DePaul University
University Libraries

DePaul Journal of Art, Technology & Intellectual Property Law

Volume 31
Issue 1 *2021 Issue*

Article 1

# The Data Privacy Landscape During COVID-19: An Exploration of Some of the Major Data Privacy Regulations and Trends

Gitanjali Deb

# THE DATA PRIVACY LANDSCAPE DURING COVID-19: AN EXPLORATION OF SOME OF THE MAJOR DATA PRIVACY REGULATIONS AND TRENDS

*Gitanjali Deb**

In light of the current global pandemic, data privacy regulations are more important than ever before. Historically with the rise of the internet, the dawning of an electronic communications era took hold around the world. Starting in the 1990s, advancements in internet-based communications technology have expanded from rudimentary email, simple message boards, and chat rooms to include everything from the World Wide Web, biometric records, GIS technologies, social media platforms, cryptocurrencies, the internet of things, and much more.[1] All of these technologies have the capacity to collect, analyze, store, and use data in cyberspace.[2] With many countries around the world on lockdowns due to COVID-19, everyone has become more reliant on these technologies. How we collect, store, use, and protect this data has and will continue to have a dramatic effect on issues from personal

* Gitanjali "Mishty" Deb graduated from the University of Texas law school in 2005. She is the co-founding partner of LaSusa & Deb, PLLC, which is a general practice law firm. Mishty has worked extensively in the governmental, nonprofit, and private sectors throughout her legal career. Her primary focus is to provide practical counsel and has handled numerous cases for businesses of all sizes as well as for non-profits, entrepreneurs, and individuals.

[1] Gil Press, *A Very Short History of the Internet and the Web*, FORBES.COM (Jan. 2, 2015), https://www.forbes.com/sites/gilpress/2015/01/02/a-very-short-history-of-the-internet-and-the-web-2/?sh=108780c7a4e2; Evan Andres, *Who invented the Internet?*, HISOTRY.COM (Updated Oct. 28, 2019, Original Dec. 18, 2013), https://www.history.com/news/who-invented-the-internet; Michael Aaron Dennis, *Internet: Computer Network*, BRITANNICA.COM (last updated Feb. 26, 2020), https://www.britannica.com/technology/Internet.

[2] Ernesto Rubio, *Big Data: Where is our Data Stored: Law and Cyber Security*, SANTANDERGLOBALTECH.COM, (Nov. 19, 2019), https://santanderglobaltech.com/en/where-is-our-data-stored-law-and-cyber-security/; *Patrick McFadin, Internet of things: Where does the Data Go?*, WIRED.COM (Mar. 2015), https://www.wired.com/insights/2015/03/internet-things-data-go/.

privacy, safety, terrorism, national security, the economy, and more.[3]

As we integrate more of this technology into our daily lives, these issues have started to affect every aspect of modern society. Under the pandemic we have experienced a situation in which much of the world's population has been subject to mandatory or voluntary shutdowns forcing individuals and businesses to become reliant upon internet-based purchasing, delivery, and communication.[4] This in turn arguably has pushed our society even further from having in-person physical transactions towards living primarily through web-based communication.[5] This trend is putting even

[3] *See* Statement of F.T.C. Comm'r Chopra et al., Regarding Social Media and Video Streaming Service Providers' Privacy Practices, File No. P205402 (Dec. 14, 2020), https://www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-social-media-video-streaming-service-providers/joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf.; Email from Donald Rumsfeld, Secretary of Defense, to William Schneider, Jr., Chair of Defense Science Board (April 30, 2001, 06:02pm), https://assets.documentcloud.org/documents/4357755/11-L-0559-First-Release-Bates-1-912.pdf#page=198; S. Staniford et al., *The US is Not Safe in a Cyberwar* (presented to DARPA, Sept. 2000) https://assets.documentcloud.org/documents/4357755/11-L-0559-First-Release-Bates-1-912.pdf#page=198; Brennan Weiss, *New York is Quietly Working to Prevent a Major Cyber Attack That Could Bring Down the Financial System*, BUSINESSINSIDER.COM (Feb. 25, 2018), https://www.businessinsider.com/new-york-cybersecurity-regulations-protect-wall-street-2018-2.

[4] Lillian Rizzo & Sawyer Click, *How Covid-19 Changed Americans' Internet Habits: Broadband Usage surged in mid-March as Millions of Americans turned to the internet to work, Learn and Communicate at Home,* THE WALL STREET JOURNAL (Aug. 15, 2020), https://www.wsj.com/articles/coronavirus-lockdown-tested-internets-backbone-11597503600; Rahul De', Neena Pandey, & Abhipsa Pal, *Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice*, 55 INT'L J. INFO. MGMT. (Dec. 2020), https://www.sciencedirect.com/science/article/abs/pii/S0268401220309622?via%3Dihub.

[5] Giada Pietrabissa & Susan G. Simpson, *Psychological Consequences of Social Isolation During COVID-19 Outbreak*, FRONT. PSYCHOL. (Sept. 9, 2020), https://www.frontiersin.org/articles/10.3389/fpsyg.2020.02201/full; Chris Stokel-Walker, *We'll be less touchy-feely and far more wary, but the transition will feel strange*, BBC.COM (Apr. 29, 2020), https://www.bbc.com/future/article/20200429-will-personal-contact-change-

more power into the hands of few tech giants, who profit primarily from their ability to collect and use data.[6]

Therefore, the need for regulation is clear. Incidents such as the Apple iCloud photo leaks in 2014[7], the Equifax data breach in 2017[8], the Target data breach in 2013[9], the Capital One breach in 2019[10], the 2016 U.S. Cambridge Analytica scandal[11], and the current

due-to-coronavirus; Kathryn Vasel, *Here's How the Pandemic Has Changed Work Forever*, CNN.COM (Dec. 21, 2020), https://www.cnn.com/2020/12/21/success/job-change-remote-work-pandemic/index.html; Nick Hartley, *Coronavirus: Will lockdown change the way we shop forever?*, BBC.COM (Jun. 20, 2020), https://www.bbc.com/news/uk-wales-53052556; Gideon Lichfield, *We're Not Going Back to Normal: Social Distancing is Here to Stay for Much More Than a Few Weeks. It Will Upend Our Way of Life, in Some Ways Forever*, MIT TECHNOLOGY REVIEW (March 17, 2020), https://www.technologyreview.com/2020/03/17/905264/coronavirus-pandemic-social-distancing-18-months/.

[6] Rani Molla, *As CoVID-19 Surges, the World's Biggest Tech Companies Report Staggering Profits- Despite Antitrust Investigations and a Recession, Big Tech is doing Great.*, VOX.COM (Oct. 30, 2020), https://www.vox.com/recode/2020/10/30/21541699/big-tech-google-facebook-amazon-apple-coronavirus-profits.

[7] Steve Kovach, *We Still Don't Have Assurance From Apple That iCloud Is Safe*, BUSINESSINSIDER.COM (Sept. 2, 2014), https://www.businessinsider.com/apple-statement-on-icloud-hack-2014-9.

[8] Federal Trade Commission, *Equifax Data Breach Settlement*, FTC.GOV, (Jan. 2020), https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

[9] Maggie McGrath, *Target Data Breach Spilled Info. on as Many as 70 Million Customers*, FORBES.COM, (Jan. 10, 2014), https://www.forbes.com/sites/maggiemcgrath/2014/01/10/target-data-breach-spilled-info-on-as-many-as-70-million-customers/?sh=37aeed17e795.

