Northwestern Journal of International Law & Business

Volume 41
Issue 2 *Winter*

Article 3

Winter 2021

Outsourcing the Police: How Reliance on the Private Sector for Law Enforcement Threatens Privacy Legislation Around the World

Karl Colbary

Vol. 41, No. 2
Northwestern Journal of International Law & Business

Outsourcing the Police: How Reliance on the Private Sector for Law Enforcement Threatens Privacy Legislation Around the World

Karl Colbary

Abstract

Data privacy is an increasingly important issue in the world today. People are increasingly aware of, and concerned about, their digital footprint. As a result, many jurisdictions around the world—the United States excluded—have enacted legislation with an eye towards giving their citizens greater control over their data. However, the movement to give individuals greater control over how their data is used by tech providers often overlooks the fact that the government is one of the biggest consumers of the data that tech providers collect. Therefore, data privacy regimes that allow the flow of personal information to the government do not meaningfully protect individual privacy. As the people of the United States continue to debate how to best safeguard their personal information, they should be mindful of how law enforcement demand for their information can undermine those efforts.

This note begins by observing how the current legal framework in the United States is ill equipped to deal with the privacy issues of an increasingly digital world. Then, it examines the impact that data privacy legislation in China and Europe has had on the relationship between tech companies and law enforcement. Finally, by applying the lessons learned in China and Europe, this note attempts to predict how efforts to protect consumers' data privacy may work in the United States. Ultimately, this note argues that, because law enforcement in the United States is reliant on the data collected by the private sector, meaningful data privacy reform is likely impossible unless it applies to both the private sector and government equally.

TABLE OF CONTENTS

I. Introduction 216
II. United States 217
A. Privacy Law 217
B. Government Access to Personal Data.....218
III. Privacy and Law Enforcement Around the World 223
A. Data Privacy Law in China and the European Union.....223
B. Government Access to Data in the EU and China.....228
IV. Private Providers and Government Surveillance.....231
V. Conclusion 240

I. INTRODUCTION

All around the world, governments are trying to play catch up and respond to the privacy implications of the swift expansion of an economy based on monetizing users' personal data. Not only are more people than ever connected to one another, it is also a near impossibility for individuals to live in today's world without their personal data being collected and used by a third party down the road. As a result, governments around the world have been compelled to amend or craft new law to give their citizens better control over how their data is used by third parties. At the same time, those same governments, also with the goal of protecting their citizens, are actively encroaching on the very same privacy interests to further their law enforcement and national security goals.

Much of the current discussion regarding data privacy focuses on how tech providers such as Google and Facebook collect and monetize our data. The focus of this note is, instead, how law enforcement uses that data. As we will see, there is not necessarily a bright line separating the two spheres. An entire industry has emerged that monetizes personal data by selling law enforcement services to government. But, as a general matter, the recent trend of governments expanding personal data privacy protections is antithetical to the desires of law enforcement to get their hands on as much of that personal data as possible.

At first glance, it may seem that the use of personal data by private actors in a commercial context is entirely separate from the government's use of personal data. However, this note will argue that they are inextricably linked, and that modern law enforcement and government surveillance necessarily rely on the broad collection and processing of user data by private actors. As discussed below, this includes everything from social media to an individual's shopping history. Just as individual people have come to rely on these things in their day to day lives, so have governments. In effect, private collection of user data is the faucet from which law enforcement drinks.

This note will analyze the dynamic between the government's attempts to protect the data privacy of its citizens from private actors while law enforcement agencies are simultaneously collecting as much of that same information as possible. This note will employ a comparative approach by contrasting different data privacy and surveillance schemes in the United States to the schemes in the European Union and China.

Part II of this article will discuss in some detail the current privacy law in the United States and how it has enabled law enforcement to build an expansive surveillance framework. Part III examines current privacy law innovations in the European Union and China with an eye towards how that legislation can thwart government law enforcement goals. In Part VI, this article will examine the impact these different privacy schemes have on private tech providers. This article then concludes with a discussion of what

impact privacy law will have going forward in this area.

II. UNITED STATES

A. Privacy Law

The United States, unlike the European Union or even China, has not enacted any broad data privacy legislation.[1] Unfortunately, this means that understanding United States privacy law is not as simple as just looking up the relevant statute. Any discussion of the privacy law landscape in the United States necessarily requires a careful examination of the underlying case law and its history. To the extent statutory legal protection exists, it is in the form of sector-specific legislation that applies only to specific industries such as healthcare and financial services.[2] The U.S. Constitution does not provide a fundamental right of data privacy; to the extent such a constitutional right exists in the United States it has developed through case law.[3]

These privacy rights, where they do exist, are ill suited to deal with twenty-first century data privacy concerns. Privacy rights found in the U.S. Constitution are generally derived from the Fourth Amendment prohibition on "unreasonable searches and seizures" and place restrictions on state, not private, conduct.[4] In the physical world, the scope of the protections offered by the Fourth Amendment are fairly easily defined and understood by applying an inside/outside test where the "entering [of] enclosed spaces ordinarily constitutes a search that triggers the Fourth Amendment."[5] Alternatively, where a person is out in the open, where there is no "reasonable expectation of privacy," the Fourth Amendment does not operate.[6]

In the context of the internet and data stored electronically, the inside/outside test fails us.[7] Further, much of our Fourth Amendment jurisprudence fails to protect electronically stored data. The biggest factor is the "third-party doctrine," the Fourth Amendment rule that a person forfeits their Fourth Amendment rights with regards to information that they disclose to a third party.[8] The third-party doctrine has been roundly

---

[1] Nicholas F. Palmieri III, *Data Protection in an Increasingly Globalized World*, 94 IND. L.J. 297, 306 (2019).

[2] *Id.* at 323.

[3] *Id.*

[4] *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1017 (2010).

[5] *Id.* at 1010.

[6] *Id.*

[7] *Id.* at 1012.

[8] Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563 (2009).

criticized by commentators and state Supreme Courts alike.[9] A strict application of the third-party doctrine to the modern day leads to an absurd result: no person has a "reasonable expectation of privacy" for any information stored with a provider.[10] This simply cannot be the case.

The U.S. Supreme Court, since establishing the third-party doctrine in *Smith v. Maryland*,[11] has shown some appetite for narrowing the scope of the doctrine as it applies to electronically stored data.[12] To the extent that the pendulum has started to swing away from the third-party doctrine, the phenomenon is most on display in *Carpenter v. United States*. In *Carpenter*, the Court ruled that law enforcement needed a warrant in order to obtain a person's cell site location information—information about the location of a cell phone each time it connects to a cell site—from the cell phone service provider.[13]

The Fourth Amendment protections do not extend to a general right of privacy.[14] The right to be "left alone" and free from intrusion into one's personal affairs by other persons is left to the law of other states.[15] To that end, California is the first state that has passed legislation in this area: The California Consumer Privacy Act which, in many ways, mirrors the European Union's General Data Protection Regulation (GDPR).[16] Much like the GDPR, as discussed below, it is not yet clear what effect the CCPA will have. However, it is likely that, as a state law, it will be less effective at curbing the surveillance efforts of the federal government.

B. Government Access to Personal Data

In February 2018, the U.S. Supreme Court heard arguments in *United States v. Microsoft*,[17] a case that sought to answer the question of whether or not the United States government could compel an American email service provider to comply with a warrant under the Stored Communications Act (SCA)[18] for material under the provider's control

---

[9] *Id.* at 564.

[10] *See* Carpenter v. United States, 138 S.Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting).

[11] Smith v. Maryland, 442 U.S. 735, 744-45 (1979) ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

[12] *See e.g.*, Riley v. California, 573 U.S. 373, 403 (2014) ("The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.").

[13] *Carpenter*, 138 S.Ct. at 2221.

[14] *See* Katz v. United States, 389 U.S. 347, 350 (1967) (there is no "general 'constitutional right to privacy'").

[15] *Id.* at 350-51.

[16] *See* DataGuidance and Future of Privacy Forum, *Comparing Privacy Laws: GDPR v. CCPA*, FUTURE OF PRIVACY FORUM (Nov. 2018), https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

[17] United States v. Microsoft Corp., 138 S.Ct. 1186 (2018).

[18] 18 U.S.C. § 2703 (2010).

where the provider has decided to store the material abroad. The SCA, enacted in 1986, provides authority for the government to compel a communications service provider to disclose content of materials stored electronically responsive to a court order.[19] The SCA did not contemplate the present-day reality that such information is often stored on servers all over the world.

The lower court in *Microsoft*, the Second Circuit Court of Appeals, held that the SCA did not allow the government to compel a provider to produce content responsive to a court order.[20] However, a Pennsylvania District Court ruled contrary to the Second Circuit's holding in *Microsoft* in a similar case involving information stored by Google.[21] *Google Pennsylvania* was distinguishable from *Microsoft* as the two providers used different underlying cloud models. The storage method used by Microsoft, known as data localization, is where a provider stores information in a cloud "that is restricted to a single country or region."[22] The method used by Google, known as data shard storage, is where a provider "operates a cloud network that 'automatically moves data from one location on Google's network to another.'"[23]

Under the SCA as it existed when these cases were decided, without the authority to compel disclosure via court order, the U.S. government would have to go through diplomatic channels and request the information through the government where the data was stored. In the case of *Microsoft*, this was straightforward enough; the server was located in Ireland so the United States would have to petition the Irish government to compel Microsoft to comply with the court order. As we will see, this was, and remains, an imperfect procedure, but there was at least a framework in place to deal with these issues.

