapons of mass destruction, or terrorist applications or could provide the United States with a qualitative military or intelligence advantage.”¹⁶⁶ A 2019 meeting with BIS and its interagency partners concluded that six other technologies that were recently developed or were being developed, were essential to the United States’ national security and therefore warranted treatment as “emerging technologies”:

- (1) Hybrid additive manufacturing (AM)/computer numerically controlled (CNC) tools
- (2) Certain computational lithography software designed for the fabrication of extreme ultraviolet masks (EUV)
- (3) Technology for finishing wafers for 5nm production
- (4) Forensics tools that circumvent authentication or authorization

165. Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58201, 58202 (Nov. 19, 2018).

166. *Id.* at 58201.

controls on a computer or communications device and extract raw data

(5) Software for monitoring and analysis of communications and metadata acquired from a telecommunications service provider via a handover interface

(6) Sub-orbital aircraft¹⁶⁷

These controls that have been imposed impact not only the United States, but all global partners that they interact with for business. The Export Control Reform Act (ECRA) also required BIS to coordinate with the United States' allies and international export control regimes in order to encourage widespread adoption of similar controls on items deemed "emerging technologies," thereby avoiding a fragmented regulatory environment that could promote the offshoring of "emerging technology" development and shifting production from America to other jurisdictions with the goal of avoiding U.S. export controls.¹⁶⁸ The United States is a leader in the world's importing and exporting industries, and thus their regulations are certain to impact those of other jurisdictions.¹⁶⁹ At times, a coordinated approach like the one discussed above is taken to ensure a unified front is presented across the globe. However, this is not always the case and there are conflicting demands from differing governing bodies.¹⁷⁰

B) GLOBAL LEGISLATION ON PRIVACY

If a demand for access to data falls outside of the United States, then the U.S. laws and regulations may not be the appropriate precedent for determining how to manage that particular situation. However, the United States Constitution is far from being the only legislative authority that discusses or alludes to the rights that individuals have to

167. Press Release, Gibson Dunn, New Controls on Emerging Technologies Released, While U.S. Commerce Department Comes Under Fire for Delay (Oct. 27, 2020), <https://www.gibsondunn.com/wp-content/uploads/2020/10/new-controls-on-emerging-technologies-released-while-us-commerce-department-comes-under-fire-for-delay.pdf>.

168. *Id.* at 3.

169. *Id.*

170. See, e.g., G.A. Res. 217 (III) A, art. 12, Universal Declaration of Human Rights (Dec. 10, 1948) [hereinafter UDHR] (providing that people have the right to protection against arbitrary interference with privacy).

privacy.¹⁷¹ The rules that govern cross-border access to data have undeniable implications for the right to privacy, which is deeply enshrined in the 1948 United Nations (U.N.) Universal Declaration of Human Rights, Article 12:

“No one shall be subjected to arbitrary interference with his privacy, family, home, or correspondence nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.”¹⁷²

Other sources that include the right to privacy include the European Charter on Human Rights and the European Union Charter of Fundamental Rights.¹⁷³ Yet, not all countries follow these ordinances and data differs from other types of security issues because it can exist across various international borders and fall under the jurisdiction of more than one nation. As such, attaining said data can be a frustrating and extensive process.

Professor Jennifer Daskal from the American University Washington College of Law has studied the evolving security and rights issues of law enforcement gaining access to data from across borders.¹⁷⁴ She explains that several nations are either considering or have passed mandatory data localization requirements, according to which companies who do business under their jurisdiction are required to store data or copies of said data locally.¹⁷⁵ These measures facilitate the practice of domestic surveillance, increase the cost of carrying out business, and undercut the growth potential of the Internet by placing restrictions on the otherwise free and most efficient movement of data.¹⁷⁶ However, other nations—including the United States—assert

171. See, e.g., *id.* (“No one shall be subjected to arbitrary interference with his privacy . . . Everyone has the right to the protection of the law against such interference or attacks”).

172. *Id.*

173. See Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT’L SEC. L. & POL’Y 473, 481 (2016) (enumerating the international agreements that govern privacy rights).

174. See *id.* at 473 (explaining that the problems associated with law enforcement access to cross-border data is an emerging field).

175. See *id.* at 475, 486–87, 501 (summarizing how some countries have implemented data localization requirements).

176. See *id.* at 497 (explaining alternative means foreign governments will turn to instead of complying with existing diplomatic procedures).

that they can unilaterally compel ISPs that work under their jurisdiction to produce emails and various other forms of private communication stored under the jurisdiction of other nations, sans regard to the location or nationality of the target.¹⁷⁷ This leaves ISPs left in the middle, as they are forced to choose between adhering to the laws of one nation that seeks production of data, and honoring another nation's laws that prohibits this type of production.¹⁷⁸

An example of this took place in 2015 when the Brazilian authorities detained a Microsoft executive for refusing to turn over the Skype data of a Brazilian customer.¹⁷⁹ The data in question was stored in the United States, rather than Brazil, and it would have been illegal under United States law for Microsoft to complete the request.¹⁸⁰ Another instance of data privacy across borders took place later that year with North Korea. In Los Angeles, Sony Pictures Entertainment employees went to the office and discovered that some of their computers did not work and they could not access their email or retrieve their documents.¹⁸¹ As data, both personal and business-related, was posted, it became evident that this was not a fluke, but rather a deliberately coordinated attack.¹⁸² During the ensuing investigation, the trail crossed the United States and landed in North Korea.¹⁸³

The North Korean government denied responsibility, but one of the demands of the hackers was for Sony Pictures Entertainment to cancel their upcoming movie, "The Interview," which was about journalists recruited by the CIA to assassinate Kim Jong-un.¹⁸⁴ After promises of

177. See *id.* at 473, 498 (detailing the difficulties ISPs have complying with competing legal obligations in multiple jurisdictions).

178. See *id.* at 480 (explaining that providers have to consider multiple competing legal obligations).

179. See *id.* at 473, 477–78 (stating that the Brazil instance was an example of competing legal obligations ISPs encounter).

180. See Brad Smith, *In the Cloud We Trust: It's Time to Rebuild the World's Faith in the Technology that Empowers Us All*, MICROSOFT STORY LABS, <https://news.microsoft.com/stories/inthecloudwetrust/> (last visited Mar. 15, 2021) (outlining the facts of the Microsoft situation in Brazil).

181. See *id.* (setting forth the facts of the Sony case).

182. See *id.* (explaining Sony was under attack).

183. See *id.* (detailing that the investigation led to North Korea).

184. See *id.* (describing how the hackers wanted "The Interview" to be cancelled).

more hacking and violent threats at cinemas, several major movie theaters initially decided not to show the controversial film.¹⁸⁵ In response, President Obama said “Again, I’m sympathetic that Sony as a private company was worried about liabilities and this and that and the other. I wish they had spoken to me first. I would have told them, ‘Do not get into a pattern in which you’re intimidated by these kinds of criminal attacks.’” Following Obama’s statement, Microsoft and Google announced days later that they would distribute “The Interview” in order to support America’s principles of freedom of expression.¹⁸⁶ Still, Microsoft and Google are global companies that have access to data from all over the world.

The United States is one of the leading nations when it comes to standards for data privacy.¹⁸⁷ They also protect their data from other countries vociferously, which has not always been met with appreciation.¹⁸⁸ Foreign governments’ responses include the mandatory data localization requirements discussed earlier, unilateral assertions of extraterritorial jurisdiction, threats against employees or officers of local subsidiaries, mandatory anti-encryption regimes that facilitate live interception of the data as it transits through outside government jurisdictions, and an increased use of malware and other less accountable means of accessing the data that in turn weaken security for all users.¹⁸⁹

With this, it must be acknowledged that today’s world faces much

185. *See id.* (stating that movie theaters opted to not show the film).

186. *See id.*

187. *See id.* (comparing the U.S. standards to other standards).

188. *See id.* (explaining the changes in privacy and data residency laws around the world in response to the U.S.’s laws).

189. *See* Sergei Blagov, *Russia Pledges More Data Localization Audits*, BLOOMBERG L. (Nov. 13, 2015), <https://news.bloomberglaw.com/tech-and-telecom-law/russia-pledges-more-data-localization-audits> (outlining Russia’s laws regarding data localization); Daskal, *supra* note 173, at 476–78 (explaining how the U.K. and Brazil are replacing current laws to include the authority to compel the production of stored content from companies); Smith, *supra* note 180 (showing how foreign governments are proposing new privacy laws with respect to data residency); Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JUST SEC. (Sept. 16, 2014), <https://www.justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/> (describing the Network Investigative Techniques the FBI has begun to implement).

more confusion in terms of borders, laws, and enforcement of certain regulations because of the lack of a coherent response when it comes to Internet security.

IV. ONLINE SECURITY AND SURVEILLANCE HAPPENING MORE FREQUENTLY AND WITH GREATER INTENSITY

Knowledge of the extent to which personal data is tracked and sold for corporate fiscal gain is gradually becoming more familiar to the public.¹⁹⁰ This gathered information includes sensitive information like credit card details, social security numbers, digital communication history like chat logs, text messages and emails, health history, web search history, physical location, and more.¹⁹¹ Recent major lawsuits and scandals have made it more imperative for new legislation and regulation to be created and enforced for the companies and/or organizations that engage in data harvesting for lucrative or misleading claims of security purposes.¹⁹² This indeed includes the United States federal government.

A) INTERNET SURVEILLANCE REACHES ARE INFRINGING ON CONSTITUTIONAL RIGHTS

The Internet is one of the most incredible tools ever created in human history. Yet, it facilitates such intensive surveillance on individuals that some have described it as a “level of surveillance previously only written about in science fiction novels.”¹⁹³ This

190. Jeff Desjardins, *How Much is Your Personal Data Worth?*, VISUAL CAPITALIST (Dec. 12, 2016), <https://www.visualcapitalist.com/much-personal-data-worth/> (showing what types of data are collected, how they are collected, how much they are sold for, and to whom they are sold).

191. See *Protecting Personal Information: A Guide for Business*, FTC 1, 6 (2016), <https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business> (detailing what type of data is stolen or sold and how to protect it).

192. See e.g., S. Shah, *TikTok Will Pay \$92 Million to Settle Class-Action Data Harvesting Lawsuit*, ENGADGET (Feb. 26, 2021), <https://www.engadget.com/tiktok-class-action-data-harvesting-lawsuit-settlement-105004598.html> (describing the TikTok data-harvesting lawsuits).