[10] Emily Flitter & Karen Weise, *Capital One Data Breach Compromises Data of Over 100 Million*, NYTIMES.COM (July 29, 2019), https://www.nytimes.com/2019/07/29/business/capital-one-data-breach-hacked.html.

[11] Alexandra Ma & Ben Gilbert, *Facebook Understood How Dangerous the Trump-linked Data Firm Cambridge Analytica Could Be Much Earlier Than it Previously Said. Here's Everything That's Happened Up Until Now*, BUSINESSINSIDER.COM (Aug. 3 2019), https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-

SolarWinds Orion Russian hacking scandal (estimated to have affected over 18,000 global customers, including many U.S. government agencies) [12] demonstrate the risks associated with inadequate cybersecurity protections for data collection and storage on a large scale. Combining these incidents with the uptick in the number of identity theft, online bullying, and catfishing incidents shows how cyberspace can affect individuals on a personal level as well.[13]

These issues are more complex when we acknowledge that at the heart of many of these issues are ethical concerns. Companies control the information that they collect from an individual and how they use it is a major ethical issue. This is not only because the nature of the information is both personal and sensitive, but also because the potential for abuse is enormous. This information can be used to manipulate the behavior of individuals, spread misinformation, commit terrorist attacks, commit crimes like identity theft, and much more.

These ethical issues are particularly important since personal data is highly valuable. Often this data has been collected almost passively without the affirmative consent of individuals for the benefit of

3#:~:text=In%20early%202018%2C%20Facebook%20and,the%20political%20data%2Danalytics%20firm.

[12] Alex Marquardt et al., *Microsoft identifies more than 40 organizations targeted in massive cyber breach*, CNN.COM (Dec. 17, 2020), https://www.cnn.com/2020/12/17/politics/microsoft-hack-organizations/index.html?fbclid=IwAR3iPRVSc58vDYam__cOTH5gBnG_XompeuHUXO0eS-VvmB3YU8ZMFqQB1Sg.

[13] Scott Ikeda, *New Security Report Breaks Down Increase in Cyber Attacks Due to Remote Work; Lack of Training, Overwhelmed IT Departments are the Main Issues*, CPOMAGAZINE.COM (Oct. 16, 2020) https://www.cpomagazine.com/cyber-security/new-security-report-breaks-down-increase-in-cyber-attacks-due-to-remote-work-lack-of-training-overwhelmed-it-departments-are-the-main-issues/; Tom Burt, *Microsoft Report Shows Increasing Sophistication of Cyber Threats*, BLOGS.MICROSOFT.COM, (Sept. 29, 2020), https://blogs.microsoft.com/on-the-issues/2020/09/29/microsoft-digital-defense-report-cyber-threats/; Sam Cook, *Cyberbullying Facts and Statistics for 2020*, COMPARITECH.COM (Nov. 11, 2020), https://www.comparitech.com/internet-providers/cyberbullying-statistics/.

corporations.[14] The more data a corporation can collect the more powerful it can become. [15] This is perfectly demonstrated with the recent case of FaceAPP a selfie-taking mobile app, which altered the appearance of users to look older. The app asked users to sign over the rights to their own images to be used for whatever purposes the FaceAPP owners want to use them for. Many users not reading the fine print signed over these rights to their images without even knowing it. FaceAPP later clarified their policy, but consumers are still suspicious of the app's intentions.[16]

The recent documentary, *The Social Dilemma*, serves to further highlight ethical issues by underscoring the implications of companies and political interests collecting an individual's data to manipulate and alter their behavior. The possibilities for manipulation of thought and behavior both on individual and societal scales are very troubling, to say the least.[17]

In addition to ethical concerns, the way in which data is collected, stored, and used data has national security issues at its core as well. The more data a country or government can collect, the more powerful it can become. This can be seen with the 2016 U.S.

---

[14] Natasha Lomas, *Europe is Drawing Fresh Battle Line Around the Ethics of Big Data- First GDPR Fines Coming this Year is Just the Start, Says Data Protection Supervisor*, TECHCRUNCH.COM (Oct. 3, 2018), https://techcrunch.com https://techcrunch.com/2015/10/13/whats-the-value-of-your-data//2018/10/03/europe-is-drawing-fresh-battle-lines-around-the-ethics-of-big-data/; Stephen Ritter, *The Ethical Data Dilemma: Why Ethics Will Separate Data Privacy Leaders From Followers*, FORBES.COM (Mar. 31, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/03/31/the-ethical-data-dilemma-why-ethics-will-separate-data-privacy-leaders-from-followers/?sh=c4edfbd14c6a; Peter K. Yu, *The Political Economy of Data Protection*, 84 CHI.-KENT L. REV. 777, 777-801 (2010).

[15] Pauline Glikman & Nicolas Glady, *What's the Value of Your Data*, TECHCRUNCH.COM (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

[16] Chris Baranuik, *Can You Trust FaceAPP With Your Face*, BBC.COM (July 17, 2019), https://www.bbc.com/news/technology-49018103#:~:text=But%20since%20the%20face%2Dediting,48%20hours%20of%20being%20uploaded.

[17] THE SOCIAL DILEMMA (Netflix 2020).

presidential election and the recent Solar Orion hacking of U.S. government agencies, the scope of which is still under investigation. Currently, we know that this incident led to data breaches of many U.S. government agencies with sensitive information.[18] Specifically, the 2016 election showed how outside groups created fake accounts and posts on social media platforms potentially influencing the results of the election. Our inability to separate real and fake posts, or real and fake posters, is a major concern that creates real sociopolitical and national security issues. Furthermore, it brought to light the direct risk of foreign governments and organizations simply hacking into data stored in databases as important for national security.[19]

Even though safety, security, and privacy issues make it clear that regulation is needed, there have been concerns about the regulatory burden laws place on businesses, governments, and individuals that until recently were able to take advantage of data collection, analysis, storage, and use online with little impunity.[20] This transfer of data and information from individuals to large corporations and governments has fueled so much wealth, power, and technological advancement, understandably there is hesitation on the who, what, when, why, and how we regulate it.[21] In the meantime, it is

[18] Marquardt et al., *supra* note 12.
[19] Elizabeth Weise, *Russian Face Accounts Showed Posts to 126 Million Facebook Users*, USATODAY.COM (Oct. 30, 2017), https://www.usatoday.com/story/tech/2017/10/30/russian-fake-accounts-showed-posts-126-million-facebook-users/815342001/; S. Staniford et al., *The US is Not Safe in a Cyberwar*, Paper presented to DARPA (Sept. 2000), https://assets.documentcloud.org/documents/4357755/11-L-0559-First-Release-Bates-1-912.pdf#page=198.
[20] William R. Denny, *Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act*, AMERICANBAR.ORG (June 20, 2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/06/cyber_center_denny/.
[21] *See* FTC, Statement of Comm'r Chopra, Slaughter, & Wilson, Regarding Social Media and Video Streaming Service Providers' Privacy Practices Commission File No. P205402 (Dec. 14, 2020), https://www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-social-media-video-streaming-service-

becoming apparent that the large companies controlling the data and the platforms like Facebook, Amazon, Twitter, and Google are growing more powerful.[22] That power previously went mostly unchecked until 2002 when the Federal Trade Commission (FTC) started pursuing cybersecurity cases as unfair practices[23]. But we are slowly seeing that change with the recent events of the last 15 years serving as wake-up calls to governments and individuals around the world creating trends of specific data regulations.