The data shard storage used in *Google Pennsylvania* complicated the government's ability to avail itself of this diplomatic option. Data shard storage involves constantly moving data around between servers, and, as a result, it may be impossible for Google to know exactly where the physical location of a particular content is at any given time. Therefore, the government cannot submit a request with a foreign state because it is impossible to know which state to ask. Further, it is also possible for the

---

[19] *See id.* § 2703(a) ("A governmental entity may require the disclosure . . . pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction.").

[20] *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016), *vacated and remanded sub nom.* United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

[21] *In re* Search Warrant No. 16-960-M-01, 232 F. Supp. 3d 708 (E.D. Pa. 2017) ("*Google Pennsylvania*"), *aff'd*, 275 F. Supp. 3d 605 (E.D. Pa. 2017).

[22] Paul M. Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV. 1681, 1696 (2018).

[23] *Id.* at 1695.

"shards" that make up the content in question to be stored in many different places at once. Effectively, if the government could not compel Google, or any provider using data shard storage, to produce content responsive to a court order under the SCA, there may not have been another option.[24]

Given the discord on the issue within a single circuit, and indeed throughout the country, this was clearly a question that needed to be answered. Before the Court could rule in *Microsoft*, Congress enacted the Clarifying Lawful Overseas Use of Data (CLOUD) Act as part of an over 2,000-page omnibus budget bill.[25] The CLOUD Act was passed with the support of many cloud storage providers, including Microsoft and Google.[26]

The CLOUD Act contained two main parts. The first part amended the SCA and provided the government with the authority to compel compliance with a warrant in cases where the subscriber was in the United States and the production of responsive material would happen in the United States. This answered the question before the Court in *Microsoft*, and the case was dismissed as moot.[27]

There is little question that it was necessary to amend the SCA.[28] The SCA itself was enacted because technology had begun to outpace the law. Before the SCA, there was little protection for electronic information stored with third parties. The Fourth Amendment, because of the third-party doctrine, afforded little protection.[29] Congress, by enacting the SCA, was acknowledging that, as technology changed, so too must the law. With that in mind, it is almost hard to believe that it took another thirty-three years before Congress addressed the issue again. It is also alarming that, when they finally did take up the issue, they passed the CLOUD Act in a rush, tacked onto a 2,232-page omnibus budget bill without review by a committee in either house.[30]

The CLOUD Act also went a step further than simply amending the SCA to solve the extraterritorial issue in *Microsoft*. The second part

---

[24] *Google Pennsylvania*, 232 F. Supp. 3d at 723-25.

[25] Consolidated Appropriations Act of 2018, Pub. L. No. 115-141, 132 Stat. 348, 1212-25.

[26] Letter from Apple, Google, Microsoft, & Oath to Sens. Orinn Hatch, Christopher Coons, Lindsey Graham, & Sheldon Whitehouse (Feb. 6, 2018), https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf [hereinafter, Letter from Apple, Google, Microsoft].

[27] After the enactment of the CLOUD Act, the government served Microsoft with a new warrant under that authority. The Court remanded the case back to the Second Circuit with instructions to dismiss the case as moot. United States v. Microsoft Corp., 138 S. Ct. 1188 (2018).

[28] *See* Christine Galvagna, *The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform*, 9 NOTRE DAME J. INT'L & COMP. L. 57, 58 (2019).

[29] *See* Kerr, *supra* note 8.

[30] *See* David Ruiz, *Responsibility Deflected, the CLOUD Act Passes*, ELEC. FRONTIER FOUND. (Mar. 22, 2018), https://www.eff.org/deeplinks/2018/03/responsibility-deflected-cloud-act-passes.

empowered the Attorney General to enter into executive agreements with foreign countries, lifting the blocking provisions in the SCA on a country-by-country basis.[31] It is the second part of the CLOUD Act that has the greatest privacy implications.

Part two of the CLOUD Act allows the Attorney General to enter into such agreements only when the other country's law "affords robust and procedural protections for privacy and civil liberties in light of the data collection and activities that the foreign government that will be subject to the agreement."[32] The CLOUD Act includes a non-exhaustive list of factors that the Attorney General should consider, such as prohibitions against torture and fair trial rights, but does not make any of the factors mandatory, or otherwise assign weight to any of the factors.

Further, the ability to review or oversee the implementation of agreements made under the CLOUD Act is, simply put, non-existent. The Attorney General is charged with drafting, entering, and maintaining the agreements. The Act does include a provision that the foreign government must agree to a periodic review by the United States government.[33] However, there is no requirement that the U.S. government actually conduct such review. Further, even if such review were to be conducted, it would not necessarily be conducted by the Attorney General.

There is no mechanism for the content of the agreements to be disclosed. The first country that the United States has entered an agreement with is the United Kingdom. The U.S. government declined to release a draft of the agreement prior to its ratification and did not release the content of the agreement afterwards. There have been reports that other countries have discussed entering into such agreements with the United States, but there are few publicly available details.[34] There are some parallels to this such as the secret treaty that formed the basis of the United States-United Kingdom spy alliance that led to the creation of the Five Eyes alliance: the intelligence alliance comprised of the United States, United Kingdom, Canada, Australia, and New Zealand.[35] Given the general distrust of the international community regarding the actions of the United States and its allies, the fact that the U.S. government will not disclose even who it has discussed such agreements with will surely raise eyebrows. For instance, if the United States were to have only negotiated agreements with other Five

---

[31] Jennifer Daskal, *Privacy and Security Across Borders*, 128 Yale L.J. F. 1029, 1038 (2019).

[32] CLOUD Act §105, 18 U.S.C. § 2523(b)(1).

[33] *Id.* at § 2523(J).

[34] *See, e.g.*, Joint Statement Announcing United States and Australian Negotiation of a CLOUD Act Agreement by U.S. Attorney General William Barr and Minister for Home Affairs Peter Dutton, DEP'T OF JUST. (Oct. 7, 2019), https://www.justice.gov/opa/pr/joint-statement-announcing-united-states-and-australian-negotiation-cloud-act-agreement-us.

[35] Leo Kelion, *NSA-GCHQ Snowden Leaks: A Glossary of Key Terms*, BRITISH BROAD. CORP. (Jan. 28, 2014), https://www.bbc.com/news/technology-25085592.

Eyes nations, or with Israel, but not nations such as Germany and France, this would undoubtedly have an impact on international relations with the United States, as well as American companies.

The effect is that the standards set out for the Attorney General to follow are—much like the Pirate Code—mere guidelines rather than actual standards.[36] As the chief law enforcement officer, it is hard to imagine an Attorney General protecting individual privacy interests at the expense of more expansive law enforcement powers.

This is not to say that the part two of the CLOUD Act is an answer in search of a problem. In the investigation underlying *Microsoft*, the U.S. government made a conscious decision to pursue a warrant under the SCA, despite the fact that the law was unsettled. There was another, well-established, method through which the government could have sought the data that Microsoft had stored on its servers in Iceland: Mutual Legal Assistance Treaties ("MLAT").[37]

The United States is a party to more than fifty bilateral MLATs, as well as similar agreements with the European Union and foreign states.[38] Requests made under MLATs are processed on a case-by-case basis. The requesting state reaches out to the government with jurisdiction over the property and then waits for the government to respond.[39] This process is slow, and particularly ill-suited with regards to digital evidence.[40] Meanwhile, the number of MLAT requests has grown exponentially.[41]

Other than the general inefficiency and inefficacy of the MLAT process, there was no reason why the government could not have used the MLAT process in the case underlying *Microsoft*. The magistrate in the District Court, in support of the issuance of the warrant, noted that the "slow and laborious" MLAT procedures constituted such a "substantial"

---

[36] *See* Sabrina A. Morris, *Rethinking the Extraterritorial Scope of the United States' Access to Data Stored by a Third Party*, 42 FORDHAM INT'L L.J. 183, 213 (2018) (observing that the statute "provides only *factors, not requirements*" that the Attorney General must consider before approving a data sharing agreement and noting that the agreements are not subject to judicial review)(citation omitted); Captain Hector Barbossa, PIRATES OF THE CARIBBEAN: THE CURSE OF THE BLACK PEARL (Walt Disney Pictures and Jerry Bruckheimer Films 2003) (40:50) ("The Code is more what you'd call guidelines than actual rules.").

[37] See Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. L. SCH. NAT'L. SECURITY J. (Jan. 28, 2015), https://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/ for an overview of the MLAT process.

[38] RESTATEMENT (FOURTH) OF THE FOREIGN RELATIONS OF LAW OF THE U.S. § 429 Reporter's Note 1 (AM. LAW INST. 2018).

[39] Daskal, *supra* note 31 at 1034.

[40] Morris, *supra* note 36 at 203-04.

[41] The Department of Justice estimates that number of MLAT requests "has increased by nearly 60 percent and the number of requests for computer records has increased ten-fold." U.S. Dep't of Just., *FY 2015 Budget Request* (July 13, 2014), retrieved from http://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf

burden on the government as to necessitate another option.[42] A general desire for another option is likely what motivated the government to forgo the MLAT process and seek the content through a warrant; the ensuing legal fight was worth fighting.

III. PRIVACY AND LAW ENFORCEMENT AROUND THE WORLD

This section will examine the privacy law landscape in the European Union and China. While it may seem like an odd paring at first glance, contrasting privacy law schemes between these two jurisdictions specifically helps illuminate how government law enforcement's interests can work to thwart even the most comprehensive privacy protections.