193. Marie-Helen Maras et al., *Enabling Mass Surveillance: Data Aggregation in the Age of Big Data and the Internet of Things*, 4 J. CYBER POL. 160, 160 (2018).

surveillance is then used in circumstances ranging from monetization of data for company profit to being used in serious legal matters.¹⁹⁴ This occurs particularly through social media, as the opportunity to post photos and information about yourself and/or others online has opened up a world of possibilities in terms of guarding details of everyday life.¹⁹⁵

Investigating the usage of social media as evidence in courtrooms demonstrates the major shift that has taken place even within the legal realm. A study on the use of social media evidence through the review of appellate judgments identified 5,189 appeal cases in federal and state jurisdictions from October 1st, 2000 through September 30th, 2017.¹⁹⁶ California was used for state jurisdictional analysis, while the Ninth Circuit Court of Appeals (which includes California) was used for the federal analysis.¹⁹⁷ In 2017, there was a 350% increase in Ninth Circuit cases that used social media evidence as compared to seven years earlier in 2010's first cases.¹⁹⁸ There was also a 3933% increase in the California state cases when compared to the first cases in 2007.¹⁹⁹

Much of the usage of data points gathered through surveillance is alleged to be for the purposes of national security.²⁰⁰ It has been stated that the cyber realm is indeed “increasingly vital to national security”, due largely to the advancing technological capacities enjoyed not only

194. See Marie-Helen Maras, *Internet of Things: Security and Privacy Implications*, 5 INT'L DATA PRIV. L. 99, 99–104 (2015) (warning against the inadequacy of the legal framework and regulations for data, specifically for the Internet of Things).

195. See *id.* (voicing concerns over how user privacy is threatened because of limited control and choice over the collection, retention, and distribution of data).

196. See Lynne Graves et al., *LinkedLegal: Investigating Social Media as Evidence in Courtrooms*, 38 COMPUT. L. & SEC. REV. 1, 6 (2020) (explain that the results of the study showed that 514 cases in the Ninth Circuit Court of Appeals and 4,675 cases in the California Court of Appeals used social media as evidence).

197. *Id.* at 5.

198. *Id.* at 6–7.

199. *Id.*

200. See James Pattison, *From Defence to Offence: The Ethics of Private Cybersecurity*, EUR. J. INT'L SEC. 1 (forthcoming 2020), https://www.jamespattison.org/uploads/1/2/5/1/12518815/cyber_ejis_--_final.pdf. (raising the question of how involved private security firms should be involved in data surveillance operations in the name of national security).

by the United States—but also foreign governments.²⁰¹ The United States currently has several organizations in place fighting global cyber threats within the Department of Homeland Security such as the National Cybersecurity and Communications or the ARCYBER that serve to “operate and defend Army networks and deliver cyberspace effects against adversaries to defend the nation”.²⁰² This does include data collection, as significant portions of modern terrorism are now taking place in the cyberspace or involve technology that must be collected in order for full investigations to occur. However, frequent references are made to a “cyber-Pearl Harbor”, a “digital 9/11”, or even “Cybergeddon”—all of which fail to acknowledge the reality that the most severe attacks are below the conventionally understood military threshold and instead lie in attacks against critical infrastructure such as banks or telecommunications firms.²⁰³

Other branches of government also take part in data collection. The United States Department of Defense proposed new forms of data collection in dockets DOD—2020—OS—0099 and DOD—2020—OS—0101.²⁰⁴ In describing the need for information collection, they reference the Under Secretary of Defense for Acquisition and Sustainment’s [USD(A&S)] authority to “exercise, within assigned responsibilities and functions, all authority of the Secretary of Defense derived from statute or executive order (EO) or interagency agreement except where specifically limited by state or EO to the Secretary of Defense” and cite the responsibilities of the USD(A&S) that include “maximiz[ing] U.S. competitive advantage and ensure robust, secure, and resilient national industrial base capabilities” and “support[ing] and encourage[ing] small business.”²⁰⁵ Sensitive questions include

201. *See id.* at 1, 4–5 (outlining the remarks made by various foreign governments regarding the importance of cybersecurity).

202. *About Us*, U.S. ARMY CYBER COMMAND, <https://www.arcyber.army.mil/> (last visited Mar. 15, 2021).

203. Evan F Kohlmann & Rodrigo Bijou, Commentary, *Planning Responses and Defining Attacks in Cyberspace*, 126 HARV. L. REV. F. 173, 173 (2013).

204. Dep’t of Def. Dir. 5135.02, of the Under Sec’y of Def. for Acquisition and Sustainment, at 6, U.S. DEP’T OF DEF. (July 15, 2020) (outlining a new data management system that enables the DOD to perform data analysis and reporting in a timely, accurate, authoritative, and reliable manner to support oversight, decision making, and improved outcomes).

205. *Id.* at 18.

business proprietary, banking, taxation, and financial questions in order to determine an applicant's eligibility for participation on the Trusted Capital Digital Marketplace (TCDM) platform and assess for adversarial foreign ownership, influence, control, or other national security risks.²⁰⁶

The primary source of information gathering may not in fact require any sort of lengthy process of obtaining warrants or the proper legal statutes.²⁰⁷ During the sign-up process, many social media websites request your full name, date of birth, phone number, and email address. Once a user on the website, there are opportunities to fill in numerous other types of personal details: where you work, where you went to school, what your sexual orientation is, what your religious beliefs are, who your family members are, what types of food you enjoy eating, what type of music you like to listen to, etc. This type of information can seem to be an innocuous expression of personality, but history demonstrates a lengthy narrative of these data points being tracked, stored, and used numerous times in order to achieve a certain agenda.²⁰⁸ The rights to privacy seemingly go out the window once an online presence is established. Some users opt to follow certain "privacy" settings for their profiles, as an attempt to maintain some semblance of personal security. However, this data does not necessarily remain secure, as proven by various leaks and hacks.

In 2014, a major leak containing intimate photos of A-list actresses and performers cast serious doubts on the security of popular online storage sites.²⁰⁹ Jennifer Lawrence, an Oscar-winning actress, had

206. See Press Release, Dep't of Def., Department of Defense Announces Establishment of the Trusted Capital Digital Marketplace (Jan. 13, 2021) (on file with Dep't of Def.) (announcing the Trusted Capital Digital Marketplace and its goals of providing funding for providers for combatting predatory investment practices).

207. See John C. Eustice, *Understand the Intersection Between Data Privacy Laws and Cloud Computing*, REUTERS, <https://legal.thomsonreuters.com/en/insights/articles/understanding-data-privacy-and-cloud-computing> (last visited Mar. 15, 2021) (discussing the advent of cloud computing for network storage for general counsel of corporations).

208. See *id.* (stating how data privacy and protection statutes are enacted to protect personal information, but can vary widely from country to country, so tracking electronic data is important).

209. See Andrea Peterson et al., *Leaks of Nude Celebrity Photos Raise Concerns About Security of the Cloud*, WASH. POST (Sept. 1, 2014),

photographs leaked that were allegedly obtained from a personal iCloud account, a service that is operated by Apple© and often used to automatically store photos that are taken with the user's cell phone.²¹⁰ In the statements made immediately after the leaks by the FBI and Apple spokespeople, both stated active investigations were taking place; and other experts weighed in by suggesting ways that the leak could have happened—including exploiting alleged vulnerabilities in the “Find My iPhone” application.²¹¹ It appeared that these leaks were specifically targeted, most likely for the photographed individuals' celebrity statuses and the money that could be obtained through the selling of these images, but still revealed the precarious nature of digital technology.²¹² Digital presences can be susceptible to hacking and leaks, which can feel extremely violating for the victims as it goes against all notions of privacy both in the Constitution and in our innate reactions.

B) SOCIAL MEDIA: THE MODERN WEAPON

The benefits of social media are so plentiful that it can feel uncomfortable to discuss the dangerous aspects of modern technological developments. Still, there are serious problems associated with social media usage that can have major implications for the democratic political process in the United States. In 2016, a scandal involving Facebook and Cambridge Analytica saw a former employee of Cambridge Analytica that played a crucial role in Donald Trump's victorious presidential campaign claimed that the company had utilized Facebook's collection of data to bombard specifically chosen individuals with certain ads in hopes of swaying their political views.²¹³

https://www.washingtonpost.com/politics/leaks-of-nude-celebrity-photos-raise-concerns-about-security-of-the-cloud/2014/09/01/59dcd37e-3219-11e4-8f02-03c644b2d7d0_story.html (detailing the iCloud hack and the FBI's and Apple's response).

210. *Id.*

211. *See id.* (providing examples of how the hack could have occurred).

212. *See id.* (explaining that nude photos of celebrities are often faked and posted on the Internet in exploitative ways).

213. *See Tracey Lien, A Data Mining Company Allegedly Used Facebook to Distort Users' Reality*, L.A. TIMES (Mar. 20, 2018), <https://www.latimes.com/business/technology/la-fi-tn-facebook-information->

This led to a Senate hearing, where Facebook CEO Mark Zuckerberg was called in to testify.²¹⁴ When questioned on the security and privacy of Facebook and confronted with the fact that “a quiz app used by approximately 300,000 people led to information about 87 million Facebook users being obtained by the company Cambridge Analytica” and asked “why didn’t Facebook notify 87 million users that their personally identifiable information had been taken, and it was being also used—why were they not informed—for unauthorized political purposes?”²¹⁵ Theodore F. Claypool is Chair of the American Bar Association’s Cyberspace Committee in the Business Law Section, and said in a magazine published by the American Bar Association, “every bit of information we disclose is another data bite to be mined and measured, sorted and sold.”²¹⁶ This is a frightening new stage of human history, as growing concerns about disinformation, privacy breaches, and spreading harmful speech pervade society.

In a publication by Johns Hopkins University Press, “three painful truths” are defined as such because of the reluctance to squarely acknowledge the depth of the problems and the changes that would be required in order to mitigate said problems.²¹⁷ Deibert states:

The first painful truth is that the social-media business is built around personal-data surveillance, with products ultimately designed to spy on us in order to push advertising in our direction. The second painful truth is that we have consented to this, but not entirely wittingly: Social media are designed as addiction machines, expressly programmed to draw upon our

dominance-20180320-story.html. (discussing how Cambridge Analytica tailors ads and articles that individual users can see).

214. *Transcript of Mark Zuckerberg’s Senate Hearing*, WASH. POST (Apr. 10, 2018), <https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/>.

215. *Id.*

216. Theodore F. Claypoole, *Privacy and Social Media*, ABA BUS. L. (Jan. 23, 2014), https://www.americanbar.org/groups/business_law/publications/blt/2014/01/03a_claypoole/.

217. See Ronald Deibert, *The Road to Digital Unfreedom: Three Painful Truths About Social Media*, 30 J. DEMOCRACY 25, 25–26 (2019), <https://www.journalofdemocracy.org/articles/the-road-to-digital-unfreedom-three-painful-truths-about-social-media/> (outlining the three painful truths surrounding social media).

emotions. The third painful truth is that the attention-grabbing algorithms underlying social media also propel authoritarian practices that aim to sow confusion, ignorance, prejudice, and chaos, thereby facilitating manipulation and undermining accountability. Moreover, the fine-grained surveillance that companies perform for economic reasons is a valuable proxy for authoritarian control.²¹⁸

This contains several critical facts that should change the way social media should be publicly perceived. Many of the products advertised via social media are driven with the intent to sell a product, whether that be a certain look or a physical product. They are also specifically designed to be addicting and irresistible. The 2020 film *The Social Dilemma* describes today's social media-addicted culture with interviews from major network executive and a secondary narrative plot that tells the reality of social media addiction. The film includes the quotes "[o]nly two organizations call their customers 'users': illegal drugs and software" and "we have a moral responsibility, as Google, for solving this problem [of social media-addiction]"²¹⁹ The last point is one of the most fundamental concepts in regard to modern day American politics. The media has been lambasted countless times on both sides of the aisle for controlling the narratives, presenting alternative versions of reality, or even spreading dangerous misinformation.