This paper will look at the current major data privacy regulations in place in the U.S. and Europe as well as the different trends in regulation and enforcement. In particular, the paper will review the key points of the regulatory frameworks under General Data Protection Regulation ("GDPR")[24] in the EU; 15 U.S.C. § 45 ("Section 5")[25]; 15 U.S.C. § 46(b) & (f) ("Section 6")[26], and Children's Online Privacy Protection Act (COPPA)[27] in the U.S.; and the California Consumer Privacy Act ("CCPA") in the state of California.[28] Additionally, the paper will examine the questions of how the rights of individuals, corporations, and governments might

providers/joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf.

[22] Rani Molla, *As CoVID-19 Surges, the World's Biggest Tech Companies Report Staggering Profits- Despite Antitrust Investigations and a Recession, Big Tech is doing Great.*, VOX.COM (Oct. 30, 2020), https://www.vox.com/recode/2020/10/30/21541699/big-tech-google-facebook-amazon-apple-coronavirus-profits.

[23] Denny, *supra* note 20.

[24] Reg. 2016-679 of the European Parliament and of the Council on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Advancement of Such Data, and repealing Directive 95-46-EC, 2016 O.J.L./1 [Hereinafter the "General Data Protection Regulations" or "GDPR"].

[25] Federal Trade Commission Act, 15 U.S.C. § 45 (2019) .

[26] *Id.* § 46(b),(f).

[27] Children's Online Privacy Protection Act, 15 U.S.C. § 6501 *et seq* [Hereinafter "COPPA"].

[28] California Consumer Privacy Act of 2018, Cal. Civ. Code § 1798.1 *et seq* [Hereinafter "CCPA"].

play out in these upcoming big data wars by looking at some of the current enforcement trends.

**European Union (EU) General Data Protection Regulation (GDPR):**

The European Union's General Data Protection Regulation ("GDPR") is likely what comes to mind as the most comprehensive cybersecurity regulation adopted by a government. Coming into full force in May of 2018 the world has been watching the EU's rollout of GDPR closely.[29] It replaced the earlier 1995 Data Protection Directive ("DPD").[30] To understand the regulation more fully it is important to look at the jurisdiction and scope that it covers, the subject matter it regulates, the liabilities it creates, how it has been enforced, the central provisions, and some both observable and predicted trends.

1. *Subject Matter and Jurisdiction.* When we think of jurisdiction in terms of regulations, we are typically thinking of what types of subject matter or cases would fall under the regulation, and who would be subject to the regulation. In this case, we will look at what fall under GDPR's territorial and material scope. The subject matter regulated under GDPR can be broadly defined as data.[31] More specifically, to be governed by GDPR, data must be the personal data of natural persons.[32] GDPR itself excludes the data of corporations by its language stating, "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[33] GDPR goes on to narrow its scope to only the data of those natural persons, who are EU citizens or residents, individuals located inside the EU.[34]

[29] GDPR, *supra* note 24.
[30] Council Directive 95-46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. L. 28132.
[31] GDPR, art. 1.
[32] GDPR, art. 2-3.
[33] GDPR, art. 1(2).
[34] GDPR, art. 2, 4(1); Ben Wolford, *Does the GDPR apply to companies outside of the EU?*, Complete guide to GDPR compliance, PROTON TECHNOLOGIES AG

Interestingly, this means that the drafters intentionally excluded data from non-natural persons. This makes logical sense as such corporate data would normally fall under other regulations such as Intellectual Property Rights and trade secrets.

The regulation also goes so far as establishing specific rights for the natural persons that will be protected under the statute. These rights include, but are not limited to, the right of natural persons to (1) opt-out of data collection[35], (2) right to prevent others from profiting from their data[36], (3) the right to access any data collected from them[37], (4) the right to know how their data will be used[38], and (5) the right for their data to be forgotten or the right of data portability[39].

Now that we understand the rights that the statute sets out and who it protects, we should ask who will be governed and regulated by the statute? GDPR limits its scope to regulating those parties that are engaging in:

> "(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union." [40]

This means that parties do not have to be located within the European Union to be subject to GDPR.[41] Does this mean that anyone who has a website accessible to those

(2020), http:// https://gdpr.eu/companies-outside-of-europe/#:~:text=The%20GDPR%20does%20apply%20outside,%E2%80%9Cextra%2Dterritorial%20effect.%E2%80%9D.

[35] GDPR, art. 6-8.
[36] GDPR, art. 18.
[37] GDPR, art. 15.
[38] GDPR, art. 13.
[39] GDPR, art. 17, 19, 20.
[40] GDPR, art. 3(2)(a).
[41] *Id.*

in the EU is subject to GDPR? Not exactly. Accessibility alone is not enough. A website must somehow be customized to the EU viewer. For example, the use of different languages, country-specific domains, the listing of prices in EU currencies, or marketing campaigns targeted specifically at EU citizens are factors that will make a site subject to GDPR[42]

It is also important to note that GDPR makes a point of directly targeting certain means of data collection by stating, "the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system."[43] It then goes further to list several exceptions such as natural persons collecting data for normal family or household activities or law enforcement agencies trying to investigate or prosecute criminal activity.[44] Both important, practical, and logical exceptions balancing the need for law enforcement to access and use data, and the need of individuals to be able to access and control data for members of their household against personal data collection for other purposes.

2. *Liabilities.* The GDPR maximum penalties are limited to the greater of 4% of worldwide annual revenue or €20 million.[45] These maximum penalties are of course intended to grab the attention of large companies and incentivize them to comply.

3. *Enforcement.* To examine GDPR's implementation we can look at the major cases that have been decided under the regulation. While there are many GDPR cases that are

[42] Detlev Gabel & Tim Hickman, *Chapter 1: The Rapid Evolution of Data Protection Laws*, THE INTERNATIONAL COMPARATIVE LEGAL GUIDE TO: DATA PROTECTION 2019 1 (6 ed.), https://iapp.org/media/pdf/resource_center/comparative_legal_guide_2019.pdf.
[43] GDPR, art. 2(1).
[44] GDPR, art. 2(2).
[45] GDPR, art. 83.

currently pending, there are arguably a handful of precedent-setting cases to take note of.

A. *Google.* The largest fine collected so far at a remarkable €50 million was imposed against Google by the French Data Regulator (CNIL)[46] for, "lack of transparency, inadequate information and lack of valid consent regarding the ads personalization."[47] In this case, the regulators faulted Google for not make it clear to users how their data was being used or how it was being collected. This put Google in violation of Article 12(1) of GDPR. Additionally, they found that because of the lack of clearly stated information the consent given by users did not meet the threshold for clear and informed consent under Article 7 of GDPR. Due to these shortcomings regulators also found that Google failed to establish a legal basis authorizing them to collect and process data from those individuals under Article 6 (1)(a) of GDPR.[48]

B. *Anonymous or "John Doe" LLC.* This case deals with information that we ordinarily might think is not personal data because it deals with public places, where often legally it is deemed that people do not or should not have an expectation of privacy.

[46] Adam Satariano, *Google is Fined $57 Million Under Europe's Data Privacy Law*, NYT.COM (Jan. 21, 2019), https://www.nytimes.com/2019/01/21/technology/google-europe-gdpr-fine.html.

[47] CNIL-National Commission for Computing and Liberties, *The CNIL's restricted committee imposes a financial penalty of 50 Million euros against Google LLC*, CNIL.FR (Jan. 19, 2020), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

[48] Council of State, *Sanction imposed on Google by the CNIL*, CONSEIL-ESTAT.FR (June 19, 2020), https://www.conseil-etat.fr/ressources/decisions-contentieuses/dernieres-decisions-importantes/conseil-d-etat-19-juin-2020-sanction-infligee-a-google-par-la-cnil; Vera Cherepanova, *GDPR Enforcement Report (May 2019)*, THE FCPA BLOG (May 14, 2019), https://fcpablog.com/2019/5/14/gdpr-enforcement-report-may-2019/.