A. Data Privacy Law in China and the European Union

In 2016, the European Union passed its landmark privacy legislation, the General Data Protection Regulation ("GDPR").[43] It has been recognized as one of the strongest and most comprehensive attempts by a government to safeguard individuals' personal data.[44] The GDPR is part of a larger trend of the European Union's attempts to help protect the privacy of its citizens. The Data Protection Directive, adopted by the E.U. in the 1995, required "each of the twenty-eight Member States to enact national legislation that protects 'the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.'" [45] In 2014, the Court of Justice of the European Union recognized a "right to be forgotten."[46]

Despite the relative inaction on the part of the United States, the European Union is not the only jurisdiction which has sought to enact strong statutory individual privacy protections. China has enacted privacy laws that, on their face, are as comprehensive as the GDPR.[47] Though there are many reasons why the Chinese privacy laws have not received the same attention—the EU is a first mover and a longtime ally of the United States—it must also be due, at least in part, to China's past abuses in this area.[48] Simply put, it is easy to dismiss Chinese privacy protections because

---

[42] *In re A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466, 474 (S.D.N.Y. 2014) (citing Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. Pa. L. Rev. 373, 409 (2014)).

[43] Commission Regulation 2016/679, 2016 O.J. (L119).

[44] *The EU General Data Protection Regulation*, HUMAN RIGHTS WATCH (June 6, 2018, 5:00 AM). https://www.hrw.org/news/2018/06/06/eu-general-data-protection-regulation#.

[45] Michael L. Rustad & Thomas H. Koenig, *Towards a Global Data Privacy Standard*, 71 Fla. L. Rev. 365, 373-74 (2019) (citing Council Directive 95/46/EC, art. 1).

[46] Case C-131/12, *Google Spain SL v. Agencia Espanola de Proteccion de Datos*, 2014 E.C.R. 317 (2014).

[47] Griffen Thorne, *GDPR Meets its Match . . . in China*, CHINA LAW BLOG (July 14, 2019), https://www.chinalawblog.com/2019/07/gdpr-meets-its-match-in-china.html.

[48] *See, e.g.*, Nithin Coca, *China's Xinjiang Surveillance is the Dystopian Future Nobody*

many believe that the Chinese government, and perhaps the Chinese culture broadly, traditionally do not value individual privacy.[49]

However, this attitude towards Chinese privacy legislation misses the point. In some respects, the Chinese law places even greater burdens on providers before they collect and use personal data, especially with regards to gaining user consent.[50] Companies doing business in China, including those from the United States or European Union, must comply with these standards just as they must with the GDPR in Europe. Both the GDPR and Chinese law require companies with no physical presence in the respective jurisdictions to comply with the law.[51] It is true that the goal of Chinese privacy law may not so much be the protection of privacy itself but the goal of the Chinese government to protect its internet and domestic providers from foreign companies.[52] This does not change the fact that these standards still have the impact of protecting the data privacy of its citizens, though it may not be the driving force.

Further, it is not yet clear whether the GDPR will be able to achieve its lofty goals. Despite its history of legal protections for individual data privacy, such regulations in Europe have not always proven effective.[53]

Wants, ENGADGET (Feb. 22, 2018), https://www.engadget.com/2018-02-22-china-xinjiang-surveillance-tech-spread.html (observing that the Chinese government shut off the internet following deadly protests in 2009); Chris Buckley, *Crackdown on Bloggers is Mounted by China*, N.Y. TIMES (Sept. 10, 2013), https://www.nytimes.com/2013/09/11/world/asia/china-cracks-down-on-online-opinion-makers.html (discussing the arrest of bloggers critical of the Chinese government).

[49] *See, e.g.*, Xiaofeng Lin, *A Dangerous Game: China's Big Data Advantage and How the U.S. Should Respond*, 2020 U. ILL. J.L. TECH. & POL'Y 253, 269-70 (2020) (contrasting the American concept of "privacy as a fundamental human right" with the traditional Chinese cultural view that privacy "has a negative connotation"); Tiffany Li, Zhou Zhou & Jill Bronfman, *Saving Face: Unfolding the Screen of Chinese Privacy Law*, J.L., INFO., & SCI., 5 (forthcoming), https://papers.ssrn.com/abstract=2826087 ("The idea of an individual having the right to an intangible concept like *privacy* . . . was [] relatively unheard of."); Ann Bartow, *The Second Wave of Global Privacy Protection: Privacy Laws and Privacy Levers: Online Surveillance Versus Economic Development in the People's Republic of China*, 74 OHIO ST. L.J. 853, 856 (2013) (observing that "longstanding social norms" thwart individual freedom protections and that "Chinese citizens participate in a culture of peer observation and orchestrated scrutiny"); *cf.* Clay Chandler & David Z. Morris, *China's Lax Attitude About Privacy is Shifting – Data Sheet*, FORTUNE (Aug. 20, 2019, 2:03 PM), https://fortune.com/2019/08/20/china-privacy-data-sheet/ (observing that the traditional notion that "Chinese culture generally doesn't place the same value on privacy that Western culture does" is changing); Harrison Jacobs, *Chinese People Don't Care About Privacy on the Internet — Here's Why, According to a Top Professor in China*, INSIDER (June 26, 2018, 1:08 PM), https://www.businessinsider.com/why-china-chinese-people-dont-care-about-privacy-2018-6 (comparing the more subdued reaction to revelations regarding misuse of data in China to similar events in the United States and Europe that sparked outrage in part because "[They] don't have privacy in China traditionally").

[50] Thorne, *supra* note 47.

[51] *Id.*

[52] *Id.*

[53] Neil Hodge, *Privacy Advocate Schrems Foresees Lax Enforcement of GDPR*,

There are reasons to believe that the GDPR itself may suffer from some of the same issues as the laws that came before it.[54] Ultimately, it will take some time before we know just how effective the GDPR will be. As with any new law, the rights and duties of providers under the GDPR will crystalize over time as people and companies challenge competing interpretations and practices. To that end, there is reason to be bullish on the real-world impact that the GDPR will ultimately have. Google is still the largest lobbyist in the European Union and the United States.[55] Meanwhile, at the other end of the spectrum, the GDPR has had an adverse effect on European tech startups.[56] Beyond the tech industry, there is evidence that the GDPR has had a negative impact on the economy of the European Union as a whole.[57] This is all in addition to the direct cost to European governments of enforcing the GDPR. Companies doing business in the European Union, rather than risk being penalized for failing to comply with the European Union, have overreported potential issues to regulators.[58] The result has been that regulators have struggled to keep up with the increased workload under the GDPR.[59] Despite all of the costs, the European people—the people the GDPR was enacted to protect—do not believe that they have any more control over their data, nor has it increased trust on the internet.[60]

Given the many costs of the GDPR, it is easy to see how the law may fail to live up to its potential. A foreseeable outcome of the law is to restrict the growth of new tech companies in Europe and large providers such as Facebook and Google are able to use their influence and resources to either change or avoid the law. A common criticism of large tech companies is the practice of buying startups and preventing them from growing into

---

COMPLIANCE WEEK (Nov. 28, 2018 3:30 AM), https://www.complianceweek.com/data-privacy/privacy-advocate-schrems-foresees-lax-enforcement-of-gdpr/24736.article (observing that the EU data protection directive that proceeded the GDPR was ineffective as it made more financial sense for companies to ignore the law and pay the penalties).

[54] *Id.*

[55] SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 124-25 (PublicAffairs 2019).

[56] *See generally* Jian Jia et al., *The Short-Run Effects of GDPR on Technology Venture Investment* (Nat'l Bureau of Econ. Res., Working Paper No. 25248, Nov. 8, 2019), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912.

[57] Merrill Corp., *GDPR Burdens Hinder M&A Transactions in the EMEA Region*, (Nov. 13, 2018), https://www.merrillcorp.com/us/en/company/news/press-releases/gdpr-burdens-hinder-m-a-transactions-in-the-emea-region.html.

[58] Catherine Stupp, *European Privacy Regulators Find Their Workload Expands Along With Authority*, WALL ST. J. (Apr. 12, 2019 7:44 AM), https://www.wsj.com/articles/european-privacy-regulators-find-their-workload-expands-along-with-authority-11555061402.

[59] *Id.*

[60] Eline Chivot, *What the Evidence Shows About the Impact of the GDPR After One Year*, CTR. FOR DATA INNOVATION (June 17, 2019), https://www.datainnovation.org/2019/06/what-the-evidence-shows-about-the-impact-of-the-gdpr-after-one-year/.

competitors.[61] Indeed, to this point the GDPR has resulted in Google receiving more user data than it did before.[62] If this trend continues, the negative impact on the economy as a whole does not reverse, public sentiment does not change, and the cost to regulators remains high, countries in the European Union may start underenforcing the GDPR, just as has happened with previous data privacy schemes in the European Union. It is possible that this is already occurring. At least three member states of the European Union have yet to fully adapt their national legislation to the standards required by the GDPR.[63]

Of course, it is still early. It is possible for the European Union to work out the kinks. Even if the GDPR does not accomplish everything it set out to, as the most comprehensive privacy legislation in the world, it may still achieve quite a lot. On the other hand, acknowledging that the future of the GDPR is uncertain is also acknowledging there is a possibility that it might fail. It then becomes appropriate to wonder what is so special about the GDPR that has earned it praise from privacy advocates who, at the same time, have not quite embraced similar privacy protections in China. There are any number of explanations. China has long criticized the Western media of being biased against China.[64] Though western bias almost certainly plays some role, another factor is likely the motivation behind the laws themselves. The motivation behind the GDPR is the protection of individual personal privacy, whereas the motivation behind Chinese privacy law is the protection of Chinese interests.[65] There seems to be a belief that, because the guiding principle behind the GDPR is the protection of individuals, that enforcement and adjudication of the GDPR will, on the whole, reflect this principle.

On the other hand, where the Chinese government is motivated by protecting China, any conflicts will be resolved in favor of the government rather than individual privacy interests. Personal privacy concerns have not prevented the Chinese government from establishing an expansive surveillance state.[66] Much of the infrastructure behind the current surveillance framework in China relies on its ability to filter and control the

---

[61] Richard Waters, *Big Tech's 'buy and kill' tactics come under scrutiny*, FIN. TIMES (Feb. 13, 2020), https://www.ft.com/content/39b5c3a8-4e1a-11ea-95a0-43d18ec715f5.