The 2020 American Presidential Election and the COVID-19 pandemic have highlighted this issue, as several major tech companies have begun "fact-checking" the content on their site from powerful political figures.²²⁰ This included flagging content by placing warning

218. *Id.*

219. See Nayeli Mendoza, *The Social Dilemma: Addiction in the Time of Social Media*, SAINT SCROLL (Nov. 6, 2020), <https://saintscroll.com/6092/entertainment/the-social-dilemma-addiction-in-the-time-of-social-media/> (providing quotes from the documentary 'The Social Dilemma' and explaining their significance); Joseph Lalonde, *Quotes and Leadership Lessons from the Social Dilemma*, J.M. LALONDE (Sept. 21, 2020), <https://www.jmlalonde.com/quotes-and-leadership-lessons-from-the-social-dilemma/>. (providing quotes from the documentary The Social Dilemma and explaining their significance).

220. See, e.g., Steven Overly, *Pressure Rises on Facebook, Twitter to Rein in Trump as False Claims Spread*, POLITICO (Nov. 4, 2020), <https://www.politico.com/news/2020/11/04/social-media-election-aftermath-434120> (reporting that Twitter and Facebook curtailed false claims from former

labels or fact checking misleading posts, and in some cases preventing the particular content from being liked or shared.²²¹ Still, it does not seem to yet be enough to prevent the rapid disintegration of trust between the American people and media. The 2016 Facebook and Cambridge Analytica scandal demonstrates the role that social media plays in manipulating the perspectives of viewers and does indeed “facilitate[e] manipulation and undermin[e] accountability”.²²²

V. THE AGE OF SURVEILLANCE CAPITALISM AND MODERN TECHNOLOGY HERE TO STAY

Much of the data collected from users is used for advertising purposes, but this also leads to the point that the data is being sold for financial gains—often unbeknownst to the user whose data it is.²²³ Once an Internet user searches a website for a certain item, the company is able to monitor and track that data.²²⁴ For companies like Visa, AT&T, or Facebook, this is a goldmine.²²⁵ The newly acquired information tells the company what the user searches for, purchases, the frequency at which they purchase, and more.²²⁶ The attention that companies spend on tracking you has several different results. Firstly, they are able to recognize the types of products that you are interested in, so they can find others similar to it that may appeal to you.²²⁷ Secondly, they can sell your data to other companies to continue the profit train.²²⁸ What is more comfortably called “advertising” could

President Trump about the election).

221. *See id.* (explaining the use of flags on certain content to prevent the spread of misinformation).

222. Deibert, *supra* note 217, at 25.

223. *See* Max Eddy, *How Companies Turn Your Data Into Money*, PC MAG (Oct. 10, 2018), <https://www.pcmag.com/news/how-companies-turn-your-data-into-money> (explaining that data is valuable because it can be used in online advertising, which makes a company money).

224. *See id.* (detailing how the method of “ad targeting” is used to track user movement from one site to the next).

225. *See id.* (speculating that large companies like Facebook would not exist without the data collected).

226. *See id.* (describing how any type of data can be purchased for the right price, including credit card data).

227. *See id.* (illustrating how targeted ads are based on previous purchases).

228. *See id.* (lamenting how the lack of regulation allows data to freely flow

more accurately be described as “the process by which different businesses study and sell your data to make profits.”²²⁹ At the end of the day, many of the most commonly browsed websites are simply data-selling companies.²³⁰ Through the pandemic and gradual trend towards e-commerce, this new age of internet capitalism and subsequent surveillance is an inextricable piece of contemporary developed society.²³¹

A) AMAZON’S ROLE IN THE MARKETPLACE DURING COVID-19

Since Amazon’s creation, their “two-day shipping” has revolutionized the world.²³² Long before COVID-19 had ever arrived, Amazon had joined other major retailers in dominating the markets to the extent that small mom-and-pop type shops were put out of business.²³³ Once the pandemic hit, Amazon’s reach grew even larger because consumers were not willing to go to those same big-brand retailers that put the mom-and-pop shops out of business due to fear

between companies willing to pay for it).

229. See, e.g., Megan Graham & Jennifer Elias, *How Google’s \$150 Billion Advertising Business Works*, CNBC (May 18, 2021), <https://www.cnbc.com/2021/05/18/how-does-google-make-money-advertising-business-breakdown-.html> (explaining how companies monetize data of consumers on their websites and apps by selling consumer data to advertisers).

230. See Eddy, *supra* note 223 (warning that companies like Facebook and Google make the biggest part of their profits from collecting data).

231. Shoshana Zuboff, *Surveillance Capitalism and the Challenge of Collective Action*, 28 NEW LAB. F. 10, 11 (2019).

232. Gaby Del Valle, *Amazon Created the Expectation of 2-day Shipping. Now It Needs to Scale Back.*, VOX (Apr. 24, 2019), <https://www.vox.com/the-goods/2019/4/23/18508093/amazon-prime-two-day-shipping>.

233. Xianzheng Fang, *Exploring the Impact of E-Commerce on Cities and Villages: The Case of Amazon and Alibaba*, TUFTS UNIV. PRAC. VISIONARIES (Oct. 7, 2020), <http://www.practical-visionaries.org/exploring-the-impact-of-e-commerce-on-cities-and-villages-the-case-of-amazon-and-alibaba/>; Cory Mitchell, *Amazon Effect*, INVESTOPEDIA, <https://www.investopedia.com/terms/a/amazon-effect.asp> (last visited Apr. 3, 2021); Chazen Global Insights, *Mom-and-Pop vs. Big Box*, COLUM. BUS. SCH. IDEAS & INSIGHTS (Mar. 9, 2016), <https://www8.gsb.columbia.edu/articles/chazen-global-insights/mom-and-pop-vs-big-box> (discussing Kinshuk Jerath et al., COLUM. BUS. SCH., *A Model of Unorganized and Organized Retailing in Emerging Economies*, Research Paper No. 15-38 (2015), available at <https://ssrn.com/abstract=2585601>).

of contracting the virus.²³⁴ Instead, millions of people around the United States and the world logged onto their computers and went to Amazon for their needs.²³⁵

The amount of data that Amazon has on its users is astounding: credit card information, billing addresses, shipping addresses, birthdays, full names, the list goes on.²³⁶ Multiply that by millions, and one company's data trove is practically incomprehensible. In 2018, Amazon suffered a major data breach that then resulted in customer names and email addresses being disclosed on its website.²³⁷ Richard Walters, chief technical officer of cybersecurity firm CensorNet, said: "if the reports are correct, the information leaked—names and email addresses—is less significant than some of these other breaches, which saw card details leaked."²³⁸ However, it would be wrong to assume that this makes the breach inconsequential. Cyber-criminals can do a lot of damage with a large database of names and emails.²³⁹ A large majority of people still use predictable passwords, and thanks to previous high-profile breaches many people's passwords are also readily available on the dark web.²⁴⁰ For cyber-criminals, it then just becomes an exercise in joining the dots."²⁴¹

So many more people are relying on Amazon for groceries, gifts, and household necessities during the pandemic than were in 2018.²⁴²

234. Fang, *supra* note 233; Annie Palmer, *How the Coronavirus and Retail Closures Are Accelerating the Rise of Amazon*, CNBC (Apr. 19, 2020), <https://www.cnbc.com/2020/04/19/coronavirus-retail-closures-speed-the-rise-of-amazon.html>.

235. Palmer, *supra* note 234.

236. *Amazon.com Privacy Notice: Examples of Information Collected*, AMAZON, <https://www.amazon.com/gp/help/customer/display.html> (search "legal privacy notice" and click on "Amazon.com Privacy Notice") (last visited Mar. 12, 2021) [hereinafter *Amazon.com Privacy Notice*].

237. See Miles Brignall, *Amazon Hit With Major Data Breach Days Before Black Friday*, GUARDIAN (Nov. 21, 2018), <https://www.theguardian.com/technology/2018/nov/21/amazon-hit-with-major-data-breach-days-before-black-friday>.

238. *Id.*

239. *Id.*

240. *Id.*

241. *Id.*

242. Palmer, *supra* note 234.

This is an incredible development, but very invasive.²⁴³ If the government determined there was a need to examine the purchasing history of an individual, their address, or some other type of information that Amazon has access to, they could avoid coming directly to an individual and instead gather enormous amounts of information about you, your friends, family, co-workers, or others all from one account.²⁴⁴

B) THE LURKING DANGERS OF THE CYBERSPACE

Computers, phones, and the rapid advancements of technology have taken off so quickly that the public can scarcely keep up.²⁴⁵ These changes pose critical questions for our society and pace of progression: are these technological developments making the world a better and safer place? The former CEO of Google has said “there’s no question that Huawei has engaged in some [data] practices that are not acceptable in national security.”²⁴⁶ There are certainly convenience benefits, but the reality of cybersecurity and the imminent breaches of data are far more dangerous than the average user realizes.²⁴⁷ The realities of cybersecurity and the drive for profits in the age of data value demands higher standards for companies engaging in these profitability schemes in order to protect consumers and their data footprint.²⁴⁸

The public enjoys certain freedoms, rights, and privileges in much of their everyday life, but many users do not enjoy full protections in

243. Zuboff, *supra* note 231, at 11–12, 18, 23; *Amazon.com Privacy Notice*, *supra* note 236.

244. Oscar Gonzales, *Amazon Says Governments Requested Record Amount of User Data Last Year*, CNET (Feb. 1, 2021), <https://www.cnet.com/news/amazon-says-governments-requested-record-amount-of-user-data-last-year/> (citing *Amazon Information Request Report*, AMAZON 1, 1–2 (Jan. 31, 2021), https://d1.awsstatic.com/certifications/Information_Request_Report_December_2020.pdf).

245. TINA P. SRIVASTAVA, *INNOVATING IN A SECRET WORLD* 133 (2019).

246. Ryan Browne, *Former Google CEO Eric Schmidt Says There’s ‘No Question’ Huawei Routed Data to Beijing*, CNBC (June 18, 2020), <https://www.cnbc.com/2020/06/18/ex-google-ceo-eric-schmidt-no-question-huawei-routed-data-to-china.html>.