However, we can look at GDPR as a regulation being imposed on data collectors rather than a regulation based on the privacy expectations of the individual data subjects, which in this case would be their expectation for public spaces to not be private. In this case, the limited liability company acting as the data collector, which was kept anonymous, was a sports betting café. The LLC installed CCTV cameras on public streets and parking lots. The Austrian Data Regulator (DSB) fined the LLC for violating GDPR regulations. Specifically, they found that the LLC had violated lawfulness, fairness, and transparency under Article 5(1) of GDPR, the requirement to apply the data minimization principle under Article 5(1)(c) of GDPR and, therefore, had failed to establish a legal basis authorizing them to collect and process data from those individuals under Article 6(1)(a) of GDPR. [49]

C. *Centro Hospital Barreiro Montijo.* This case focused on several different violations of GDPR. Portuguese Data Regulator (CNPD) fined Centro Hospital Montijo ("Centro Hospital"), €400,000 for these violations. It was discovered that the hospital had only 296 doctors working at the hospital, but 985 doctor accounts. Additionally, the information available to these accounts granted unlimited access to patient records and was not limited in any way based on the specialty of the doctor. Regulators found this to violate (1) the data minimization principle established under Article 5(1) of GDPR, (2)

[49] European Data Protection Board, *First Australian Fine: CCTV Coverage - Summary*, EDPB.EUROPA.EU (Sept. 12, 2018), https://edpb.europa.eu/news/national-news/2018/first-austrian-fine-cctv-coverage-summary_en; Vera Cherepanova, *GDPR Enforcement Report (May 2019)*, THE FCPA BLOG (May 14, 2019), https://fcpablog.com/2019/5/14/gdpr-enforcement-report-may-2019/; Gernot Fritz, *First GDPR Fine Issued by Austrian Data Protection Regulator*, FRESHFIELDS BRUCKHAUS DERINGER (Oct. 5, 2018), https://digital.freshfields.com/post/102f39w/first-gdpr-fine-issued-by-austrian-data-protection-regulator.

the integrity and confidentiality principle established under Article 5(1)(f) of GDPR and (3) its duty to implement appropriate security measure under Article 32 of GDPR.[50]

D. *Knuddels.de.* This case is notably the only one of these major cases that involves a data breach. The breach involved outside hackers, who were able to collect 808,000 user email addresses and passwords that had been stored by Knuddels.de in an unencrypted form. Regulators deemed this to be a breach of the requirement for data collectors to guarantee to store personal data in a secure form under Article 32 (1)(a) of GDPR. The German Data Regulator (LfDI) imposed a €20 thousand fine against Knuddles for this violation. When comparing this fine to the fines imposed on the other cases we have looked it at it appears at first glance to be nominal. However, in this case, it seems the size of the fine was intentionally low as regulators stated the company cooperated with regulators and has since the breach occurred made intentional and systematic improvements to its IT security.[51]

When looking at these cases, there are some clear takeaways at least in terms of how the regulation has been enforced so far. European data protection agencies are particularly focused on Articles 5, 6, 7, 12, and 32. Of course, there are a lot of cases that are still pending in court and it may still be too early to know if this will be a lasting

[50] Ana Monteiro, *First GDPR Fine in Portugal Issued Against Hospital for Three Violations*, IAPP.ORG (Jan. 3, 2019), https://iapp.org/news/a/first-gdpr-fine-in-portugal-issued-against-hospital-for-three-violations/; Vera Cherepanova, *GDPR Enforcement Report (May 2019)*, THE FCPA BLOG (May 14, 2019), https://fcpablog.com/2019/5/14/gdpr-enforcement-report-may-2019/.
[51] Oliver Smidt, *Germany's First Fine Under the GDPR Offers Enforcement Insights*, IAPP.ORG (Nov. 27, 2018), https://iapp.org/news/a/germanys-first-fine-under-the-gdpr-offers-enforcement-insights/; Vera Cherepanova, *GDPR Enforcement Report (May 2019)*, THE FCPA BLOG (May 14, 2019), https://fcpablog.com/2019/5/14/gdpr-enforcement-report-may-2019/.

prosecutorial trend or not. There have been thousands of complaints filed to Data Regulators and thousands of breaches reported. [52] Many countries were initially unprepared. [53] Regulators may shift their focus to other provisions as time passes and they refine their systems.

4. *Central Provision.* Given that regulators are focusing on Articles 5, 6, 7, 12, and 32 going through and further examining these articles can be helpful.

    A. *Article 5: Principles relating to processing of personal data.* This article of GDPR clearly lists out limitations on how the personal data of individuals may be processed or used. In particular, it states that processing should be done only in accordance with the following principles: (i) the principle of lawfulness, fairness, and transparency: that personal data will be "processed lawfully, fairly and in a transparent manner in relation to the data subject,"[54] (ii) the principle of purpose limitation: that personal data must "be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes,"[55] except when processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes,"[56] (iii) the principle data minimization: that personal data collection will be "adequate, relevant and limited to what is

[52] Natasha Lomas, *Privacy Complaints Received by Tech Giant's Favorite EU Watchdog Up More Than 2x Since GDPR*, TECHCRUNCH.COM (Feb. 28, 2019), https://techcrunch.com/2019/02/28/privacy-complaints-received-by-tech-giants-favorite-eu-watchdog-up-more-than-2x-since-gdpr/; John Choudhari, *Cataloging GDPR Complaints Since May 25*, IAPP.ORG (June 25, 2018), https://iapp.org/news/a/cataloguing-gdpr-complaints-since-may-25/.

[53] Donata Kalnenaite, *Week Two of GDPR: We're Still Not Ready,* THENEXTWEB.COM (June 9, 2018), https://thenextweb.com/contributors/2018/06/09/week-two-of-gdpr-were-still-not-ready/.

[54] GDPR, art. 5(1)(a).

[55] GDPR, art. 5(1)(b).

[56] *Id*.

necessary in relation to the purposes for which they are processed."[57], (iv) the principle of accuracy: that the data must be accurate and kept accurate, (v) the principle of storage limitation: that personal data, which is identifiable to the individual must not be "kept for longer than necessary," [58] and (vi) the principle of integrity and confidentiality: that personal data must be kept securely " including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures." [59] This article also affirmatively states that the collectors and processors of the personal data are responsible for demonstrating compliance with these regulations. [60]

B. *Article 6: The Lawfulness of processing.* This article of GDPR limits what types of data processing are legal. For the purposes of understanding this section, it is important to note that GDPR generally defines data processing as "the gathering, processing or use of personal data by a processor in accordance with the instructions of the controller based on a contract."[61] Wherein the processor and controller are defined by their roles. The controller being the point of initial contact with the data subject and primarily responsible for legal compliance and the processor is limited to process data in accordance with the instructions of the controller. This section states that data processing is allowed with the data subject's consent.[62] Furthermore, Paragraph 1 of this article specifically lists a series of limiting circumstances

[57] GDPR, art. 5(1)(c).
[58] GDPR, art. 5(1)(e).
[59] GDPR, art. 5(1)(f).
[60] GDPR, art. 5(2).
[61] GDPR, art. 4(2); Intersoft Consulting, *GDPR Processing*, GDPR-INFO.EDU (Dec. 2020), https://gdpr-info.eu/issues/processing/.
[62] GDPR, art. 6(1)(a).