[62] Björn Greif, *Study: Google is the Biggest Beneficiary of the GDPR*, CLIQZ (Oct. 10, 2018), https://cliqz.com/en/magazine/study-google-is-the-biggest-beneficiary-of-the-gdpr.

[63] Chivot, *supra* note 60.

[64] Bethany Allen-Ebrahimian, *How China Won the War Against Western Media*, FOREIGN POL'Y (Mar. 4, 2016, 1:09 PM), https://foreignpolicy.com/2016/03/04/china-won-war-western-media-censorship-propaganda-communist-party/.

[65] Thorne, *supra* note 47.

[66] Anna Mitchell & Larry Diamond, *China's Surveillance State Should Scare Everyone*, THE ATLANTIC (Feb. 2, 2018), https://www.theatlantic.com/international/archive/2018/02/china-surveillance/552203/.

internet.[67] The Chinese government has worked towards developing a social credit system—an attempt to place a value on each citizen's social and political behavior—by keeping track of each communication, transaction, and website visit made by its citizens.[68] Similar data collection has fueled China's predictive policing efforts.[69] Enabled by its vast surveillance network, law enforcement assigns a "score" for certain activities, such as praying regularly or leaving the house through the back door, and arrests people with scores below a certain threshold or people deemed threats by an algorithm.[70] Such efforts make it clear that, however concerned the Chinese government is with protecting the personal information of its citizens, it is more concerned with protecting the Chinese government.

Though there is certainly room to debate the true motivations of the EU and China in enacting their otherwise similarly comprehensive privacy protection schemes, it is clear that there is more skepticism of China's efforts because they prioritize state interests over those of individuals. This, however, assumes that the European Union, and by extension the GDPR, is not susceptible of falling into the same trap. After all, the GDPR does contain broad exceptions related to law enforcement and national security.[71] The Chinese have also implicated law enforcement and national security concerns in order to justify their surveillance schemes.[72] It may be easy to say that the E.U. and China are so fundamentally different that the inadequacy of Chinese privacy law to protect it from the Chinese government itself is a uniquely Chinese phenomenon. To a certain extent, that is certainly true.[73] However, it would be a mistake to assume that the GDPR could not be similarly thwarted in the name of law enforcement and national security.[74]

---

[67] *Id.*

[68] *China invents the digital totalitarian state*, THE ECONOMIST (Dec. 17, 2016), https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state.

[69] Emma Graham-Harrison and Juliette Garside, *Revealed: Power and Reach of China's Surveillance Dragnet*, THE GUARDIAN (Nov. 24, 2019 6:03 PM), https://www.theguardian.com/world/2019/nov/24/china-cables-revealed-power-and-reach-of-chinas-surveillance-dragnet.

[70] *Id.*; Interview by Dave Davies with Kai Strittmatter, *Facial Recognition and Beyond: Journalist Ventures Inside China's 'Surveillance State'*, NPR (Jan. 5, 2021) (transcript at https://www.npr.org/transcripts/953515627); Josh Chin, *About to Break the Law? Chinese Police are Already on to You*, WALL STREET J. (Feb. 27, 2018), https://www.wsj.com/articles/china-said-to-deploy-big-data-for-predictive-policing-in-xinjiang-1519719096.

[71] GDPR, *supra* note 16 art. 23.

[72] Mitchell, *supra* note 66.

[73] *See, e.g.*, Amy Hawkins, *Chinese Citizens Want the Government to Rank Them*, FOREIGN POL'Y (May 24, 2017), https://foreignpolicy.com/2017/05/24/chinese-citizens-want-the-government-to-rank-them/ (observing that there is real support among the Chinese citizenry for a social credit system maintained by the Chinese government).

[74] Natalia Drozdiak, *EU Privacy Laws May Be Hampering Pursuit of Terrorists*, BLOOMBERG (July 8, 2019), https://www.bloomberg.com/news/articles/2019-07-

B. Government Access to Data in the EU and China

For all the GDPR may do to protect the data privacy of individuals, it is unlikely to curtail large scale government surveillance.[75] As discussed above, there are a number of reasons that the GDPR may be underenforced by member states. That is even before considering the competing interests of law enforcement. Though law enforcement and national security interests are unlikely to completely handicap the GDPR, it seems likely that it will prevent the GDPR from having the far-reaching impact that many privacy advocates hope for.

There is evidence that the European Union is willing to sacrifice privacy protections for individuals, in the name of law enforcement and national security. In 2017, the United States entered into an agreement, the E.U.-U.S. Privacy Shield, that allows for companies to freely transfer user data from the European Union to the United States.[76] Though the E.U.-U.S. Privacy Shield does not directly implicate national security or law enforcement—it allows providers to transfer data freely between the two jurisdictions—the E.U. entering the agreement can be seen as an endorsement of the surveillance schemes in the United States.[77] At the very least, it indicates that the E.U., or at least individual member states, may establish similar programs without running afoul of the GDPR.

As part of entering into the agreement with the United States, the European Union stated that the agreement was prudent because the United States had sufficient privacy protections in place.[78] The E.U. reached this conclusion despite the existence of multiple government surveillance programs that fall well short of E.U. privacy protection requirements.[79] As discussed above, the citizens of the United States do not have any general right to personal privacy. To the extent that there are Fourth Amendment protections, they do not extend outside of the jurisdiction of the United States and would offer no protection to non-U.S. citizen users in Europe.[80] The Privacy Shield allows for companies to freely transfer user data from the European Union to the United States. United States law "empowers the intelligence agencies to 'target' non-U.S. persons overseas for warrantless telephone or internet monitoring."[81] This means that the United States

---

08/european-privacy-laws-may-be-hampering-those-catching-terrorists.

[75] *The EU General Data Protection Regulation*, *supra* note 44.

[76] Maria McFarland Sanchez-Moreno of Human Rights Watch and Iverna McGowan of Amnesty International, *Joint Letter to European Commission on EU-US Privacy Shield*, HUMAN RIGHTS WATCH (July 26, 2017), https://www.hrw.org/news/2017/07/26/joint-letter-european-commission-eu-us-privacy-shield#.

[77] *Id.*

[78] *US Surveillance Makes Privacy Shield Invalid*, HUMAN RIGHTS WATCH (July 26, 2017), https://www.hrw.org/news/2017/07/26/us-surveillance-makes-privacy-shield-invalid.

[79] *Id.*

[80] *Joint Letter*, HUMAN RIGHTS WATCH, *supra* note 76, at 5 n.16.

[81] *Id.* at 7.

government can request, without a court order, the user data that private companies collect on users within the European Union.[82]

It is possible, if not likely, that the European Union entered into the Privacy Shield agreement because it could not afford to sever ties with the United States—not because it actually believed the United States had sufficient privacy protections in place. The European Union has clearly been dissatisfied with the privacy protections offered for E.U. citizens by the United States, to the point where the European Union threatened to pull out of the agreement.[83] Two years later, despite uneven progress at best, the Privacy Shield remains in place, calling into question how serious the EU is about U.S. compliance.[84]

Another reason that the European Union may not be willing to seriously object is that, in spite of all of its efforts to protect the privacy of its citizens from abuse by providers, it does not have similar reservations about government use of the same data. While the European Union was enacting the GDPR and E.U. Courts were deciding cases like *Google v. Spain*,[85] member states of the E.U. were also building their own mass surveillance programs which were, in turn, legitimized by E.U. courts.[86] Also, the European Union is currently attempting to answer the same jurisdictional question that Part 2 of the CLOUD Act was intended to solve. The European Union's proposal regulating e-evidence[87] grants jurisdiction over a person's data when a requesting government otherwise has jurisdiction over that person, regardless of where the data is stored. Despite the GDPR having just gone into effect, the e-evidence regulation as it stands is almost completely devoid of any meaningful protections for personal privacy.[88] Private companies have spoken out against the e-evidence regulation for not protecting fundamental privacy rights.[89] Some

---

[82] *Id.*

[83] Hayley Evans & Shannon Togawa Mercer, *Privacy Shield on Shaky Ground: What's Up With EU-U.S. Data Privacy Regulations*, LAWFARE (Sept. 2, 2018, 2:31 PM), https://www.lawfareblog.com/privacy-shield-shaky-ground-whats-eu-us-data-privacy-regulations.

[84] Nicole Lindsey, *Second Review of EU-US Privacy Shield Shows Improvements*, CPO MAG. (Jan. 15, 2019), https://www.cpomagazine.com/data-protection/second-review-of-eu-us-privacy-shield-shows-improvements/.

[85] Case C-131/12, *Google Spain SL v. Agencia Espanola de Proteccion de Datos*, 2014 E.C.R. 317 (2014).

[86] Asaf Lubin, *Legitimizing Foreign Mass Surveillance in the European Court of Human Rights*, JUST SEC. (Aug. 2, 2018), https://www.justsecurity.org/59923/legitimizing-foreign-mass-surveillance-european-court-human-rights/.

[87] *Regulation on Cross Border Access to E-Evidence: Council Agrees its Position*, EUROPEAN COUNCIL (Dec. 7, 2018), https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/.

[88] *"E-evidence": Repairing the Unrepairable*, EUROPEAN DIG. RIGHTS (Nov. 14, 2019), https://edri.org/e-evidence-repairing-the-unrepairable/.