247. CHRISTIAN J. PULVER, *METABOLIZING CAPITAL* 94–95 (2020); SRIVASTAVA, *supra* note 245, at 133.

248. PULVER, *supra* note 247, at 94–95.

the cyberspace.²⁴⁹ This does not only apply for at-home browsing, but within the workplace as well: only 30% of executives whose companies use workforce data reported being highly confident they are using the data responsibly.²⁵⁰

If user privacy is not a top priority for companies, then their first line of customer advocacy in terms of cybersecurity is already down. There are certain moral obligations that people and companies must meet and protecting those who are susceptible must be valued.²⁵¹ However, fiscal success does not always align with moral excellence. Dr. Martin Luther King, Jr. said “there comes a time when one must take a position that is neither safe nor political nor popular, but he must take it because his conscience tells him it is right.”²⁵² It can be challenging to do the “right” thing in a climate where everyone else is doing the “wrong” thing and reaping financial reward.²⁵³ However, in order to build a lasting, loyal relations with employees and customers alike and fulfill humanitarian obligations, companies must continue to pursue further commitment to privacy.²⁵⁴ Some sites already do this, but their informing of users that their data may be tracked and monitored is often written in language that is difficult to understand or embedded in numerous paragraphs.²⁵⁵ These actions do little to inform or educate users, as most do not stop to read 500 words on a pop-up ad when they can simply click a box saying “agree” to access the

249. Germán M. Teruel Lozano, *Fundamental Rights in the Digital Society*, 46 REV. CHILENA DE DER. 301, 301–03 (2019).

250. See Ellyn Shook et al., *How Companies Can Use Employee Data Responsibly*, HARV. BUS. REV. (Feb. 15, 2019), <https://hbr.org/2019/02/how-companies-can-use-employee-data-responsibly>.

251. Gonzales, *supra* note 244.

252. Rev. Dr. Martin Luther King, Jr., *A Proper Sense of Priorities*, Address Delivered to Clergy and Laymen in Washington, D.C., Concerning the Vietnam War (Feb. 6, 1968).

253. *Id.*

254. Michael McFarland, *Why We Care About Privacy*, MARKKULA CTR. FOR APPLIED ETHICS (June 1, 2012), <https://www.scu.edu/ethics/focus-areas/internet-ethics/resources/why-we-care-about-privacy/>.

255. Kevin Litman-Navarro, *We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.*, N.Y. TIMES (June 12, 2019), <https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html>.

content.²⁵⁶

In the book *The Age of Surveillance Capitalism*, Shoshana Zuboff writes “in place of ‘policy’ or ‘social contract’ it is capitalism, and increasingly surveillance capitalism, that shapes the action.”²⁵⁷ The United States prides itself on encouraging capitalism and free market growth, but the technology industry is unparalleled to any other in history.²⁵⁸ The rate at which it has grown, its potential for growth, lucrativeness, and difficulty in forming guiding legislation from the governmental level is unprecedented.²⁵⁹ Still, although the capitalist economy may thrive under technological developments, and even more so under surveillance capitalism, there is still a much-needed role from a federal or state policy level in securing the rights of individuals to privacy from these mega corporations.²⁶⁰

C) ARE THERE LIMITS TO INCREASING INNOVATION?

Technology has undergone numerous revolutionary changes in the last few decades. This has impacted not only the more common communication apps for social media like Facebook, Twitter, or Instagram, or the e-commerce business like Amazon, AliBaba, or SheIn, but also intersected tech and privacy issues altogether.²⁶¹ The rapid innovation and consumer reliance on digital platforms are irreversible.²⁶² Amazon is a prime example: the convenience of being able to receive your order within two days of ordering is relatively

256. Brooke Auxier et al., *Americans' Attitudes and Experiences with Privacy Policies and Laws*, PEW RSCH. CTR. (Nov. 15, 2019), <https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/>.

257. SHOSHANA ZUBOFF, *THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER* 209 (2019) [hereinafter *THE AGE OF SURVEILLANCE CAPITALISM*].

258. Zuboff, *supra* note 231, at 11–12.

259. Jesse Pound, *U.S. Tech Stocks Are Now Worth More Than the Entire European Stock Market*, CNBC (Aug. 28, 2020, 9:08 PM), <https://www.cnbc.com/2020/08/28/us-tech-stocks-are-now-worth-more-than-the-entire-european-stock-market.html>.

260. See Lozano, *supra* note 249, at 301–03; PULVER, *supra* note 247, at 94–95; Zuboff, *supra* note 231, at 11.

261. Avi Goldfarb & Catherine Tucker, *Privacy and Innovation*, 12 INNOVATION POL'Y & ECON. 65, 65–66 (2012).

262. See Zuboff, *supra* note 231, at 11–12, 24–25.

unmatched.²⁶³ This is simply the reality of where we are now. Mall businesses have taken a huge hit during the pandemic, and many have filed bankruptcy.²⁶⁴ Amazon is a company here to stay.

Regardless of personal feelings about the growing power of these types of companies, it is important to eventually ask the realistic question: “What can really be done?” We rely heavily on these companies for basic necessities, and this reliance grows more intensely every year.²⁶⁵ These companies also have benefits for surveillance measures, as the government can reach out to these types of businesses and access a huge amount of consumer information that can be beneficial for the protection of national security.²⁶⁶ At all times, national security must be prioritized for the sake of all people.²⁶⁷ As a leader and advocate of democracy, the world looks to America as an example of what modern democracy can look like.²⁶⁸ As such, it is vital that the country is able to protect itself from outside and internal attacks on democracy through cyberspace.²⁶⁹ Although it may feel uncomfortably vulnerable to subject oneself to such intensive surveillance, the convenience factor is invaluable.²⁷⁰ Particularly during a period where it may not be as comfortable to leave one’s home and do in-person shopping, being able to order virtually any item

263. See, e.g., Christopher Mims, *The Prime Effect: How Amazon’s Two-Day Shipping is Disrupting Retail*, WSJ (Sept. 20, 2018), <https://www.wsj.com/articles/the-prime-effect-how-amazons-2-day-shipping-is-disrupting-retail-1537448425>.

264. Joan Verdon, *Largest U.S. Mall Operator Simon Shuts Down, More Mall Closings Likely*, FORBES (Mar. 19, 2020, 3:15 PM), <https://www.forbes.com/sites/joanverdon/2020/03/19/largest-us-mall-operator-simon-shuts-down-more-mall-closings-likely/?sh=22ce816983ca> (explaining how malls, whose primary business and revenue is derived from in-store customer sales, are financially struggling because of state and federal restrictions on indoor gatherings due to the Covid-19 pandemic).

265. Fang, *supra* note 233; Mitchell, *supra* note 233; Del Valle, *supra* note 232; Zuboff, *supra* note 231, at 11–12, 24–25.

266. Gonzales, *supra* note 244; SRIVASTAVA, *supra* note 245, at 133.

267. SRIVASTAVA, *supra* note 245, at 133.

268. *Id.*; Justin Sherman, *Biden Faces a Steep Challenge to Unite Democracies on Tech*, WIRED (Feb. 24, 2021), <https://www.wired.com/story/opinion-biden-faces-a-steep-challenge-to-unite-democracies-on-tech/>.

269. SRIVASTAVA, *supra* note 245, at 133.

270. Zuboff, *supra* note 231, at 11–12, 24–25.

imaginable is an irreplaceable convenience of life.²⁷¹

With excessive government interference, there is no telling as to whether innovation will continue to push the boundaries of what is possible. In order to continue to be global leaders, countries typically continuously push forward into unexplored ideas.²⁷² For the government to set and enforce limits on what private companies can and cannot do, may have serious repercussions on the perception of the country.²⁷³

VI. LANDMARK LEGISLATION HAPPENING FOR CYBERSPACE THAT WILL LIMIT REACH

Certain companies have faced longstanding accusations of monopolizing the markets, particularly in the social media sector.²⁷⁴ Emerging in the world of domination of the market are two countries: The United States and China.²⁷⁵ Chinese apps like TikTok and WeChat have gained huge popularity in the United States, boasting more than 100 million users in 2020.²⁷⁶ Amidst growing concern over the security issues associated with the Chinese risk to American national security, President Trump threatened to ban the app unless it was sold to an American company.²⁷⁷ Companies like Microsoft emerged as early bidders, but it eventually was announced that Oracle and Walmart

271. *Id.*; Palmer, *supra* note 234.

272. SRIVASTAVA, *supra* note 245, at 134.

273. Goldfarb & Tucker, *supra* note 261, at 65–67, 69; SRIVASTAVA, *supra* note 245, at 134; Sherman, *supra* note 268.

274. PULVER, *supra* note 247, at 96–97; Lozano, *supra* note 249, at 301–03.

275. IMF RSCH. DEP'T, *The Rise of Corporate Market Power and Its Macroeconomic Effects*, in WORLD ECONOMIC OUTLOOK 55 (2019); Steve Goldstein, *Monopoly Power Is Growing Across the Developed World — and It's Hurting Workers*, IMF Finds, MARKETWATCH (Apr. 3, 2019), <https://www.marketwatch.com/story/monopoly-power-is-growing-across-the-developed-world-and-hurting-workers-imf-finds-2019-04-03>; Fang, *supra* note 233.

276. See Jeanne Whalen et al., *U.S. Bans WeChat, TikTok as China Becomes Major Focus of Election*, WASH. POST (Sept. 18, 2020), <https://www.washingtonpost.com/technology/2020/09/18/tiktok-wechat-ban-trump/>.

277. See Paige Leskin, *Trump's Push to Ban TikTok, Explained in 30 Seconds*, BUSINESS INSIDER (Sept. 18, 2020), <https://www.businessinsider.com/donald-trump-tiktok-ban-us-china-explained-in-30-seconds-2020-8>.

would replace ByteDance as the majority shareholders, thus placating President Trump and permitting the app to remain on the U.S. app store.²⁷⁸

Chinese apps are not the only ones facing scrutiny, as Facebook has been particularly targeted for their rapidly acquiring of numerous social media platforms.²⁷⁹ This has included Senate hearings and Federal Trade Commission antitrust lawsuits.²⁸⁰ Their reasonings for these measures circulate largely over the illegal alleged monopoly created by the company.²⁸¹

A) TECH TITANS FACING SCRUTINY OVER GROWING MONOPOLIZATION OF THE INTERNET MARKETS

In a Washington Post article, Sacha Baron Cohen challenged technological CEOs' position in America: "this is ideological imperialism -- six unelected individuals in Silicon Valley imposing their vision on the rest of the world, unaccountable to any government and acting like they're above the reach of law".²⁸² The six unelected individuals in Silicon Valley he speaks of are referencing the six CEOs of technology giants: Mark Zuckerberg of Facebook, Sundar Pichai of Google, Larry Page and Sergey Brin of Alphabet Inc. and Google, Susan Wojcicki of YouTube, and Jack Dorsey of Twitter.²⁸³ The 15-

278. *Id.*; Siladitya Ray & Rachel Sandler, *Oracle And Walmart To Acquire 20% Stake In TikTok, Trump Gives His 'Blessing'*, FORBES (Sept. 20, 2020), <https://www.forbes.com/sites/siladityaray/2020/09/19/oracle-and-walmart-to-acquire-20-stake-in-tiktok-trump-gives-his-blessing/?sh=271cf2b76107>.

279. Cecilia Kang & David McCabe, *Lawmakers, United in Their Ire, Lash Out at Big Tech's Leaders*, N.Y. TIMES (July 29, 2020), <https://www.nytimes.com/2020/07/29/technology/big-tech-hearing-apple-amazon-facebook-google.html>.