under which data processing is legal if the data subject has not consented. These include if the processing is necessary to perform a contract at the data subjects request, to comply with a legal obligation, to protect the vital interests of a natural person, carry out a task in the public interest, or for the purposes of a legitimate interest of the comptroller or third party. The paragraph specifically excepts instances when the rights, freedoms, and interests of the data subject, particularly when the data subject is a minor, require protection of personal data.[63] Paragraphs 2 & 3 elaborate the criteria for each member state to implement this part of the regulation into their own rules, how to apply it, and, also, how to enact rules to elaborate on the legal interest and public interest might be under that member state's laws.[64] Paragraph 4 sets out factors for a controller to use to determine if processing for another purpose is allowable absent the data subjects consent or absence of specific member state regulation. These factors include: (a) a link between the purpose of the data collection and the need for processing, (b) the context of the original data collection including the relationship between the data subject and the controller, (c) the nature of the data collected, particularly, if in relation to criminal history information, (d) the consequences of the processing for the data subjects, and (e) safeguards being used including pseudonymization and encryption.[65]

C. *Article 7: Conditions for consent.* This article puts the burden on the controller to be able to demonstrably prove that the data subject has given consent. It states that language used to obtain consent should be clear and easily understood. The

[63] GDPR, art. 6(1).
[64] GDPR, art. 6(2)-(3).
[65] GDPR, art. 6(4).

article further states that the controller must allow the data subject to withdraw consent at any time, but that such withdrawal will not make any processing that occurred after the initial consent and prior to the withdrawal a violation. Last but not least, the provision states that if data processing is not required or necessary for the controller to perform on a contract then it should not be requiring consent from a data subject to enter into said contract. [66]

D. *Article 12: Transparent information, communication, and modalities for the exercise of the rights of the data subject.* This article makes it clear that controllers must be completely transparent regarding their processing and use of the data subject's data. Specifically, it states that all communication with the data subject must be, "concise, transparent, intelligible, and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child." [67] This makes practical sense since often minors are the ones that are using and accessing various websites that may be collecting data. The article goes on to state that a controller should facilitate a data subject's rights and may not refuse to act upon a request by a data subject to exercise their rights.[68] Similarly, the section states that controllers must act on requests from data subjects wanting to exercise their rights, as enumerated in Articles 15-22 of GDPR, within a specified time period and without delay.[69] It goes on to state that such action requests or communications under Articles 13-22 and Article 34 will be provided by the controller for the data subject free of charge.[70] The article does, however, provide exceptions for

[66] GDPR, art. 7.
[67] GDPR, art. 12(1).
[68] *Id.*
[69] GDPR, art. 12, 15-22.
[70] GDPR, art. 12-22, 34.

circumstances where the data subjects are unfounded, excessive, or repetitive. In such circumstances, the controller may charge an administrative fee or refuse to act. [71] Note that in such circumstances the controller will be responsible for providing evidence that the request was unfounded or excessive should a complaint be filed under the statute. Here in this article, we also see that the controller may actually require the data subject to provide information necessary to verify their identity.[72] Interestingly, the article also specifically addresses the issue of using icons to clearly communicate the intended processing stating that such icons must be machine-readable and that the commission may create its own acts to father elaborate on the use of such icons.[73]

E. *Article 32. Security of Processing.* This article addresses one of the central concerns that many have regarding the use and processing of data online, which is security. Some of the factors that a controller and processor must consider when determining if their security measures are adequate include assessing the risk of a data subject's information and rights being compromised, the severity of such possible compromise, and that the level of security that would be appropriate for the amount of assessed risk along with its the cost of implementation.[74] The article states that the risks associated with accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed are all risks that the controller and processor need to factor into their risk assessment.[75] The article also clearly states minimum requirements

[71] GDPR, art. 12(5).
[72] GDPR, art. 12(5)-(6).
[73] GDPR, art. 12(7).
[74] GDPR, art. 32(1).
[75] GDPR, art. 32(2).

> for security in data processing. Specifically, that such processing shall allow for: the encryption of personal data; the pseudonymization of personal data; to allow for the timely restoration of access and availability of personal data in the event of an incident or event; the ability to ensure ongoing integrity, availability, and confidentiality; the ability to have resilient processing services and systems; and have a set process for ongoing testing, evaluation, and assessment of the organizational and technical mechanisms being used to provide secure processing in accordance with these requirements.[76] It is important to note that here the regulation particularly states that the controller and processor are responsible for the actions of all natural persons acting under their authority.[77] This is important because it demonstrates the intent of the drafters to not allow controllers and processors to escape liability by blaming employees. This seems like a rather onerous burden. However, the article also provides two methods by which a controller or processor can be assured they are taking the rights steps. One is to use a code of conduct under Article 40, which allows trade and industry organizations as well as member states to establish a code of conduct for security measures.[78] The other is to use an approved certification method set out under Article 42, which a voluntary transparent process allowing for controllers and processors to ensure compliance before any issues arise.[79]

5. *Implementation/Trends.* As we look at the major GDPR cases we see a focus on the provisions of articles 5, 6, 7, 12, and 32. More specifically emphasis on clear communication to users,

[76] GDPR, art. 32.
[77] GDPR, art. 32(4).
[78] GDPR, art. 32, 40.
[79] GDPR, art. 32, 42.

clear consent from users, minimizing the data collected, limitations on processing, and adequate security for any data stored. Additionally, it can be observed that cooperation and transparency play a crucial role in lessening penalties for violation. Thus, enforcement agencies want to encourage cooperation and transparency from data collectors. Looking at so many data privacy regulations that have been inspired by GDPR globally it would be reasonable to expect those regulations to also but a heavy emphasis on these types of provisions.

Though, GDPR itself has been a highly controversial piece of legislation. Many critics had warned of a variety of potential negative consequences due to any attempts at regulating the data marketplace. Some of the more popular of these hypothesized consequences have included, but are not limited to, (A) there is no need for regulation, (B) the high cost of implementation creating market stagnation, barriers to entry, loss of innovation, and relatedly loss of jobs; (C) opt-in fatigue and poor customer service; (E) roadblock to blockchain technology; and (F) less privacy.[80] In order to understand these arguments we should explore them individually:

A. *No need for Regulation.* Companies like Facebook and Google fundamentally make a large amount of their revenue from their ability to collect, store, process, and use data they collect from individuals. This allows these companies to sell products and services through targeted advertising or to allow other companies to use their platform to target advertising to their users.[81] In turn, individuals get to

[80] Alec Stapp, *GDPR After One Year: Costs and Unintended Consequences*, TRUTH ON THE MARKET (May 24, 2019), https://truthonthemarket.com/2019/05/24/gdpr-after-one-year-costs-and-unintended-consequences/; Forbes Technology Council, *15 Unexpected Consequences of GDPR*, FORBES (Aug. 15, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=3365f14994ad.

[81] Peter Fisk, *How Big Tech Makes Money… Alphabet, Amazon, Apple, Facebook, Microsoft… Are You the Customer or the Product,*

use their products for free. Many might argue that data privacy regulations like GDPR are overkill and there is no need to regulate the data collection market.[82]

In the past these companies have not had to pay for the information that they collected, nor did they have to be transparent on what information they were collecting from users, how they were collecting it, how they were storing it, why they were collecting it and how they were using it. This meant consumers were largely unaware of what was being done with their data and largely unaware of what they were consenting to when using these platforms and

THEGENUSWORKS.COM (March 1, 2019), https://www.thegeniusworks.com/2019/03/alphabet-amazon-apple-facebook-microsoft-are-you-the-customer-or-the-product/; Jeff Dunn, *The Tech Indsutry is Dominated by Big Companies- Here's How Each Makes Its Money*, BUSINESSINSIDER.COM (Mar. 26, 2017), https://www.businessinsider.com/how-google-apple-facebook-amazon-microsoft-make-money-chart-2017-5; Jennifer Golbeck, *Your Social Media "likes" Expose More Than You Think*, TED.COM (Oct. 2013), https://www.ted.com/talks/jennifer_golbeck_your_social_media_likes_expose_more_than_you_think?referrer=playlist-the_dark_side_of_data; Thu-Huong Ha, *What Are You Revealing Online? Much More Than You Think*, IDEAS.TED.COM (July 1, 2014), https://ideas.ted.com/do-you-know-what-youre-revealing-online-much-more-than-you-think/.