[89] John Frank, *E-Evidence: Robust Fundamental Rights Protections Are Needed for*

privacy advocates have even expressed concern that the e-evidence regulation could lead to de-facto "privatization of law enforcement."[90] There is some evidence that we are seeing the beginning of this kind of privatization of law enforcement with regard to national security. The European Union has suggested, similar to China, that the tech industry has an obligation to develop tools that can automatically detect and remove content that may incite terrorism.[91] Further, the European Union has said "subject to appropriate safeguards, the availability of data should be secured" to preserve government access to electronic evidence.[92]

None of this is to say that the regulations and law enforcement data collection schemes in the European Union are exceedingly draconian. In China, any tech provider that collects personal data must also store the data in China.[93] Though the Chinese government insists that this is in order to protect the privacy of the Chinese people, it is generally understood to "give the government unrestricted access to almost all personal data."[94] Chinese tech companies—from online retailers and search engines to social media and messaging providers—routinely turn over data to the Chinese government.[95] The Chinese government also has the ability to target and suspend social media accounts that contain key terms.[96] The state has also asked companies to develop software that can use data collected to predict terrorist attacks.[97]

Again, these programs are far more draconian than anything in place in the European Union or United States. But, as tempting as it may be, it would be a mistake to believe that such programs could not exist in the West because we have a fundamentally different understanding of individual rights than China. As true as that may be, it has not always been enough to keep Western governments from engaging in surveillance and data collection programs that would be impossible if those governments, or at least the people who ran the programs, placed any real importance in the

---

European Law Enforcement Authorities' Access to Data, MICROSOFT (Nov. 6, 2019), https://blogs.microsoft.com/eupolicy/2019/11/06/e-evidence-fundamental-rights-protections-needed/.

[90] Katitza Rodriguez, *A Tale of Two Poorly Designed Cross-Border Data Access Regimes*, ELEC. FRONTIER FOUND. (Apr. 25, 2018), https://www.eff.org/deeplinks/2018/04/tale-two-poorly-designed-cross-border-data-access-regimes.

[91] *European Council Conclusions on Security and Defence, 22/06/2017*, EUROPEAN COUNCIL (June 22, 2017), https://www.consilium.europa.eu/en/press/press-releases/2017/06/22/euco-security-defence/.

[92] *Id.*

[93] Sara Xia, *China Data Protection Regulations (CDPR)*, CHINA LAW BLOG (May 20, 2018), https://www.chinalawblog.com/2018/05/china-data-protection-regulations-cdpr.html.

[94] *China Invents the Digital Totalitarian State*, *supra* note 68.

[95] *Id.*

[96] *Id.*

[97] *Id.*

privacy rights of individuals.[98] The only absolute barrier that exists is that in the European Union and the United States, governments do not have the same degree of control over the tech providers in their jurisdictions as the Chinese government does over Chinese companies. In China, technology companies are, in many ways, de facto arms of the state and cannot refuse to cooperate with the Chinese government.[99] As such state control does not exist in the West, providers can oppose new regulation that may be harmful to their consumers, and by extension, the companies themselves.[100] However, this requires the tech companies to be willing to stand up to the government rather than conduct the surveillance on the government's behalf. To the extent that what separates the West from China is that companies in China "have no meaningful ability to tell the Chinese Communist Party 'no,'"[101] it requires that the companies in the West who can say no do so when necessary.

IV. PRIVATE PROVIDERS AND GOVERNMENT SURVEILLANCE

Thus far, we have seen what government has required, or can require, of providers in order to ensure individuals some measure of privacy with regards to their personal data. We have also seen how law enforcement and national security interests can be antagonistic to attempts by government to protect the privacy of its people. At this point, it is important to examine the role that the providers themselves have in the struggle between privacy and law enforcement interests.

Tech providers play an active role in shaping public policy in a wide

---

[98] *See, e.g.*, *COINTELPRO FBI Records: The Vault*, FED. BUREAU INVESTIGATION (last visited Mar. 15, 2020), https://vault.fbi.gov/cointel-pro (In the mid-twentieth century, the FBI engaged in surveillance of social and political activist organizations such as the Communist Party, the Black Panther Party, and individual leaders such as Martin Luther King Jr. The FBI concedes that the surveillance was improper for "abridging first amendment rights and for other reasons.").

[99] *See, e.g.*, Alex Johnson, *'An Arm of the Chinese State': What's Behind the Huawei Indictments*, NBC NEWS (Jan. 29, 2019), https://www.nbcnews.com/tech/security/arm-chinese-state-what-s-behind-huawei-indictments-n963776 (observing that, according to U.S. government officials the Chinese government subsidizes Huawei and that using Huawei's products made users vulnerable to Chinese surveillance); Jane Li, *A US Official Says Tech Giants Alibaba and Tencent Present Similar Risks as Huawei*, QUARTZ (Sept. 13, 2019), https://qz.com/1708662/chinese-tech-giants-tools-of-the-communist-party-us-official/
(reporting that a U.S. State Department official suggested that other large tech companies are either de facto or de jure arms of the state in part because they cannot refuse requests from the Chinese government).

[100] An easy example of this is the *Microsoft* case that triggered the passage of the CLOUD Act. Microsoft itself, not the individual in question, challenged the subpoena for the emails related to a certain account. United States v. Microsoft Corp., 138 S.Ct. (2018). Of course, Microsoft also supported the CLOUD Act, suggesting that, at least in part, it objected to the subpoena because it felt obligated to rather than out of a sense of duty to protect a user's personal data. *See* Letter from Apple, Google, Microsoft, *supra* note 26.

[101] Li, *supra* note 99.

range of areas, including privacy and law enforcement.[102] In 2017, Google spent more money on lobbying than any other company in the United States.[103] In the European Union, Google engaged in a "hiring blitz" of former government officials with the aim to "boost its influence in European policy circles."[104] Other tech providers have followed Google's lead.[105] The role of tech providers in this sphere is not limited to trying to shape policy through traditional lobbying—they are also indispensable to modern law enforcement and national security efforts.[106]

In mid-2013, Edward Snowden, an employee of the National Security Agency (NSA), leaked highly classified information which revealed extensive global surveillance programs, many of which were run by the NSA.[107] Snowden collected about 1.7 million intelligence files[108] documenting the surveillance practices of the United States and the rest of the Five Eyes alliance. In particular, the Snowden disclosures detailed the PRISM surveillance program, a program under which the NSA collected electronic communications through various U.S. internet companies; in some cases, with the help of the providers themselves.[109] The surveillance

---

[102] *See* Tony Romm, *Tech Giants Led by Amazon, Facebook, and Google Spent Nearly Half a Billion on Lobbying Over the Past Decade, New Data Shows*, WASH. POST (Jan. 22, 2020 8:32 AM) ("Google lobbyists focused heavily on privacy.") (quotation omitted); Deborah D'Souza, *Tech Lobby: Internet Giants Spend Record Amounts, Electronics Firms Trim Budgets*, INVESTOPEDIA (June 25, 2019), https://www.investopedia.com/tech/what-are-tech-giants-lobbying-trump-era/ ("Tech companies have continued fighting the government on surveillance issues, especially government requests for data.").

[103] Hamza Shaban, *Google for the First Time Outspent Every Other Company to Influence Washington in 2017*, WASH. POST (Jan. 23, 2018 6:35 PM), https://www.washingtonpost.com/news/the-switch/wp/2018/01/23/google-outspent-every-other-company-on-federal-lobbying-in-2017/.

[104] *Google's European Revolving Door*, TECH TRANSPARENCY PROJECT (June 4, 2016), https://www.techtransparencyproject.org/articles/googles-european-revolving-door.

[105] *See* Tony Romm, *Amazon, Facebook, Other Tech Giants Spent Roughly $65 Million to Lobby Washington Last Year*, WASH. POST (Jan. 22, 2021 10:15 AM), https://www.washingtonpost.com/technology/2021/01/22/amazon-facebook-google-lobbying-2020/ (outlining lobbying efforts by tech firms in the U.S.); Adam Satariano & Matina Stevis-Gridneff, *Big Tech Turns its Lobbyists Loose on Europe, Alarming Regulators*, N.Y. TIMES (Dec. 14, 2020), https://www.nytimes.com/2020/12/14/technology/big-tech-lobbying-europe.html (observing the same in the European Union).

[106] *See Chapter One: Cooperation or Resistance?: The Role of Tech Companies In Government Surveillance*, 131 HARV. L. REV. 1722, 1722 (2018).

[107] See Margaret Hu, *Taxonomy of the Edward Snowden Disclosures*, 72 WASH. & LEE L. REV. 1679, for a comprehensive compilation and classification of the Snowden disclosures.

[108] Chris Strohm & Del Quentin Wilber, *Pentagon Says Snowden Took Most U.S. Secrets Ever: Rogers*, BLOOMBERG (Jan. 9, 2014), https://www.bloomberg.com/news/articles/2014-01-09/pentagon-finds-snowden-took-1-7-million-files-rogers-says.

[109] An NSA PowerPoint presentation released as part of the Snowden disclosures claimed that PRISM—which collected data directly from the servers of providers—was run with the assistance of the providers. Providers generally denied collaborating with the NSA, or even being aware of PRISM, but subsequent disclosures showed that some of the largest providers were willing participants in the program. Glenn Greenwald & Ewen MacAskill,

programs revealed in the Snowden disclosures were merely part of an overall trend of law enforcement's reliance on third party providers.