280. *FTC Sues Facebook for Illegal Monopolization*, FTC (Dec. 9, 2020), <https://www.ftc.gov/news-events/press-releases/2020/12/ftc-sues-facebook-illegal-monopolization>; Irina Ivanova, *Federal Government and 46 States File Antitrust Suit Seeking to Split Up Facebook*, CBS (Dec. 10, 2020), <https://www.cbsnews.com/news/facebook-antitrust-lawsuit-ftc-46-states-instagram-whatsapp/>; Kang & McCabe, *supra* note 279.

281. Kang & McCabe, *supra* note 279.

282. See Sacha Baron Cohen, *The 'Silicon Six' Spread Propaganda. It's Time to Regulate Social Media Sites*, WASH. POST (Nov. 25, 2019), <http://www.washingtonpost.com/outlook/2019/11/25/silicon-six-spread-propaganda-its-time-regulate-social-media-sites/>.

283. Mary Meisenzahl, *Sacha Baron Cohen Just Called Out the 'Silicon Six,' a*

member House Judiciary Antitrust Subcommittee asked questions of Amazon's Jeff Bezos, Apple's Tim Cook, and Facebook's Mark Zuckerberg, and Google's Sundar Pichai in a July 2020 hearing.²⁸⁴ The popularity of the tech giants with consumers had partially shielded them from strict legislation, but the hearing indicated that circumstances were changing for the "Tech Titans".²⁸⁵

During the hearing, Facebook chief Mark Zuckerberg admitted in an email exchange with Chief Financial Officer (CFO) David Ebersman that his approach towards mergers and acquisitions was to 'neutralize a competitor' and 'integrate their products with ours'.²⁸⁶ This type of language did little to assuage the fears that Facebook was monopolizing the market, and only a few months after the hearing it emerged that Facebook had secured an estimated \$1 billion deal with the customer-service software maker Kustomer in order to bolster efforts to monetize its messaging business.²⁸⁷ Facebook's messaging was expanding to include customer-service products that help companies interact with people via chat apps like WhatsApp and Messenger, the former being another company that Facebook purchased.²⁸⁸

At the end of 2020, the Federal Trade Commission filed an antitrust lawsuit against Facebook that alleged the company was "illegally maintaining its personal social networking monopoly through a years-long course of anticompetitive conduct".²⁸⁹ The primary issue in the

Group of American Billionaires that He Says 'Care More About Boosting Their Share Price Than Protecting Democracy', BUSINESS INSIDER (Nov. 23, 2019), <https://www.businessinsider.com/sacha-baron-cohen-criticizes-silicon-six-billionaires-adl-speech-video-2019-11?op=1>.

284. Kang & McCabe, *supra* note 279.

285. *Id.*

286. See Samuel Stolton, *Facebook Accused of 'Copy, Acquire and Kill' Tactics in US Antitrust Hearing*, EURACTIV (July 30, 2020), <https://www.euractiv.com/section/digital/news/facebook-accused-of-copy-acquire-and-kill-tactics-in-us-antitrust-hearing/>.

287. See Kurt Wagner, *Facebook Buys Customer-Service Software Maker Kustomer*, BLOOMBERG (Nov. 30, 2020), <https://www.bloomberg.com/news/articles/2020-11-30/facebook-buys-customer-service-software-maker-kustomer?sref=dZ65CIng>.

288. *Id.*

289. *FTC Sues Facebook for Illegal Monopolization*, *supra* note 280; Jessica Guynn, *Should Facebook Be Broken Up? FTC, 46 States Sue Tech Giant for*

suit were the \$1 billion purchase of Instagram in 2012 and the \$19 billion purchase of WhatsApp in 2014, forming a dangerously powerful trifecta that allowed Facebook to dominate social media.²⁹⁰ The lawsuit seeks a permanent injunction that could include taking apart the acquisitions of the two companies.²⁹¹ Ian Conner, Director of the FTC's Bureau of Competition stated: "Facebook's actions to entrench and maintain its monopoly deny consumers the benefits of competition. Our aim is to roll back Facebook's anticompetitive conduct and restore competition so that innovation and free competition can thrive".²⁹²

B) RELATIONSHIP BETWEEN BIG TECH AND U.S FEDERAL GOVERNMENT

The government's hearings to confront the heads of Big Tech sends a message to the American people that efforts are being made to combat the monopolization and ownership of the data being taken from users.²⁹³ The amounts of power held by only a few figures was abundantly clear through the flagging of content from politicians during the 2020 Presidential Election, as tech companies made the completely unprecedented move to "filter" certain people.²⁹⁴ This had never happened before, and many felt that it was a move by Big Tech to silence Conservative perspectives.²⁹⁵ A private company has never before had the right to block communication between a president and the people.²⁹⁶

Antitrust Over Instagram, WhatsApp Acquisitions, USA TODAY (Dec. 8, 2020), <https://www.usatoday.com/story/tech/2020/12/08/facebook-antitrust-lawsuits-instagram-whatsapp-mark-zuckerberg/6502309002/>.

290. *FTC Sues Facebook for Illegal Monopolization*, *supra* note 282.

291. *Id.*

292. Gynn, *supra* note 289.

293. *Id.*; Kang & McCabe, *supra* note 279.

294. Rachel Sandler, *Twitter, Facebook Temporarily Block Trump From Posting*, FORBES (Jan. 6, 2021), <https://www.forbes.com/sites/rachelsandler/2021/01/06/twitter-locks-trumps-account-and-threatens-permanent-ban/?sh=397b1cae5c13>.

295. *Id.*

296. Jaclyn Diaz, *Jack Dorsey Says Trump's Twitter Ban Was 'Right Decision' But Worries About Precedent*, NPR (Jan. 14, 2021), <https://www.npr.org/2021/01/14/956664893/twitter-ceo-tweets-about-banning-trump-from-site>.

The monopolization lawsuits also are indicative of action being taken against Big Tech.²⁹⁷ However, it is really to the government's benefit to have these mammoth companies where branches of government, like the Department of Defense, can approach and get data from all types of companies rather than diffusing it out to different businesses. While the FTC lawsuit indicates that they are trying to break up the monopoly because of the extensive power potential, the government also stands to benefit from it.²⁹⁸ These issues of freedom of speech/expression, defense, communication, and surveillance are all overlapping in a way that has never happened before.²⁹⁹

VII. CONCLUSIONS

From its founding, the United States was based on freedom-based notions that we can now view as safeguarding equity, inclusion, disclosure, and accountability.³⁰⁰ This is written into the most fundamental fibers of the Constitution and is vehemently protected today.³⁰¹ However, there is an implicit obligation for the government to be able to step in and protect its citizens.³⁰² In the digital age, this is intrinsically tied with digital security, of which data surveillance is a hugely valuable tool.³⁰³ As major e-commerce companies secure their grasp during the pandemic, a slippery slope emerges in which individual freedoms, collective security, and innovative progress

297. Ivanova, *supra* note 280.

298. Gonzales, *supra* note 244.

299. See generally THE AGE OF SURVEILLANCE CAPITALISM, *supra* note 257, at 8.

300. The Preamble to the United States Constitution reads:

"We the People of the united States, in Order to form a more perfect Union, establish Justice, insure domestic Tranquility, provide for the common defense, promote the general welfare, and secure the Blessings of Liberty to ourselves and our Posterity, do ordain and establish this Constitution for the United States of America." U.S. CONST. pmbl.

301. Carol Harlow, *Accountability and Constitutional Law*, in 1 OXFORD HANDBOOK OF PUBLIC ACCOUNTABILITY 201 (Bovens, Goodin & Schiellmans eds., 2014); Christina Koningisor, *Transparency Deserts*, 114 N.W. L. REV. 1461, 1461–62 (2020); Jonathan Cinnamon, *Social Injustice in Surveillance Capitalism*, 15 SURVEILLANCE & SOC. 609, 611, 613 (2017).

302. Lozano, *supra* note 249, at 310.

303. See SRIVASTAVA, *supra* note 245, at 133.

collide with no simple solution.³⁰⁴

A) THE POLITICS OF TECHNOLOGY

As tech collides more and more frequently with the government, some have come to the conclusion that many of the tech companies have political influence in achieving their own agendas.³⁰⁵ As such, alternatives to the Tech Titans emerged in the aftermath of the 2020 Presidential Election, such as Parler, to give users the opportunity to “speak freely and express yourself openly, without fear of being ‘deplatformed’ for your views”.³⁰⁶

The role of government in controlling the field of technology is highly controversial as it is perceived by some as being overly controlling while others believe that they are within their obligations of protecting the free market and national security.³⁰⁷ When it comes to the abundance of data points and digital surveillance being carried out, little has been done.³⁰⁸ Even when confronted with evidence suggesting ethical issues surrounding the roles that both Facebook and Cambridge Analytica played in the 2016 U.S. Presidential Election, little changed at the federal level.³⁰⁹ A Senate hearing took place, and other than reprimand—Facebook has only continued to grow and track more of its users.³¹⁰ Still, the question of how much can truly be done to combat this issue remains. No one is forced to sign up for social media accounts. People are willingly trading their privacy and rights to have access to their friends, post photos, offer likes, make posts, etc.³¹¹ Users are aware that it is addicting, but at the present moment

304. Lozano, *supra* note 249, at 310.

305. See Farhad Manjoo, *Silicon Valley's Politics: Liberal, With One Big Exception*, N.Y. TIMES (Sept. 6, 2017), <https://www.nytimes.com/2017/09/06/technology/silicon-valley-politics.html>.

306. See generally PARLER, <https://parler.com/> (last visited Mar. 12, 2021).

307. Goldfarb & Tucker, *supra* note 261, at 67.

308. Zuboff, *supra* note 231, at 12.

309. See Ankit Bhatia, *Two Years Since Cambridge Analytica: What has Changed?*, CPO MAGAZINE (May 20, 2020).

310. *Id.*

311. See Cadie Thompson, *What You Really Sign Up for When You Use Social Media*, CNBC (May 20, 2015), <https://www.cnbc.com/2015/05/20/what-you-really-sign-up-for-when-you-use-social-media.html> (stating consumers are giving up their rights to big data when using social media).

this “addiction” is far less troubling than a traditional alcohol or drug addiction.³¹² Despite proof that technology is addictive, users still make tacit consent to allowing the government to scrape through their private details.³¹³ Even with the existence of sites like Parler that encourage free speech, data bytes are still being tracked.³¹⁴

Websites like Zoom, that have been heavily relied upon during the COVID-19 pandemic, have servers in China, crossing international boundaries which raises huge questions for data security and jurisdictional power.³¹⁵ The modern era that is dominated by technology will only continue to evolve.³¹⁶ After two Senate hearings in a matter of a few years, Facebook still went through with its purchase of Kustomer.³¹⁷ While allowing the government to embed itself into the free market and go into head to head combat with American technology companies may not seem ideal, it may be the only choice we have left to preserve our individual rights to data privacy and a competitive market.³¹⁸

312. See Jena Hilliard, *New Study Suggests Excessive Social Media Use is Comparable to Drug Addiction*, ADDICTION CTR. (Sept. 4, 2019), <https://www.addictioncenter.com/news/2019/09/excessive-social-media-use/> (discussing a study that was done to examine the relationship between social media and risky decision-making capabilities).