[82] Phil Robinson, *6 Myths About GDPR that Organizations are Falling For*, GLOBALSIGN.COM (Feb. 9, 2018), https://www.globalsign.com/en-sg/blog/6-myths-about-gdpr; Flowz, *Myth 5: GDPR is an Unnecessary Burden on Organizations*, FLOWZ.CO.UK (Nov. 14, 2017), https://flowz.co.uk/2017/11/14/myth-5-gdpr-is-an-unnecessary-burden-on-organisations/; Oliver Wessling, *GDPR: Tech Giant's Deathblow to Small Business and the Privacy Lie*, CPO MAGAZINE (June 4, 2018), https://www.cpomagazine.com/data-privacy/gdpr-tech-giants-deathblow-to-small-businesses-and-the-privacy-lie/; Forbes Technology Council, *15 Unexpected Consequences of GDPR*, FORBES (Aug. 15, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=3365f14994ad.

services. This is especially true when data collected from all these interactions are put together.[83]

For example, your Google GPS is collecting information on the places you go and where you are;[84] your Roomba robot vacuum has a map of your house; [85] your online Amazon purchase history shows what you buy; [86] your Facebook/Instagram/Twitter social media feeds show your political leanings, where your children go to school, your cultural background, who your friends are;[87] and your LinkedIn profile lets people know where you work and maybe a good idea of how much money you make.[88]

[83] Golbeck, *supra* note 81; Ha, *supra* note 81; Angela Moscaritolo, *What Does Big tech Know About You? Basically Everything*. ENTREPRENEUR.COM (Feb. 5, 2019), https://www.entrepreneur.com/article/327513.

[84] Robin Burks, *Google Maps Knows Where You're Going and Where You've Been*, TECHTIMES.COM (Aug.18, 2014), https://www.techtimes.com/articles/13326/20140818/google-maps-knows-where-youre-going-and-where-youve-been.htm.

[85] Maggie Astor, *Your Roomba May Be Mapping Your Home, Collecting Data That Could be Shared*, NYTIMES.COM (July 25, 2017), https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html.

[86] Jennifer Wills, *6 Ways Amazon Uses Big Data to Stalk You- Given What Amazon Knows, Should be Worried About Your Privacy?*, INVESTOPEDIA.COM (Oct. 5, 2020), https://www.investopedia.com/articles/insights/090716/7-ways-amazon-uses-big-data-stalk-you-amzn.asp.

[87] Andrew Hutchinson, *What Does Facebook Know About you Really?*, SOCIALMEDIATODAY.COM (Jan. 23, 2019), https://www.socialmediatoday.com/news/what-does-facebook-know-about-you-really/546502/; Kari Paul, *The Shocking Details You Reveal About Yourself When you "Like" Things on Facebook,* MARKETWATCH.COM (Mar. 25, 2018), https://www.marketwatch.com/story/the-shocking-things-you-reveal-about-yourself-when-you-like-things-on-facebook-2017-05-16; Golbeck, *supra* note 81; Ha, *supra* note 81; Moscaritolo, *supra* note 83.

[88] Lydia Dishman, *LinkedIn's New Salary Tool Offers Paycheck Insights, But There's A Catch,* FASTCOMPANY.COM (Feb. 27, 2019), https://www.fastcompany.com/90312931/linkedins-new-salary-tool-offers-paycheck-insights-but-theres-a-catch.

> When these companies start to share and sell this data they have collected about you, they can start marketing things to you before you even know you want them.[89] This may or may not be a bad thing until we consider what happens when that data gets breached or someone uses that information against you. Identity theft, fraud, revenge porn, blackmail, kidnapping, slander, terrorism, breaches in national security, and public safety are just the tip of the iceberg when it comes to how data can be abused when it is in the wrong hands.[90]
>
> It is important to see that before data privacy regulations these large organizations that collected the data bore little to no responsibility for its

[89] Golbeck, *supra* note 81.

[90] Al Habsi, A., Butler, M., Percy, A. et al., *Blackmail on social media: what do we know and what remains unknown?*, Secur J (2020), https://doi.org/10.1057/s41284-020-00246-2; Federal Bureau of Investigation, *Crimes Against Children/Online Predators*, FBI.GOV (last visited December 27, 2020), https://www.fbi.gov/investigate/violent-crime/cac; *Cyberbullying Facts and Statistics for 2020*, COMPARITECH.COM (Nov. 11, 2020), https://www.comparitech.com/internet-providers/cyberbullying-statistics/; *See* Fed. Trade Comm'n, *Statement of Comm'r Chopra, Slaughter, and Wilson, Regarding Social Media and Video Streaming Service Providers' Privacy Practices Commission*, File No. P205402 (Dec. 14, 2020), https://www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-social-media-video-streaming-service-providers/joint_statement_of_ftc_commissioners_chopra_slaughter_and_wilson_regarding_social_media_and_video.pdf; Email from Donald Rumsfeld, Secretary of Defense, to William Schneider, Jr., Chair of Defense Science Board (Apr. 30, 2001), https://assets.documentcloud.org/documents/4357755/11-L-0559-First-Release-Bates-1-912.pdf#page=198; S. Staniford, et al., *The US is Not Safe in a Cyberwar*, DARPA (Sept. 2000), https://assets.documentcloud.org/documents/4357755/11-L-0559-First-Release-Bates-1-912.pdf#page=198; Brennan Weiss, *New York is quietly working to prevent a major cyber attach that could bring down the financial system*, BUSINESS INSIDER (Feb. 25, 2018), https://www.businessinsider.com/new-york-cybersecurity-regulations-protect-wall-street-2018-2; Cristina Criddle, *'Revenge Porn New Normal' After Cases Surge in Lockdown*, BBC.COM (Sept. 16, 2020), https://www.bbc.com/news/technology-54149682.

> mishandling.[91] Specifically, if someone was targeted for these types of cybercrimes the data collection companies were not held accountable for allowing the data to get into the wrong hands. To make an analogy: if you keep your money in the bank, you assume it is the bank's responsibility to take reasonable measures to keep it safe. If they were to leave the bank vaults unlocked, the cash out in the open, the building unlocked, never installed any cameras, and go home every night leaving the buildings unlocked, customers would surely hold the bank responsible if the thieves just walked out with the money without any resistance. Of course, it is in the banks' interest to protect the money and it is also in the online data collector's interest to protect the data as well because it is valuable to them. Data is arguable the most valuable commodity online. However, the differences here are that: (1) customers know and acknowledge that they are depositing their money with the bank, (2) how valuable their money is when they entrust it to the bank, and (3) the bank is legally liable for the security of the money if they should lose it. After all, the money belongs to the customers and not the bank. Customers also know and understand the measure the bank will take to protect it, and that the bank will be responsible if something happens to it. This is not true for data without regulations. In the past when it came to data breaches it was often only the hackers and someone in the IT department used as a liability scapegoat for inadequate protections, who were held responsible, not the data collectors or processors. We do not want banks to mishandle other people's money and we don't want companies to mishandle other people's data either.