Early examples of government relying on private companies to assist with surveillance can be seen with the enactment of so-called "lawful interception" laws in the 1990s. As telecommunications networks became increasingly digital, law enforcement wiretaps required the cooperation of providers as they could no longer simply plug into a phone line—literally tap the wire—and listen in on phone calls.[110] In the mid-1990s, governments all over the world—including the United States, United Kingdom and European Union—enacted legislation that imposed an obligation on providers to provide law enforcement access to their network and support government interception of data.[111] These regulations were eventually expanded or supplemented to require providers to store metadata and turn it over to law enforcement.[112] Though law enforcement had long relied on the cooperation of third party providers, this was the first time an affirmative burden was placed on private companies to provide access to law enforcement.[113]

As technology has progressed and more personal data is stored electronically, the U.S. government has moved quickly to ensure they did not have any interruptions in access.[114] Though, the government has not simply needed to keep pace with technological advancements. The supply of personal data available to the government also needed to keep pace with an increase in demand. In the wake of the September 11, 2001 attacks, the U.S. government greatly expanded the power of the federal government in the name of combatting terrorism.[115] It is this "militarized demand" for user data that has enabled providers to act without fear of sanction from of law enforcement because the interests of tech providers and law enforcement—increased supply—are often aligned.[116]

NSA Prism Program Taps in to User Data of Apple, Google and Others, GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data.

[110] Jeffrey Yeates, *CALEA and the RIPA: The U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World*, 12 ALB. L.J. SCI. & TECH. 125, 126, 130 (2001).

[111] Communications Assistance for Law Enforcement Act, 74 U.S.C. 1001(8)(A) (2018); Regulation of Investigatory Powers Act, 2000, c.23 (Eng.); Council Resolution of 17 January 1995, 1996 J.O. (C 329) (Resolution on the Lawful Interception of Telecommunications) (EU).

[112] *See, e.g.*, 18 U.S.C. § 2703 (2018); *Investigatory Powers Act of 2016*, 2016 c.25 (Eng.); Council Directive 2006/24/EC, 2006 O.J. (L 105) 54 (EU).

[113] Yeates, *supra* note 110 at 127.

[114] *See, e.g.*, 47 C.F.R. § 64 (2020).

[115] For a thorough examination of the expansion of government power in the years after the September 11 attacks, see Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB. POL'Y 319 (2005).

[116] ZUBOFF, *supra* note 55 at 121.

In some respects, the U.S. government is actually incentivized to rely on private companies to conduct intelligence gathering for law enforcement.[117] There is the obvious benefit to the government that, by soliciting data from various third parties, the government can collect more information than it could if it were doing the collection on its own. However, there are legal benefits as well. Professor Jon Michaels observed that by entering into informal agreements with private parties, law enforcement could avoid congressional or judicial oversight.[118] Private parties, which did not have to operate within the statutory and regulatory framework required of law enforcement, gave law enforcement greater access to user information with fewer legal hurdles to clear along the way.[119]

The Five Eyes publicly touted its collaboration with providers such as Google, Facebook, Microsoft, and Twitter to address online terrorism.[120] The European Union also announced that it expects the tech industry to develop technology and tools to help detect and remove online content that could incite terrorism.[121] Practically, governments must cooperate with private actors in order to police the internet if for no other reason than the sheer impossibility of the task.

It has generally been accepted that the loss of privacy is simply payment in exchange for the use of many modern services. Facebook, Google, and numerous other tech providers rely on a privacy-for-service business model; they do not charge their users for their service, but instead monetize user data.[122] However, there is evidence that this bargain is becoming strained. An overwhelming majority of people in the United States believe that there should be stronger privacy protections, including a "right to be forgotten," and Americans are divided on whether it is acceptable for law enforcement specifically to use or collect their personal data.[123] As a result, not only must tech providers now comply with

---

[117] Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901, 904 (2008).

[118] *Id.*

[119] *Id.*; *see also* ZUBOFF, *supra* note 55 at 303 (explaining that Facebook does not have to adhere to the same standards required of government researchers).

[120] Five Country Ministerial, *2017 Joint Communique*, PUBLIC SAFETY CANADA (June 26, 2017), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fv-cntry-mnstrl-2017/fv-cntry-mnstrl-2017-en.pdf.

[121] Press Release, European Council, European Council Conclusions on Security and Defence (June 22, 2017), https://www.consilium.europa.eu/en/press/press-releases/2017/06/22/euco-security-defence/.

[122] Shara Tibken, *Questions to Mark Zuckerberg Show Many Senators Don't Get Facebook*, C-NET (Apr. 11, 2018), https://www.cnet.com/news/some-senators-in-congress-capitol-hill-just-dont-get-facebook-and-mark-zuckerberg/.

[123] Brooke Auxier & Lee Rainie, *Key Takeaways on Americans' Views About Privacy, Surveillance and Data-Sharing*, PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-

increased privacy legislation around the world, but they must also reassure consumers that they can use tech services and products and maintain some level of privacy. Thus, providers are fighting a battle over control of users' personal data on two separate fronts.

One solution for tech providers is to repackage this data and sell it to the government. Given that the public appears to be less skeptical of the government collecting and processing their personal data, it seems that, even if it does not improve the public's opinion of tech providers, it may not have a negative impact.[124] On the other front, there is little reason to believe that governments will object with any real force to this strategy. In the United States, law enforcement has used tools developed by tech providers that scan social media for potential threats.[125] Beyond simply using tools that private tech companies have developed, the United States has taken an active role in funding these efforts, including providing funding to startups that create "threat scores" based on social media activity.[126] This phenomenon is, of course, not restricted to small startups operating in this niche space. Tech companies based in the United States have helped the Chinese build their surveillance infrastructure.[127] Facebook CEO Mark Zuckerberg even suggested that artificial intelligence could monitor private messages and flag suspicious activity, such as potential planning of terrorist attacks.[128]

The collection of personal data is not limited to privacy-for-service providers. Internet service providers—ostensibly fee-for-service providers—armed with an expansive view of the entire web, have positioned themselves to compete with entities such as Google and Facebook for surveillance revenues.[129] In 2016, the Federal Communications Commission (FCC) enacted rules that gave individuals control over how ISPs used their personal data.[130] However, these privacy protections were short lived. In 2017, Congress passed legislation that rolled back the FCC rules and prevented it from creating similar rules in the

about-privacy-surveillance-and-data-sharing/.

[124] *See id.*

[125] Jonah Engel Bromwich, Mike Isaac & Daniel Victor, *Police Use Surveillance Tool to Scan Social Media, A.C.L.U. Says*, N.Y. TIMES (Oct. 11, 2016), https://www.nytimes.com/2016/10/12/technology/aclu-facebook-twitter-instagram-geofeedia.html.

[126] Lee Fang, *The CIA is Investing in Firms That Mine Your Tweets and Instagram Photos*, THE INTERCEPT (Apr. 14, 2016), https://theintercept.com/2016/04/14/in-undisclosed-cia-investments-social-media-mining-looms-large/.

[127] Ryan Gallagher, *How U.S. Tech Giants are Helping to Build China's Surveillance State*, THE INTERCEPT (July 11, 2019), https://theintercept.com/2019/07/11/china-surveillance-google-ibm-semptian/.

[128] Karissa Bell, *Zuckerberg Removed a Line About Monitoring Private Messages from His Facebook Manifesto*, MASHABLE (Feb. 16, 2017), https://mashable.com/2017/02/16/mark-zuckerberg-manifesto-ai/.

[129] ZUBOFF, *supra* note 55 at 166.

[130] 47 C.F.R. §64 (2020).

future.[131] The result is that users are now paying ISPs for the privilege of having the whole of their internet activity available for sale, and, if history is any guide, law enforcement will be among those lining up to purchase it.[132]

Providers also work directly with law enforcement, rather than simply selling or repurposing data it collects for other purposes. One of the more well-known efforts is the deployment of facial recognition.[133] Deployment of facial recognition in the United States has been uneven. Some jurisdictions and even private companies have restricted its use by law enforcement over ethical concerns.[134] Other jurisdictions have used facial recognition software that scrapes billions of images from the internet and compares them to footage captured by security cameras to identify possible matches.[135] There are also ambitions plans to expand the use of facial recognition at the federal level where it is currently used by the Customs and Border Patrol.[136] Law enforcement is not merely using the technology to identify suspects of crimes; they are also using it to identify protestors, journalists, and track immigrants.[137] A similar technology, automatic license plate readers, allows law enforcement to track people in real time.[138]

---

[131] 115 Pub L. No. 22, § 131 Stat. 88.

[132] *See* Nathaniel Turner, *Congress: Don't Let Internet Providers Sell Our Data to the Highest Bidder*, ACLU (Mar. 7, 2017) https://www.aclu.org/blog/privacy-technology/internet-privacy/congress-dont-let-internet-providers-sell-our-data-highest (observing that the 2017 legislation enables ISPs to sell personal data to law enforcement); Nicky Wolf, *Documents Show AT&T Secretly Sells Customer Data to Law Enforcement*, THE GUARDIAN (Oct. 25, 2016 3:33 PM) https://www.theguardian.com/business/2016/oct/25/att-secretly-sells-customer-data-law-enforcement-hemisphere (describing how an ISP, AT&T, sold customer data to local and federal law enforcement in secret). It is also possible that ISPs will simply turn over personal data to the government for free as they have in the past. *See Cooperation or Resistance supra* note 106 at 1725-26 (outlining how AT&T went "above and beyond to facilitate government surveillance" for several years following 9/11); Greenwald & MacAskill *supra* note 109 (observing that tech providers willingly turned over personal data to the NSA).

[133] *See* Aaron Smith, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, PEW RESEARCH (Sept. 5, 2019), https://www.pewresearch.org/internet/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/ (observing that most Americans are aware of facial recognition technology); Sam duPont, *On Facial Recognition, the U.S. Isn't China—Yet*, LAWFARE (June 18, 2020, 8:01 AM), https://www.lawfareblog.com/facial-recognition-us-isnt-china-yet (discussing facial recognition efforts in the United States).

[134] duPont, *supra* note 133.

[135] duPont*, supra* note 133.