313. See Thompson, *supra* note 311 (stating that users give up control over their private messages and photos).

314. See Zach Whitaker, *Scraped Parler Data is a Metadata Gold Mine*, TECHCRUNCH (Jan. 11, 2021), <https://techcrunch.com/2021/01/11/scraped-parler-data-is-a-metadata-goldmine/> (stating that Parler has no content moderation policy and collected metadata from many capital rioters that could help in investigations).

315. See Bill Marczak & John Scott- Railton, *Move Fast, and Roll Your Own Crypto: Quick Look at the Confidentiality of Zoom Meetings*, CITIZEN LAB (Apr. 3, 2020), <https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/> (stating that “potential areas of concern in Zoom’s infrastructure, [includes] the transmission of meeting encryption keys through China. . .”).

316. See Kathleen Stansberry et al., *Experts Optimistic About the Next 50 Years of Digital Life*, PEW RSCH. CTR. (Oct. 28, 2019), <https://www.pewresearch.org/internet/2019/10/28/experts-optimistic-about-the-next-50-years-of-digital-life/> (discussing the next 50 years of digital life).

317. See Salvador Rodriguez, *Facebook Acquires Kustomer, a CRM Start-Up*, CNBC (Nov. 30, 2020), <https://www.cnbc.com/2020/11/30/facebook-acquires-kustomer-a-crm-start-up.html> (discussing Facebooks purchase of Kustomer).

318. See Johnathon Wareham, *Should Social Media Platforms Be Regulated?*, FORBES (Feb. 10, 2020), <https://www.forbes.com/sites/esade/2020/02/10/should->

This trifecta of issues—national security, privacy, and innovation—are pressing imminently into virtually every aspect of American life, regardless of whether or not those impacted understand how extensive the implications are for their lives.³¹⁹ COVID-19 has made the dependence on digital and virtual technologies even greater, as people avoid the traditional mediums of brick-and-mortar stores or in-person communication.³²⁰ This in turn simply expands the already numerous data points on individuals.³²¹ Of course, this leads to inevitable questions on the merits of this surveillance.³²² Since there is an abundance of surveillance, there is an expectation that there is a greater purpose for the collections.³²³ If there was ever to be another terrorist attack similar to 9/11 in either scope or style, justifiable outrage would break out and demands for answers as to how could this could have happened again when people have already given up so much privacy in the name of protecting the country from security breaches would take place.³²⁴ Data points are not only kept, but they

social-media-platforms-be-regulated/?sh=4bb9c4783370 (discussing the regulation of social media platforms).

319. See Glen S. Gerstell, *The National-Security Case for Fixing Social Media*, NEW YORKER (Nov. 13, 2020), <https://www.newyorker.com/tech/annals-of-technology/the-national-security-case-for-fixing-social-media> (“[I]t seems as though we are hemmed in on all sides, by our enemies, our technologies, our principles, and the law—that we have no choice but to learn to live with disinformation, and with the slow erosion of our public life.”).

320. See Saheli Roy Choudhury, *More People are Doing Their Holiday Shopping Online and This Trend is Here to Stay*, CNBC (Dec. 14, 2020), <https://www.cnbc.com/2020/12/15/coronavirus-pandemic-has-pushed-shoppers-to-e-commerce-sites.html> (discussing COVID-19’s impact on the online shopping industry).

321. See Suzin Wold, *Perspectives: COVID-19 is Changing How, Why, and How Much We’re Using Social Media*, DIGIT. COM. 360 (Sept. 16, 2020), <https://www.digitalcommerce360.com/2020/09/16/covid-19-is-changing-how-why-and-how-much-were-using-social-media/> (providing statistics based on users’ online usage and their feelings regarding content).

322. See Wareham, *supra* note 318 (discussing the regulation of social media platforms).

323. See Casey Ross, *After 9/11, We Gave Up Privacy for Security. Will We Make the Same Trade-Off After COVID-19?*, STAT NEWS (April 8, 2020), <https://www.statnews.com/2020/04/08/coronavirus-will-we-give-up-privacy-for-security/> (stating that surveillance data collected could be used effectively to protect public health).

324. Cf. John R. Parkinson, *NSA: ‘Over 50’ Terror Plots Foiled By Data Dragnets*, ABC NEWS (June 18, 2013), <https://abcnews.go.com/Politics/nsa->

are stored and then made profit off of.³²⁵ If national security were to be compromised despite people's privacy sacrifices and the profit made upon said data points, it would be a disaster.

A unique relationship between political figures and tech executives exists in which both rely on each other, but both pull for greater power.³²⁶ Tech executives are well-aware that the products they offer are of infinite value to the government due to their storehouse of user data that can be used to protect national security.³²⁷ However, politicians are concerned about the growing monopolization by certain companies and the potential for individual privacy rights being overlooked in the name of data profiteering.³²⁸ Politics also struggles to keep up with the rapid velocity at which technological innovation takes place, meaning that policy governing tech and establishing its boundaries is going to inevitably move much more slowly than tech.³²⁹

director-50-potential-terrorist-attacks-thwarted-controversial/story?id=19428148 (discussing the United States' surveillance of everyone and how it has been instrumental in stopping terrorist attacks).

325. See Thompson, *supra* note 311 (quoting Brad Frazer, an IT lawyer, who said "You are essentially just a commodity, you are big data generating commodity. That's really what you are, that is how social media sees you, with a big dollar sign on your forehead generating big data they can sell. And that is something else you have given up by contract.").

326. See Theodore Schleifer, *Here are the 15 Silicon Valley Millionaires Spending the Most to Beat Donald Trump*, VOX (Oct. 27, 2020), <https://www.vox.com/recode/21529490/silicon-valley-millionaires-top-donors-2020-election-donald-trump> (discussing the political impact of tech executives on silicon valley).

327. Cf. Claire Cain Miller, *Tech Companies Concede to Surveillance Program*, N.Y. TIMES (June 7, 2013), <https://www.nytimes.com/2013/06/08/technology/tech-companies-bristling-concede-to-government-surveillance-efforts.html> (detailing government negotiations with internet companies).

328. See Marcy Gordon, *What's Your Data Worth to Big Tech? Bill Would Compel Answer*, AP (June 24, 2019), <https://apnews.com/article/c897d4f2242047189b62b40b0ea7aadc> (discussing Congress floating legislation that will compel tech giants to disclose what data they are collecting from users and how much that data is worth).

329. See Gary E. Marchant, *The Growing Gap Between Emerging Technologies and the Law*, in THE GROWING GAP BETWEEN EMERGING TECHNOLOGIES AND LEGAL-ETHICAL OVERSIGHT: THE PACING PROBLEM 1, 19 (Gary Marchant, Braden Allenby & Joseph Herkert, eds., 2011) (stating emerging technologies have not evolved rapidly and legislation and judicial review are being left behind by emerging technologies).

This creates a susceptibility for individual privacy concerns, as it cannot be deemed illegal if the laws do not yet exist.³³⁰ Data-storing companies are our most important ally in national security and law enforcement.³³¹ As we try to regulate and break them up, the costs to national security protections must be weighed against these serious complexities.

B) EXTENT OF DATA COLLECTIONS INTERNATIONALLY AND DOMESTICALLY

The collections of data from both the state and federal level are extensive, and Abbie Gruwell writes for the National Conference of State Legislatures (NCSL) saying:

The increasing automation of surveillance and big data analytics through technology that allows for real-time aggregation and analysis of data also presents new privacy challenges. For example, some monitoring systems can use types of machine learning and natural-language processing and neural networks to find patterns in social media posts and potentially reach conclusions about users. Monitoring by state and federal agencies has increased, but regulations may be falling behind.³³²

The speed and technology that agencies have access to are rapidly increasing, but unfortunately the bureaucratic system that creates laws and policies are unable to keep up, thus leaving Americans susceptible to violations of key protections of privacy.³³³ Zuboff wrapped it up in one sentence: “Despite the radical prospects of the ubiquitous connected sensate computational apparatus and the often-repeated claim ‘It will change everything,’ technology firms in the US have,

330. See *id.* at 14 (stating the main law used to govern online privacy is a relic adopted in 1996, and has trouble keeping up with technological advances and is badly out of date).

331. Cf. Tatevik Sargsyan, *Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security*, 10 INT’L J. COMM’N 2221, 2228 (stating it is a consensus among governments that data localization and domestic infrastructure will provide better privacy and security).

332. See Abbie Gruwell, *Privacy and Government Surveillance*, NCSL BLOG (Sept. 23, 2020), <https://www.ncsl.org/blog/2020/09/23/privacy-and-government-surveillance.aspx> (stating “monitoring by state and federal has increased, but regulations may be falling behind.”).

333. See Marchant, *supra* note 329, at 11 (discussing the laws issue with keeping pace with exponentially changed technologies).

thus far, continued their run of relative lawlessness, unimpeded by any comprehensive social or regulatory vision.”³³⁴

These are colossally huge issues that involve controlling both domestic and international terrorism, the rights to individual privacy, and the ability to maintain a competitive market that are overlapping like never before. There may never be a 100% perfect resolution, as the United States will always be a country that elevates freedom as its highest.³³⁵ To have freedom, one must also have a safe space.³³⁶ As such, national security threats must be taken seriously.³³⁷ The advancements in technology have equipped the country to move not only defensively, but also offensively.³³⁸ In order to maintain its status as a leader of the free world, the United States must not lose its ability to adequately and reliably defend itself and its people.³³⁹ The government’s tracking of its citizens begins long before an individual chooses to sign up for social media.³⁴⁰ Social security numbers and credit card information offer the government numerous data points that can be then used to track you if they so wished.³⁴¹ There are certain

334. See *The Age of Surveillance Capitalism*, *supra* note 257, at 190 (“Despite the radical prospects of the ubiquitous connected sensate computational apparatus and the often-repeated claim ‘It will change everything,’ technology firms in the US have, thus far, continued their run of relative lawlessness, unimpeded by any comprehensive social and regulatory vision.”).

335. See J. Rufus Fears, *Freedom: The History of an Idea*, 12 FOREIGN POL. RSCH. INST. 1 (2007) (stating that US foreign policy has been based on the belief that freedom is a universal value and wanted by all people t all times).

336. See WHITE HOUSE NAT’L SEC. COUNCIL, THE NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA, <https://georgewbush-whitehouse.archives.gov/nsc/nssall.html> (last visited Mar. 15, 2021) (discussing defense of the U.S. against enemies).

337. See *id.* (stating that defending the U.S. against enemies is the “first and fundamental commitment of the Federal Government”).

338. See *id.* (stating that terrorists are organized to turn the power of modern technology against the U.S., but the U.S. will use every tool in its arsenal to defeat the threats).