[91] Denny, *supra* note 20.

> Interestingly, existing regulations regarding privacy of personal information such as HIPAA (Health Insurance Portability and Accountability Act of 1996), FCRA (Fair Credit Reporting Act of 1970), RFPA (Right to Financial Privacy Act of 1978), GLBA (Gramm–Leach–Bliley Act, also known as the Financial Services Modernization Act of 1999), and FINRA (Financial Industry Regulatory Authority), in the United States do not seem to be subject to the same level of scrutiny. HIPPA which regulates data privacy and security for patient medical information is costly for those in the healthcare industry to implement. [92] Similarly, FCRA, RFPA, GLBA, and FINRA, along with a wide variety of smaller acts that have since been integrated into these regulations, which regulate personal identifiable information processes and storage within the financial industry, are also costly for those in financial services.[93] Though many argue broader non-industry specific data privacy is too onerous curiously there doesn't seem to be the same level of vocal free-market self-regulation opposition to any and all regulatory safeguards of personal health care and financial data as general personal data regulation is receiving.[94]

[92] Kim-Lien Nguyen, *HIPPA: At What Cost?*, MEDICALECONOMICS.COM (Sept. 9, 2019), https://www.medicaleconomics.com/view/hipaa-what-cost.
[93] LexisNexis Risk Solutions, *Financial Services Firms Spend $180.9 Billion on Financial Crime Compliance, According to LexisNexis Risk Solutions Global Study*, PRNEWSWIRE.COM (Apr. 7, 2020), https://www.prnewswire.com/news-releases/financial-services-firms-spend-180-9-billion-on-financial-crime-compliance-according-to-lexisnexis-risk-solutions-global-study-301036194.html; Stuart Brock, *The Cost of Compliance*, INTERNATIONALBANKER.COM (Nov. 7, 2018), https://internationalbanker.com/technology/the-cost-of-compliance/.
[94] Stapp, *supra* note 80; Forbes Technology Council, *15 Unexpected Consequences of GDPR*, FORBES (Aug. 15, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/?sh=3365f14994ad.

B. *High cost of implementation creating market stagnation, barriers to entry, loss of innovation, and relatedly loss of jobs.* At the crux of this set of arguments is the idea that GDPR will be too costly and onerous to implement. The statute rather clearly imposes both C-suite liability and large penalties of up to 4% of global revenue specifically to grab the attention of large companies, who are primarily the ones that are benefiting from collecting data.[95]

At first glance, it may appear that much of this argument is also based on the wide-sweeping nature of GDPR and the uncertainty of what data regulators want to be a complaint.[96] However, it seems from recent cases that data regulators are particularly focusing on those provisions discussed above, so there is no longer a mystery. As more cases work through the system the clearer the precedent will be. As with any piece of new legislation, there is some uncertainty until the caselaw is established, which is not an issue specific to GDPR.

Additionally, GDPR is continuously expanded upon in the EU with the goal of making it clearer as to what is expected from data collectors and users. This includes the Directive on Security Network and Information Systems or more commonly known as the NIS Directive. This regulation creates a framework of minimum cybersecurity standards for Companies and organizations identified as either operators of essential services (OES) or Competent Authorities (CAs). These would cover any private businesses or public entities with an important role to provide security in healthcare, transport, energy, banking and

[95] Gabel & Hickman, *supra* note 42 at 2.
[96] Stapp, *supra* note 80; Forbes, *supra* note 94.

financial market infrastructure, digital infrastructure, and water supply.[97]

Some estimates on GDPR cost implementation state that the amount larger multinational companies are having to spend has increased several fold. Of course, these large companies can afford to absorb the cost. These companies have IT departments and marketing departments that are devoted to creating security systems and customer interactions that will be compliant with the new regulations. Though some have complained many largest corporations such as Google, Apple, Facebook, and Amazon have seemed to be able to innovate their own solutions to GDPR compliance.[98] Facebook launched a series of tools.[99]

But what about smaller companies? Smaller companies are not exempt from GDPR. Unlike larger companies, they are less likely to have the resources to commit to sophisticated data security measures and there are many articles discussing the great burden GDPR regulation will place on smaller companies. Much of these articles seem to be at best anecdotal and little information could be found on post GDPR data, with most information available focusing on pre-GDPR speculation. Logic would seem to indicate that smaller companies are doing far less data collection and processing. They may be more likely to be mostly collecting, storing, and processing the data of their own customers. Alternatively, they may be less likely to have the capacity to do their own data collection, storage, and

[97] Gabel & Hickman, *supra* note 42 at 2.
[98] Wessling, *supra* note 82; Forbes Technology Council, *supra* note 94.
[99] Alex Hern, *Facebook Announces Privacy Tools to 'Put People in More Control' of Data*, THEGUARDIAN.COM (Mar. 28, 2018), https://www.theguardian.com/technology/2018/mar/28/facebook-privacy-tools-put-people-control-data.

> processing. In fact, we see many larger service providers that cater to small start-ups and small businesses to simply incorporate GDPR compliance into their platform services. For example, email database platforms, like MailChimp and Constant Contact, have adapted to create GDPR compliance for their customers, most of which are smaller companies that cannot afford to have their email databases managed internally. [100]
>
> Understandably, many have speculated that these regulations may increase costs for small companies and in turn raise barriers to entry in certain markets. [101] However, ethically speaking, does that mean that smaller companies should be allowed to collect personal data from private citizens without disclosure to or minimum protections for those citizens? In fact, if we were to use the medical field as an example, where data privacy has long been protected, smaller providers have not been allowed to mishandle the personal private health information of patients just because they were small providers. Similarly, small banking institutions are not exempt from regulations regarding the privacy of the financial information of their clients. In those circumstances, it would make sense that if a facility or organization does not have the ability and resources to safeguard and protect personal healthcare related information then they should not be handling it. Yet, interestingly, many seem to be arguing that online businesses and organizations

[100] Scott, *New Mailchimp Tools to Help with the GDPR*, MAILCHIMP.COM (Mar. 6, 2018), https://mailchimp.com/resources/gdpr-tools-from-mailchimp/; Andy Hutchinson, *GDPR: What You Need to Know and How Constant Contact Helps You Comply*, BLOGS.CONSTANTCONTACT.COM (Apr. 27, 2018), https://blogs.constantcontact.com/gdpr-how-to-comply/.

[101] Geoffrey Manne & Ben Sperry, *Debunking the Myth of a Data Barrier to Entry for Online Services*, TRUTHONTHEMARKET.COM (Mar. 26, 2015), https://truthonthemarket.com/2015/03/26/debunking-the-myth-of-a-data-barrier-to-entry-for-online-services/.

should be held to lesser standards based on the size of the organization. Last but not least, if data privacy regulations were to not be applicable to smaller businesses then this may in fact create an exploitable loophole. Where, as long as a company remains "small" it can collect, store, and process personal data with abandon at a low cost and then simply sell that information to a larger corporation. This allows large corporations to skirt regulations altogether.