[136] Jay Stanley, *The Government's Nightmare Vision for Face Recognition at Airports and Beyond*, ACLU (Feb. 6, 2020), https://www.aclu.org/news/privacy-technology/the-governments-nightmare-vision-for-face-recognition-at-airports-and-beyond/.

[137] *Id.;* duPont, *supra* note 133.

[138] *See* Tanvi Misra, *Who's Tracking Your License Plate?*, BLOOMBERG (Dec. 6, 2018 9:31 AM), https://www.bloomberg.com/news/articles/2018-12-06/why-privacy-advocates-fear-license-plate-readers (noting that ALRs are akin to facial recognition for cars and enable

Further, because the data is often stored for years at a time—by both law enforcement and private contractors who monetize the data—it can be used to look backwards and see where people were after the fact, not unlike the use of cell site location data that the Supreme Court has determined requires a warrant due to the privacy interests at stake.[139]

Among the most sophisticated tools law enforcement uses are the ones that enable it to process the data it collects. One such platform, Palantir, was developed for counterinsurgency efforts in warzones and has been adapted for use by civilian law enforcement at the federal and local levels.[140] Palantir allows law enforcement to filter through millions of records in a matter of minutes using only basic information.[141] The data filtered by Palantir comes from various law enforcement databases, as well as external databases that include billions of records including things like utility bills, credit card information, retail customer lists, and social media data.[142] All of this is just scratching the surface. Law enforcement is currently collecting far more data than it has a use for, and the largest police departments are using the most sophisticated tools.[143] With time, new tools will inevitably be developed that make use of the surplus data, and will eventually filter into more law enforcement agencies.

As long as governments are willing to participate in the monetization of user data by either paying for the data itself, or funding tools developed specifically for law enforcement, there is little reason for providers to change their practices. This is because, from the perspective of the providers, privacy is not a right, but a commodity.[144] Though this may be a disquieting reality, it may also be a reason to be somewhat optimistic. To the extent that the "right" to privacy is for sale, providers can lose out on business where they cannot guarantee user privacy. American tech

---

real time tracking).

[139] *See* SARAH BRAYNE, PROTECT AND SURVEIL: DATA, DISCRETION AND THE FUTURE OF POLICING 51 (Oxford University Press 2021) ("[T]he most common use of ALPRs is simply to store data for potential use during a future investigation."); *Automatic License Plate Readers (ALPRs),* EFF (Aug. 28, 2017), https://www.eff.org/pages/automated-license-plate-readers-alpr (observing that the data is stored for years and offered for sale by private contractors); Carpenter v. United States, 138 S.Ct. 2206, 2212-13 (2018) (the police used cell site location information to determine that Carpenter was at each location in a string of robberies).

[140] BRAYNE, *supra* note 139 at 7.

[141] *Id.* at 37-39.

[142] *Id.* at 41, 53-54.

[143] *Id.* at 7, 89.

[144] Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2055, 2056 (2004). While the commodification of privacy has been a boon for the tech industry, it has been criticized as an inadequate framework for protecting the privacy interests of individuals. Proposed privacy reforms argue for recognizing privacy as a right, rather than as a commodity. *See* Frank Pasquale, *Privacy, Antitrust, and Power*, 20 GEO. MASON. L. REV. 1009 (2013). As proposals to de-commodify privacy are just that, proposals, I attempt to find a way forward in the current "privacy as a commodity" landscape.

companies alone lost billions of dollars in the immediate aftermath of the NSA leaks with billions more in losses projected over the following decade.[145] Tech companies outside of the United States have successfully advertised that they do not have an American presence, taking business from their American competitors. Electronic communications providers have lost business as a result of United States surveillance and data collection practices.[146] Mark Zuckerberg himself was highly critical of the Obama Administration's reaction to the Snowden leaks because of the impact it had on Facebook's business.[147] Even non-tech companies have suffered as a direct result of the Snowden leaks.[148]

There is evidence that tech companies, even those with spotty track records when it comes to user privacy, recognize that they must take at least some steps to protect their users' privacy beyond the protections required by law. Mark Zuckerberg, at least publicly, abandoned his plans to mine private messages for potential terror plots.[149] Facebook, as owner of the popular WhatsApp communications app, has also recently filed a lawsuit against an Israeli company for breaking through its encryption safeguards.[150] Amazon and Microsoft suspended the use of their facial recognition software by law enforcement over ethical concerns and IBM stopped offering facial recognition software altogether.[151] The largest tech companies in the United States are constantly trying to expand their presence in even the most basic and necessary aspects of day-to-day life. Facebook has been developing its own currency in the face of criticism from both private and public sectors.[152] Given the typical users of cryptocurrency, its success very much depend on having strong protections in place for its users, especially to the extent that it requires standing up to the government.[153] Google had to table a joint project with the government

---

[145] Claire Cain Miller, *Revelations of N.S.A Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

[146] Mark Scott, *Irked by N.S.A., Germany Cancels Deal with Verizon*, N.Y. TIMES (June 25, 2014), https://www.nytimes.com/2014/06/27/business/angered-by-nsa-activities-germany-cancels-verizon-contract.html.

[147] GLENN GREENWALD, NO PLACE TO HIDE 126 (Picador 2014).

[148] Alonso Soto and Brian Winter, *Saab Wins Brazil Jet Deal After NSA Spying Sours Boeing Bid*, REUTERS (Dec. 18, 2013), https://in.reuters.com/article/uk-brazil-jets/saab-wins-brazil-jet-deal-after-nsa-spying-sours-boeing-bid-idUKBRE9BI01L20131219.

[149] Bell, *supra* note 128.

[150] Jeff Horwitz & Robert McMillan, *Facebook Sues Israel's NSO Group Over Alleged WhatsApp Attack*, WALL STREET J. (Oct. 29, 2019), https://www.wsj.com/articles/facebook-sues-israels-nso-group-over-alleged-whatsapp-attack-11572379534.

[151] duPont, *supra* note 133.

[152] Cecilia Kang & Nathaniel Popper, *Facebook Lays on the Charm for Its Libra Cryptocurrency Plan*, N.Y. TIMES (Oct. 21, 2019), https://www.nytimes.com/2019/10/21/technology/facebook-libra-marcus-lobbying.html.

[153] *See* Craig Calcaterra, Wulf A. Kaal, Vadhindran Rao, *The Rise of Fintech: Stable Cryptocurrencies*, 61 WASH. U.J.L. & POL'Y 193, 215 n.126 (2020) (observing that

to store medical records—specifically x-ray scans—over privacy concerns.[154] Though the program was compliant with federal privacy laws, it called into question the extent to which the tech giant can protect user data privacy.[155]

Even so, the public remains wary that tech providers can adequately protect their personal information. As a result, efforts by tech providers to influence potential government privacy initiatives, such as legislation, are likely to be met with skepticism. But, where their interests align, the general public and tech providers would do well to work together to ensure the effectiveness of any new privacy legislation. Though public pressure can force Congress to act, pressure alone is likely insufficient to ensure that the resulting legislation is effective, or achieves the public's desired ends.

For example, in the 1970s public outrage precipitated FISA, the act at the heart of so many privacy issues that we face today.[156] Congress enacted the USA FREEDOM Act in response to public pressure following the Snowden disclosures.[157] Clearly, public pressure can force Congress to act. However, mere action is not enough. The actions Congress takes must actually move the ball forward when it comes to protecting, or in some cases even creating the privacy rights of individuals. Any comprehensive privacy legislation, like the GDPR or CCPA, will be extremely complex. As a result, it is likely that many important details of such legislation will be lost on the general public.[158]

Tech providers, on the other hand, will have the required sophistication to understand the impact of new legislation. For better or worse, they also have experience lobbying the government to get what they want. If tech providers can be convinced that what helps the general public—their customer base—helps them as well, the chances that new

---

"[p]rivacy and freedom from government are sometimes presented as two of the big advantages of a cryptocurrency").

[154] Douglas MacMillan & Greg Bensinger, *Google Almost Made 100,000 Chest X-Rays Public—Until It Realized Personal Data Could be Exposed*, WASH. POST (Nov. 15, 2019), https://www.washingtonpost.com/technology/2019/11/15/google-almost-made-chest-x-rays-public-until-it-realized-personal-data-could-be-exposed/.

[155] *Id.*

[156] Thomas Young, *40 Years Ago, Church Committee Investigated Americans Spying on Americans*, BROOKINGS (May 6, 2015), https://www.brookings.edu/blog/brookings-now/2015/05/06/40-years-ago-church-committee-investigated-americans-spying-on-americans/.

[157] David Kris, *The NSA and the USA Freedom Act*, LAWFARE (July 2, 2018), https://www.lawfareblog.com/nsa-and-usa-freedom-act.

[158] *See* Ilya Somin, *Political Ignorance and the Countermajoritarian Difficulty: A New Perspective on the Central Obsession of Constitutional Theory*, 89 IOWA L. REV. 1287, 1334 (2004) (Professor Somin argues that "political ignorance" results in only the few statutes that are both "highly prominent and relatively simple to understand" will reflect the will of the people. While comprehensive privacy reform would probably qualify as "highly prominent" it will assuredly be, like the GDPR and CCPA, extremely complex and difficult to understand in many respects.)

privacy legislation will be effective rise exponentially.

Ultimately, tech companies seek to maximize profits and shareholder value. If the public can make it worthwhile for these companies to protect their data, there is reason to be optimistic that they will do so. In some cases, tech companies have even taken the first step by standing up to law enforcement while making their case to the public. Apple has resisted assisting the FBI with breaking through the encryption on iPhones as part of terrorism investigations, with Apple CEO Tim Cook making an impassioned public statement in defense of Apple's stance.[159] Conversely, former Attorney General Bill Barr insisted that tech companies are catering to criminals by offering shelter from government surveillance.[160] In making his own case to the public, former A.G. Barr asked "Do we want to live in a society like that?"[161] Barr, of course, does not think we do. It remains to be seen whether the people agree.