339. See *id.* (stating the U.S. will not allow terrorist efforts to succeed and will build its defenses and coordinate with other countries to curtail enemies).

340. See *NSA Timeline 1791–2015*, ELEC. FRONTIER FOUND., <https://www EFF.ORG/NSA-spying/timeline> (last visited Mar. 15, 2021) (stating the NSA surveillance history began December 15, 1791).

341. See Carolyn Puckett, *The Story of the Social Security Number*, 69 SOC. SEC. BULL. 55, 55 (2019) (stating that one’s social security number is a chief means of

aspects of freedom and privacy that must be compromised in order to guarantee the overall security of the country.³⁴² Although social media has undeniably so opened up doors to extensive scouring of your personal life, it must be recalled that this was a choice freely made by the individual.³⁴³

Many argue that the government should not have the right to carry out surveillance.³⁴⁴ However, 9/11 forever changed the way national security was ensured.³⁴⁵ This new type of terrorist warfare made it absolutely critical that American policies change in order to prevent a recurrence of the tragedy at all costs.³⁴⁶ In order to do this surveillance, the President secured numerous legal opinions to create policies that stated the government could surveil Americans when it rose to levels of threats against national security where citizens could be killed through terrorist actions.³⁴⁷ Electronic surveillance is one of, if not the only, way to limit the power that terrorists have in the modern world.³⁴⁸

identifying and gathering information about an individual).

342. See Ross, *supra* note 323 (stating anything that has the potential to make people less safe even if it gives them back their privacy is less appealing).

343. See Thompson, *supra* note 311 (quoting Brad Frazer who stated “[w]hen you sign up for those terms of service and you click on the ‘I agree’ button, you are also giving away rights to your big data.”).

344. See Erin Herro, *#Unfollowme: 5 Reasons We Should All Be Concerned About Government Surveillance*, AMNESTY INT’L (Mar. 18, 2015), <https://www.amnestyusa.org/unfollowme-5-reasons-we-should-all-be-concerned-about-government-surveillance/> (stating that a survey of over 13,000 individuals revealed more than 70% of respondents were strongly opposed to the U.S. government monitoring their internet use).

345. See Laura Santhanam & Larisa Epatko, *9/11 to Today: Ways We Have Changed*, PBS (Sep. 11, 2018), <https://www.pbs.org/newshour/nation/9-11-to-today-ways-we-have-changed> (stating that the September 11 attacks set in motion events that would change the course of life in the U.S. and around the world).

346. See *id.* (discussing the formation of the TSA as a result of the September 11 attacks).

347. Cf. Conor Friedersdorf, *Obama DOJ: John Yoo Memos on Spying Must Stay Secret*, ATLANTIC (Aug. 30, 2011), <https://www.theatlantic.com/politics/archive/2011/08/obama-doj-john-yoo-memos-on-spying-must-stay-secret/244312/> (stating “Intelligence gathering in direct support of military operations does not trigger constitutional rights against illegal searches and seizures.”).

348. See Sean Sullivan, *NSA Head: Surveillance Helped Thwart More than 50 Terror Plots*, WASH. POST (June 18, 2013), <https://www.washingtonpost.com/news/post-politics/wp/2013/06/18/nsa-head-surveillance-helped-thwart-more-than-50-terror-attempts/> (stating that

Electronic surveillance practices both domestically and internationally led to the capture and assassination of Osama bin Laden, the mastermind behind the 9/11 attacks.³⁴⁹ However, it took ten years, and estimates of the cost put it between \$280 billion and over \$5 trillion.³⁵⁰

The question remains: should we really attempt to reduce surveillance if it is going to reduce terrorism and potentially save innocent American lives? People will lose an undetermined amount of privacy rights, which cannot be pinpointed at the moment as the potential power of technology remains to be seen.³⁵¹ This power then in turn offers the government more potential to control, although they claim that they are using it to fight terrorism.³⁵² This is the reality of the digital world we live in; how can it be possible to maintain some type of individual privacy while also safeguarding to the maximal extent against terrorists?

Our phone calls, emails, text messages, digital communications through social media and messaging apps, are all susceptible to being picked up by United States intelligence agencies through programs

surveillance programs along with other intelligence have protected the U.S. and U.S. allies from terrorist threats across the globe).

349. See Craig Whitlock & Barton Gellman, *To Hunt Osama bin Laden, Satellites Watched Over Abbottabad, Pakistan, and Navy SEALs*, WASH. POST (Aug. 29, 2013), https://www.washingtonpost.com/world/national-security/to-hunt-osama-bin-laden-satellites-watched-over-abbottabad-pakistan-and-navy-seals/2013/08/29/8d32c1d6-10d5-11e3-b4cb-fd7ce041d814_story.html (stating analysts pinpointed the geographic location of a mobile phone that was linked to the compound where bin Laden was hiding).

350. See Stephen Gandel, *How Much Has Osama bin Laden Cost the US?*, TIME (May 3, 2011), <https://business.time.com/2011/05/03/how-much-has-osama-bin-laden-cost-the-us/> (stating Osama bin Laden cost the U.S. anywhere from \$280 billion to \$5 trillion).

351. See Emanuel Gross, *The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—the Proper Balance*, 37 CORNELL INT'L L.J. 27, 36 (2004) (stating that “as the concepts of privacy and national security are difficult to define there is an inherent risk that they will be perceived on an intuitive non rational level, which will undermine the ability to conduct a pertinent discussion of the proper balance that should be drawn between these values in the event of a clash.”).

352. See *id.* at 73 (stating that even though the stated purpose of laws like the Patriot Act are to strengthen law enforcements ability to fight terrorism, many of the provisions are used in ordinary criminal investigations and demonstrate the balance of national security needs over an individual's rights).

that began under the Bush Administration's war on terror but were later continued by Obama and evolved under Trump.³⁵³ Despite numerous significant partisan differences, all three administrations have engaged in surveillance practices—demonstrating the commonality of data surveillance at the governmental level.³⁵⁴ Snowden and other whistleblowers have exposed these actions, causing a global review of U.S. security practices.³⁵⁵ It is important to recognize the government's right and obligation to protect people.³⁵⁶ While people do lose individual rights, a frightening reality for those that disapprove of the surveillance practices, this is the new face of modern national security.³⁵⁷

C) RECOMMENDATIONS FOR PRIVATE LIVING IN A PUBLIC WORLD

While I do suggest there be compromise in terms of ensuring collective safety of the nation as it battles cybersecurity attacks from foreign influences and personal privacy, there also must be commitment from the government to honor its origins as a government by the people and for the people. Efforts should be made to make users aware of how their data can be used, to allow them to make the most

353. See *FAQ: What You Need to Know About the NSA's Surveillance Programs*, PROPUBLICA (Aug. 5, 2013), <https://www.propublica.org/article/nsa-data-collection-faq> (stating the NSA's broad data collection programs were originally authorized by President Bush on October 4, 2001).

354. See Jennifer Williams, *From Torture to Drone Strikes: The Disturbing Legal Legacy Obama Is Leaving for Trump*, VOX (Jan. 10, 2017), <https://www.vox.com/policy-and-politics/2016/11/14/13577464/obama-farewell-speech-torture-drones-nsa-surveillance-trump> (discussing President Bush and President Obama both expanding the power of the executive branch in the realm of national security).

355. See Mark Mazzetti & Michael S. Schmidt, *Ex-Worker at C.I.A. Says He Leaked Data on Surveillance*, N.Y. TIMES (June 9, 2013), <https://www.nytimes.com/2013/06/10/us/former-cia-worker-says-he-leaked-surveillance-data.html> (discussing a former CIA employee who "leaked data on surveillance").

356. See Steven J. Heyman, *The First Duty of Government: Protection, Liberty and the Fourteenth Amendment*, 41 DUKE L.J. 507, 510–11 (1991) (stating protection was one of the fundamental rights of citizenship).

357. See Herro, *supra* note 344 (explaining that the majority of American citizen are opposed to the U.S. government monitoring them).

educated decision when it comes to their digital profile.³⁵⁸ While some may choose to ignore it and sign up regardless, others may find themselves with a better understanding of how to safely navigate this unfamiliar technologically driven world.³⁵⁹

Supporters of surveillance say that the practice must occur in order to protect the physical and economic integrity of the United States and its people.³⁶⁰ Global powers have spies all over the globe, and, recently, ties have been uncovered between a suspected Chinese spy and American politicians.³⁶¹ Amidst these reports, Senator Rick Scott sent a letter to Speaker of the House Nancy Pelosi calling for Eric Swalwell's removal from the House Intelligence committee because of his reported ties to a Chinese spy who was backed by China's Communist Party.³⁶² In the letter, he also described how Representative Swalwell "spent years spreading Russian disinformation in an effort to take down the President, all the while being used as a pawn by the Chinese Communist Party. Representative

358. See Steve Sirich, *Data Transparency in The Age Of Privacy Protection*, FORBES (Mar. 25, 2020), <https://www.forbes.com/sites/forbescommunicationscouncil/2020/03/25/data-transparency-in-the-age-of-privacy-protection/?sh=226f790a46b2> (stating that marketers should be more transparent with consumers on what data they need and why).

359. See *id.* (stating that companies may see better results when marketing to individuals who opt-in, especially if companies help individuals understand how specific marketing benefits them, because such interactions help build trust between the company and the individual using their service or product).

360. Cf. Daniel J. Gallington, *The Case for Internet Surveillance*, U.S. NEWS (Sept. 18, 2013), <https://www.usnews.com/opinion/blogs/world-report/2013/09/18/internet-surveillance-is-a-necessary-part-of-national-security> (stating that there should be no expectation of internet privacy extended to terrorists, spies, and criminals).

361. See Bethany Allen-Ebrahimian & Zach Dorfman, *Exclusive: How a Suspected Chinese Spy Targeted California Politicians*, AXIOS (Dec. 8, 2020), <https://www.axios.com/china-spy-california-politicians-9d2dfb99-f839-4e00-8bd8-59dec0daf589.html> (saying a suspected Chinese intelligence operative developed ties with local and national politicians).

362. See *Senator Rick Scott: Eric Swalwell Has No Place on House Intelligence Committee After Ties to Chinese Spy*, SENATOR RICK SCOTT (Dec. 9, 2020), <https://www.rickscott.senate.gov/senator-rick-scott-eric-swallow-has-no-place-house-intelligence-committee-after-ties-chinese-spy> (stating Senator Rick Scott sent a letter to House Speaker Nancy Pelosi asking for Representative Eric Swalwell's removal from the House Intelligence Committee).