V. CONCLUSION

Data privacy will become a larger issue in the United States. What remains to be seen is how effective attempts to create legal privacy protections will be. At the state level, the most comprehensive effort in the United States to extend legal protections for individual data privacy, the California Consumer Privacy Act ("CCPA"), borrowed heavily from the GDPR.[162] As a result, it shares many of its vulnerabilities.[163] At the federal level, however, there is little reason to expect Congress to take up the issue in the foreseeable future.[164] Any progress made in the courts is likely to be

---

[159] Jack Nicas and Katie Benner, *F.B.I. Asks Apple to Help Unlock Two iPhones*, N.Y. TIMES (Jan. 7, 2020), https://www.nytimes.com/2020/01/07/technology/apple-fbi-iphone-encryption.html.

[160] *Id.* ("Companies like Facebook are selling the idea that 'no matter what you do, you're completely impervious to government surveillance.")

[161] *Id.*

[162] *See, e.g.*, Diane Y. Byun, *Privacy or Protection: The Catch-22 of the CCPA*, 32 LOY. CONSUMER L. REV. 246, 247 (2020) (characterizing the CCPA as the "strictest data privacy law in the United States"); Carol A. F. Umhoefer & Tracy Shapiro, *CCPA v. GDPR: The Same, Only Different*, DLA PIPER (Apr. 11, 2019), https://www.dlapiper.com/en/us/insights/publications/2019/04/ipt-news-q1-2019/ccpa-vs-gdpr/ (noting that, though there are differences between the GDPR and the California Consumer Privacy Act, they share key components); Jeewon Kim Serrato and Daniel Rosenzweig, *GDPR, CCPA and Beyond: Changes in Data Privacy Laws and Enforcement Risks to Monitor in 2019*, DATA PROTECTION REPORT (Feb. 27, 2019), https://www.dataprotectionreport.com/2019/02/gdpr-ccpa-and-beyond-changes-in-data-privacy-laws-and-enforcement-risks-to-monitor-in-2019/ (referring to new privacy legislation in the US as "GDPR copycat laws").

[163] Greg Bensinger, *So far, Under California's New Privacy Law, Firms are Disclosing Too Little Data—Or Far Too Much*, WASH. POST (Jan. 21, 2020), https://www.washingtonpost.com/technology/2020/01/21/ccpa-transparency/.

[164] David McCabe, *Congress and Trump Agreed They Want a National Privacy Law. It is Nowhere in Sight*, N.Y. TIMES (Oct. 1, 2019), https://www.nytimes.com/2019/10/01/technology/national-privacy-law.html.

slow and uneven.[165] Should the Supreme Court address the issue, lower courts and advocates on both sides will still have to figure out how to interpret any new law, even if the Court expands privacy protections.[166] All the while, technology will continue to advance.

Regardless of where data privacy protections come from, in the foreseeable future it is almost certain that they will not come from the executive branch. Much of the modern data collection apparatus was created by the George W. Bush administration,[167] expanded under the Obama administration,[168] then maintained under the Trump administration.[169] It seems unlikely that President Biden will depart from policies embraced by the Obama Administration. While it can be hard to predict technological advancements over the next five years, we can be certain that the executive's goal will be to ensure that law enforcement is able to keep pace and maintain its broad surveillance and data collection programs.

Americans will have to confront that it is likely impossible to have meaningful personal data privacy protections while maintaining current law enforcement and national security surveillance programs. This is not a new struggle. In recent years, advocates for stronger individual liberties have co-opted Benjamin Franklin's assertion that "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty or Safety."[170] Such an absolutist position is untenable, and, it turns out, not what Benjamin Franklin was endorsing at the time.[171] Rather,

---

[165] *See* Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1607, 1667-70 (1999) (arguing that common law litigation is ill-suited for developing data privacy law).

[166] *See* Louise Matsakis, *SCOTUS and Congress Leave the Right to Privacy Up for Grabs*, WIRED (July 3, 2018), https://www.wired.com/story/scotus-congress-leave-right-to-privacy-up-for-grabs/.

[167] James Risen and 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.

[168] Kate Tummarello, *Obama Expands Surveillance Powers on His Way Out*, ELECTRONIC FRONTIER FOUNDATION (Jan. 12, 2017), https://www.eff.org/deeplinks/2017/01/obama-expands-surveillance-powers-his-way-out.

[169] Frank R. Konkel, *Sessions: Surveillance Reform Could be 'Exceedingly Damaging' to National Security*, NEXTGOV (Nov. 14, 2017), https://www.nextgov.com/policy/2017/11/sessions-surveillance-reform-could-be-exceedingly-damaging-national-security/142535/ (former AG Jeff Sessions describing an update to FISA requiring law enforcement to obtain a probable cause warrant as potentially "exceedingly damaging" to national security).

[170] *See, e.g.*, John Ashcroft & Viet Dinh, *Liberty Security, and the USA PATRIOT Act*, NATIONAL REVIEW (Sept. 9, 2011), https://www.nationalreview.com/2011/09/liberty-security-and-usa-patriot-act-john-ashcroft-viet-dinh/; Simon Black, *Don't Forget What Ben Franklin Said About Domestic Terrorism*, BUSINESS INSIDER (Apr. 13, 2013), https://www.businessinsider.com/important-lessons-in-domestic-terrorism-2013-4.

[171] The context of the quote has been generally ignored, leading people to misunderstand what Benjamin Franklin meant. Benjamin Wittes, *What Ben Franklin Really Said*, LAWFARE

Franklin understood that the real struggle was to find a correct balance between liberty and safety.[172] Finding the right balance requires honesty about what the problem is and what effect privacy laws will have.

It is easy to dismiss the totalitarian surveillance state in China as a uniquely Chinese problem that could not happen in the United States or Europe. An obvious difference is that the Chinese Communist Party is the paramount authority in China and has absolute authority over many Chinese institutions, including law enforcement.[173] Further, the CCP uses its vast surveillance capabilities to commit human rights atrocities that are incomparable to anything in the United States or European Union. Via tens of millions of cameras, China uses facial recognition and "gait recognition" to monitor and identify political dissidents and minority groups—particularly Tibetans and Uighurs.[174] This has enabled China to ultimately detain over one million Uighurs and other Muslims in internment camps designed to erase religious and ethnic identities.[175] For its part, China argues that the indoctrination of the Uighurs—officially declared genocide by the United States—serves legitimate law enforcement purposes.[176] This fits in with what China sees as the purpose of law enforcement generally. Law enforcement in China does not merely protect public safety—it is also instrumental in suppressing opposition to the CCP.[177] This extends beyond the targeting of specific "threats" to the Party—i.e. political opposition—and to initiatives, such as social credit scores, designed to ensure the loyalty of the general public.[178]

However, it would be a mistake to dismiss comparisons between the surveillance tactics of law enforcement in the United States and China on the grounds that, whatever problems exist in the United States, genocide is not one of them. Facial recognition is used by law enforcement in the

---

(July 15, 2011), https://www.lawfareblog.com/what-ben-franklin-really-said.

[172] Eugene Volokh, *Liberty, Safety, and Benjamin Franklin*, THE WASH. POST (Nov. 11, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/11/11/liberty-safety-and-benjamin-franklin/.

[173] *See* United States Department of State, *Country Reports on Human Rights Practices for 2019 – China* 1 (Mar. 11, 2020), https://www.state.gov/wp-content/uploads/2020/03/CHINA-INCLUSIVE-2019-HUMAN-RIGHTS-REPORT.pdf (describing China as an authoritarian state where the CCP is the paramount authority and how law enforcement are under the authority of the CCP and the Central Military Commission, controlled by Xi Jinpaing), 23-26 (outlining how various law enforcement bodies in China use surveillance).

[174] *Id.* at 23.

[175] *Id.* at 1; duPont, *supra* note 133.

[176] Edward Wong and Chris Buckley, *U.S. Says China's Repression of Uighurs is 'Genocide'*, N.Y. TIMES (Jan. 19, 2021), https://www.nytimes.com/2021/01/19/us/politics/trump-china-xinjiang.html.

[177] *See generally China Country Report*, *supra* note 173 (discussing treatment of political dissidents, disfavored minorities, and human rights activists by law enforcement).

[178] *Id.* at 24-25; *see also China invents the digital totalitarian state, supra* note 68.

United States to identify protestors, immigrants, and even journalists.[179] License plate readers track citizens in real time.[180] Predictive policing initiatives in the United States, such as threat scores, bear a strong resemblance to similar initiatives in China.[181] And all of this just scratches the surface. American law enforcement is focused on collecting as much data as it can, and then figuring out how to use it later.[182] Undoubtedly, there are also surveillance initiatives in place that we have yet to learn about.

These tools help law enforcement solve and deter crimes, though at the expense of individual privacy. It would also be a mistake, however, to ignore the impact of getting caught in the crosshairs simply because the stakes are not as high as in China.[183] Perhaps it is a bargain Americans are willing to make.[184] If so, we should be honest about the cost.

[179] *duPont, supra* note 133.

[180] BRAYNE, *supra* note 139.

[181] Gallagher*, supra* note 127.

[182] Schwartz*, supra* note 144.

[183] *See, e.g.*, *COINTELPRO supra* note 98; BRAYNE, *supra* note 139 at 39 (noting that surveillance efforts continue apace without consideration of how it may impact people who are wrongly targeted).

[184] There is evidence to suggest that this is indeed the case. *See* Smith, *supra* note 133.