Swalwell refuses to discuss the nature of his relationship with Christina Fang, and it's unclear whether he was communicating with her while he was a member of a House Intelligence Community.”³⁶³ He also urged Speaker Pelosi “to immediately remove Representative Swalwell from his seat on the House Intelligence Committee. Nobody who has access to our nation’s most confidential intelligence should be allowed to maintain contact at any time with the Chinese Communist Party, especially considering that General Secretary Xi is actively working to undermine and harm American interests.”³⁶⁴ There are serious threats to democracy around the world from various countries, and it is important to ensure that those in positions of authority, such as the House Intelligence Committee, have America’s national security in mind.³⁶⁵

At the same time, no one likes to give up privacy.³⁶⁶ Numerous states sued Facebook in 2020 for a variety of violations ranging from antitrust to privacy issues.³⁶⁷ Facebook’s primary argument for their innocence was that their users sign up voluntarily and do it for free.³⁶⁸ In *The Social Dilemma* documentary, Tristan Harris, a former Google design ethicist and now co-founder of the Center for Humane Technology, said “as you don’t pay for the ‘product’, you are the product.”³⁶⁹ Facebook seems to take the stance that when new users

363. *Id.*

364. *Id.*

365. *See id.* (stating that “Swalwell’s failure [was] astounding” and that for national security reasons Swalwell should step down from his position on the House Intelligence Committee).

366. *See Herro, supra* note 344 (stating that 70% of respondents to a poll are opposed to the U.S. government monitoring their internet use).

367. *See* Tony Romm, *U.S., States Sue Facebook as an Illegal Monopoly, Setting Stage for Potential Breakup*, WASH. POST (Dec. 9, 2020), <https://www.washingtonpost.com/technology/2020/12/09/facebook-antitrust-lawsuit/> (stating that the U.S. government and 48 attorney generals filed antitrust suits against Facebook).

368. *See* Elizabeth Schulze, *Facebook Says it Got Users’ Permission to Share Data. Those Users Might Say Differently*, CNBC (Dec. 20, 2018), <https://www.cnbc.com/2018/12/20/facebook-data-sharing-with-amazon-microsoft-netflix.html> (stating that Facebook’s common line of defense is that they handled users data in line with the permission they received from users).

369. *See* Daniel Hövermann, *If You are Not Paying for the Product, You are the Product!*, MEDIUM (Sept. 24, 2020), <https://medium.com/change-your-mind/if-you-are-not-paying-for-the-product-you-are-the-product-4dbc15b9a3f2>; THE SOCIAL

sign up, they know they're giving up some rights.³⁷⁰ Facebook may make it more challenging to terminate your account or change privacy settings, but you still know that you're sharing personal details with people; after all, this is why they sign up in the first place.³⁷¹

This potential for data surveillance is one of the most significant issues of today that is impacting domestic privacy.³⁷² There are many dynamics at play that involve physical, economic, and security risks.³⁷³ Since much of data surveillance is done in secrecy by governmental agencies, we rarely know who is policing the government.³⁷⁴ This raises important issues for which there is no easy answer. As United States policymakers try to digest the changing world regarding foreign actors and technology, they still must try to at least give consideration to the privacy and freedom of its citizens.

Many of America's national security policies were restructured after 9/11 and the people wanted a response to ensure that this horrific act of terrorism would not be repeated.³⁷⁵ These data surveillance practices grew under different presidential administration, ultimately

DILEMMA (Netflix 2020).

370. See Schulze, *supra* note 368 (listing Facebook owner Mark Zuckerberg's comments when saying "I would imagine that probably most people do not read the whole thing. But everyone has the opportunity to and consents to it.").

371. See Kristi Oloffson, *Why is it So Hard to Delete Your Facebook Account?*, TIME (May 14, 2020), <https://newsfeed.time.com/2010/05/14/why-is-it-so-hard-to-delete-your-facebook-account/> (stating Facebook makes it hard to delete your profile because they don't want you to get rid of all of your information).

372. See Erin Kelly, *Surveillance Emerges as Issue in 2016 Race*, USA TODAY (Aug. 17, 2015), <https://www.usatoday.com/story/news/politics/elections/2015/08/17/surveillance-privacy-paul-sanders/31741595/> (stating the debate over government surveillance is emerging as a significant issue in the presidential race).

373. See Daniel J. Gallington, *The Case for Internet Surveillance*, U.S. NEWS (Sept. 18, 2013), <https://www.usnews.com/opinion/blogs/world-report/2013/09/18/internet-surveillance-is-a-necessary-part-of-national-security> (considering policy questions emerging from the technical realities of today's internet).

374. See T.C. Sottek & Janus Kopfstein, *Everything You Need to Know About PRISM*, VERGE (July 17, 2013), <https://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet> (describing PRISM as a tool used by the NSA to collect private electronic data).

375. See Santhanam, *supra* note 345 (discussing changes to air travel and safety following the September 11 attacks).

resulting in Snowden's disclosures, but are now trying to be trimmed back.³⁷⁶ Perhaps the most appropriate and longest lasting result will be enhanced surveillance with some type of oversight, but it has been a painful process where citizens have lost lots of rights and is not unique to the United States.³⁷⁷ Snowden alleged that authorities in the United Kingdom (U.K.) are operating a surveillance system where "anything goes" and their interceptions are more intrusive to people's privacy than what has been seen in the United States.³⁷⁸ This shows that other governments around the world are carrying out surveillance on their citizens, and they are doing it at a frequency higher than the already-alarming rate in the United States.³⁷⁹

The government should attempt to keep the market free for competition and innovation, as this will propel us into the coming years and keep the country competitive with others.³⁸⁰ As our country's technological capacity grows, so also do others.³⁸¹ As such, our capability must not be curbed. There must also be a collaborative approach to this solution, as it is multi-faceted and more complex than at any other point in history.³⁸² Due to data's circulation around the

376. See Jonathan Allen, *NSA to Cut System Administrators by 90 Percent to Limit Data Access*, REUTERS (Aug. 8, 2013), <https://www.reuters.com/article/us-usa-security-nsa-leaks/nsa-to-cut-system-administrators-by-90-percent-to-limit-data-access-idUSBRE97801020130809> (stating that following Snowden's disclosures, the NSA intends to eliminate 90% of its system administrators to reduce the number of people with access to secret information).

377. See Carole Cadwalladr, *Edward Snowden: State Surveillance in Britain Has No Limits*, GUARDIAN (Oct. 12, 2014), <https://www.theguardian.com/world/2014/oct/12/snowden-state-surveillance-britain-no-limits> (discussing the U.K. authorities surveillance system).

378. See *id.*

379. See *id.* (stating that the U.K. authorities are operating an "anything goes surveillance system, one that surpasses the intrusions of the U.S. government[']s surveillance system].").

380. See Wilfred Dolfma & DongBack Seo, *Government Policy and Technological Innovation—a Suggested Typology*, 33 *TECHNOVATION* 173, 177 (2013) (discussing competition in the market and ways to keep the market competitive).

381. Cf. Iman Ghosh, *Ranked: The Most Innovative Economies in the World*, VISUAL CAPITALIST (Feb. 28, 2020), <https://www.visualcapitalist.com/world-most-innovative-economies/> (ranking innovative economies and their best performing metrics).

382. See Dolfma & Seo, *supra* note 380, at 173 (suggesting two dimensions by which to characterize technologies).

world that largely avoids falling securely under the umbrella of any one particular jurisdiction, the United States must work alongside others to create a cohesive response to the issues involving data security in the modern era.³⁸³ Fundamental American freedoms must not take a back seat during this process, but we must agree that there may never be the perfect one-size-fits-all solution.³⁸⁴ There also must be agreement from social media companies that they will carry themselves in an ethically upstanding way that encourages the protection of individual freedoms and rights. While there is also room for truth at the table, the ability to express oneself without fear of suppression or retribution is one of the defining American values that sets the country apart from so many others around the world.³⁸⁵

The issues revolving around data privacy, national security, and continued innovation have no simple resolution. There is no one-size-fits-all quick fix that will resolve every nuance of this technological dilemma. Even if some parts of the power held by Amazon and other massive corporations are broken down by the Senate hearings and FTC lawsuits, the greater movement of dependability on technology will continue gaining momentum. There are differences of opinion and partisan alignment, creating a snowball effect that is certain to dominate the coming decades of American life both during and post-COVID-19. These data points and surveilling measures must be done carefully with respect to the rights to privacy outlined as a human right in both American and international legislation.³⁸⁶ Simultaneously,

383. Cf. Rachel R. Marmor, *The Global Outlook on Data Protection—A World-Wide Approach*, DAVIS WRIGHT TREMAINE LLP BLOG (June 24, 2019), <https://www.dwt.com/blogs/privacy--security-law-blog/2019/06/the-global-outlook-on-data-protection> (stating both the U.S. and European regimes rely on the accuracy of the underlying data so a system that emphasizes accuracy would benefit both models).

384. See *id.* (stating a one-size-fits-all approach means abandoning all consideration of the context in which the data was collected, and may also cost innovation).

385. U.S. CONST. amend. I.

386. Cf. Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST (Aug. 15, 2013), https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html (stating the NSA has broken privacy rules by overstepping its legal authority).

there must be an interplay between these tech giants in order to prevent them from surpassing even government authority, but at the same time, maintaining positive relationship so that the troves of data owned and/or stored by these companies can be relied upon during times of preventative action or crisis in order to protect national security.

This colossal issue is like none other ever experienced before due to the extensive reach on other aspects of American life. One cannot simply shut down these major tech companies and demand total submission to federal regulation because of the lack of clear borders in the cyberspace, reliance on data points for national security, money made from data profiteering, and more.³⁸⁷ Times are changing with the introduction of technology, and although government must establish some boundaries to protect the people from being exploited for financial or political gain, the velocity at which tech moves makes it exceedingly difficult for policy to catch up to them.³⁸⁸ Originally Senate committees dealt with education or veterans affairs, but now also include homeland security, defense, subcommittees on the Internet, and more.³⁸⁹ While it is reassuring to know that the government takes cyberthreats seriously, and likely will continue to do so, the bigger issue is that there is no singular agency or legislative body that is going to get a handle on this and give it architecture.³⁹⁰ This is partly due to the fragmented nature of American government, but does indicate that this will be a lengthy and tedious fight to protect individuals' rights to technological privacy while maintaining power

387. See Alex Hern, *Facebook and Other Tech Giants 'Too Big to Fail'*, GUARDIAN (Aug. 11, 2020), <https://www.theguardian.com/technology/2020/aug/11/facebook-too-big-to-fail-says-oxford-university-research-paper> (discussing research conducted by Oxford University that states that Facebook and other tech-giants are too big to fail).

388. See Marchant, *supra* note 329, at 19 (stating the main federal law governing online privacy is outdated and has trouble keeping up with technological advances).

389. See *generally Committees of the U.S. Congress*, CONGRESS.GOV, <https://www.congress.gov/committees> (last visited Apr. 20, 2021) (listing the armed services and homeland security committees).

390. See Ray Rothrock, *As Cyberthreats Grow, Cybersecurity Should Be Centralized*, GOVERNING.COM (Dec. 20, 2019), <https://www.governing.com/news/headlines/As-Cyberthreats-Grow-Cybersecurity-Should-Be-Centralized.html> (stating military law enforcement and civilian agencies each have their own approaches to readiness and resiliency with no strategic coordination).

and authority over cyber threats and warfare in the modern world.³⁹¹

391. *See id.* (stating cyber threats challenge the United States economy, military, national security, and its infrastructure, and that the federal government must act definitively in addressing such threats).