This naturally leads to the question of whether this loss of innovation due to an increase in barriers to entry and the general burden upon smaller companies is of such high value to society that we are willing to allow those companies to play roulette with the information and data belonging to private citizens.[102] When considering this question, it is important to note how little recourse a private citizen would have against personal data abuse and theft without any regulation. Such private citizens may suffer from significant financial loss from the breach of their financial information. They may suffer significant emotional and reputational loss from personal information breaches. When you consider the amount of damage that can be done to an individual's life and compare it to the resources available to them as opposed to the resources available to even a small start-up company, it changes the metrics of the argument. Especially since without any regulations, the small company would not be responsible or liable for the breaches of such information and, therefore, would have little incentive to put in adequate measures to protect it. The recent history of data breaches discussed above in the introduction are just the tip of the iceberg of

[102] *Id.*

what can happen in a regulation-free market for personal information. [103]

Last but not least, these companies small or large are capitalizing and profiting on the data they are collecting from individuals, who are the original owners of their own personal data. In essence, creating a situation where the cost of obtaining personal data of individuals is a negative externality for businesses. Supporting the argument that smaller businesses should not be exempt from data regulations is the fact that they are capitalizing on data collection. Not only are they capitalizing on data collection, but they are doing so without paying the individuals from whom they are collecting said valuable data from in order to make a profit. Individuals are giving their valuable information to companies for free without any compensation for those companies to profit from. Thus, arguments that such companies are victims of data regulation seem disingenuous.[104]

C. *Opt-in or Opt-out fatigue and poor customer service*. Is there a real danger that since GDPR requires individuals to opt-in whenever their data is being collected that the public will start to get opt-in fatigue? This "opt-in fatigue" argument that individuals will simply favor sites where they do not

[103] *Supra*, note *7-13*.

[104] Natasha Lomas, *Europe is Drawing Fresh Battle Line Around the Ethics of Big Data*, TECHCRUNCH.COM (Oct. 3, 2018), https://techcrunch.com https://techcrunch.com/2015/10/13/whats-the-value-of-your-data//2018/10/03/europe-is-drawing-fresh-battle-lines-around-the-ethics-of-big-data/; Stephen Ritter, *the Ethical Data Dilemma: Why Ethics Will Separate Data Privacy Leaders From Followers*, FORBES.COM (Mar. 31, 2020), https://www.forbes.com/sites/forbestechcouncil/2020/03/31/the-ethical-data-dilemma-why-ethics-will-separate-data-privacy-leaders-from-followers/?sh=c4edfbd14c6a; Peter K. Yu, *The Political Economy of Data Protection*, 84 CHI.-KENT L. REV. 777, 777-801 (2010); Pauline Glikman & Nicolas Glady, *What's the Value of Your Data*, TECHCRUNCH.COM (Oct. 13, 2015), https://techcrunch.com/2015/10/13/whats-the-value-of-your-data/.

have to opt-in may not be relevant at all if all sites adopt GDPR complaint opt-in provisions and that certainly seems to be the trend. On the other hand, there may be a real danger that individuals become so used to opting-in that it becomes routine and, therefore, their opting-in begins to look a lot less like informed consent to data collection.[105] It remains to be seen if that will in fact happen. The opposite may be true in that individuals may be more aware of who is collecting their data, and who they are granting access to. When individuals are more aware they will likely also become for discerning. This more discerning public may start opting-out of sharing their data, and if they do, online businesses will have to adapt to the fact that consumers are no longer willing to turn over their data for free. In fact, recently many have argued that individuals ought to be able to benefit from the commoditization of their own data by getting compensated for opting-in. After all, the businesses that are collecting the data are capitalizing and profiting from the data that belongs to the data subjects. At a minimum, GDPR gives consumers the option of not allowing businesses to collect any more data than necessary to get the product or service they desire and, thus, limited the extent to which businesses can extort additional information out of consumers.[106]

D. *Roadblock to blockchain technology*. Blockchain technology allows for the creation of an immutable history of any changes in a document. However, because it is immutable any data that is collected as

[105] *Supra*, note 82.

[106] Rita Heimes, *How opt-in consent really works*, IAPP.ORG (Feb. 22, 2019), https://iapp.org/news/a/yes-how-opt-in-consent-really-works/; Michael Fimin, *Five Benefits GDPR Compliance Will Bring To Your Business*, FORBES.COM (Mar. 29, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/03/29/five-benefits-gdpr-compliance-will-bring-to-your-business/?sh=538ffb62482f.

part of the history of this document cannot by the very nature of blockchain be deleted. This means that data stored using blockchain would not be GDPR compliant because the data subject's right to be forgotten would be infringed.[107] This is a topic that merits further exploration. For example, the use of encryption and pseudonymization of personal data before it the implementation of blockchain could potentially allow for its use without infringing upon the data subject's rights. This is an interesting topic because GDPR is both a data security and privacy-based regulation and blockchain is often touted as an incredible technology for securely storing data and information. This is one area that will undoubtedly be one to watch as these regulations continue to be applied to real situations.

E. *Less privacy*. This argument is based on the idea the privacy is different from protection. These regulations are aimed towards increasing protection and security of data storage and processing, but that does not mean that we are increasing privacy. Arguably, the regulation requires more paperwork and more tracking of data, which could in fact decrease privacy. Practically speaking, there is also a question of how much control it really gives individuals over their data. GDPR does give the right to portability, the right to be forgotten, and the right to know what information is being collected. [108]

[107] *Supra*, note 82.

[108] Rick Robinson, *Data Privacy vs. Data Protection*, BLOG.IPSWITCH.COM (Jan. 30, 2020), https://blog.ipswitch.com/data-privacy-vs-data-protection; Mindaugas Kiskis, *GDPR is Eroding our Privacy, Not Protecting It*, THENEXTWEB.COM (Aug. 18, 2018), https://thenextweb.com/contributors/2018/08/05/gdpr-privacy-eroding-bad/; Forbes Technology Council, *Data Privacy V. Data Protection: Understanding The Distinction in Defending Your Data*, FORBES.COM (Dec. 19, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/12/19/data-privacy-vs-data-protection-understanding-the-distinction-in-defending-your-data/?sh=2e5799a950c9; Dave Weinstein, *Privacy vs. Security: It's a False*

> However, in terms of enforcement of these rights, the cost and expense of litigation still makes recourse for individuals expensive and inefficient. At the heart of the issue, data privacy matters are still David and Goliath type issues where individuals would find it difficult to ensure against abuse of their information. These laws also may not have real long-term consequences for preventing unscrupulous individuals from hacking into data files and/or misusing data. For that, technological innovation would be a far more efficient solution. So, far however the market has not really produced a technology that would allow individuals to secure their data online.[109]

**United States of America (US) California Consumer Privacy Act:**

Unlike the European Unions' GDPR the United States has no real national or federal comprehensive data privacy specific regulation that deals particularly with issues of data collection, storage, and processing. Such regulations have been enacted primarily at the state level with CCPA being the most thorough and comprehensive. Instead, national data regulation is segmented into several different acts under several different agencies like the Federal Trade Commission (FTC), Securities and Exchange Commission (SEC), and the Federal Bureau of Investigation (FBI). In terms of online data collection, storage, processing, and privacy outside of the arena of healthcare and financial services detailed specific regulation have been at the State level. Each state has a data breach regulation requiring organizations to notify individuals if their information has

*Diemma*, WSJ.COM (Oct. 6, 2018), https://www.wsj.com/articles/privacy-vs-security-its-a-false-dilemma-11570389477.

[109] *Id.*

been breached in a timely manner or be subject to penalty.[110] However, many states are considering implementing GDPR style data privacy regulations. Most notably, California is leading the way with its new regulation AB 375, the California Consumer Privacy Act of 2018 ("CCPA"). This regulation took full effect in January of 2020. It is currently the closest U.S regulation to GDPR. To understand the regulation more fully we will look at the jurisdiction and scope that it covers, the subject matter it regulates, the liabilities it creates, how it is predicted to be enforced, the central provisions, and some both observable and some predicted trends.

1. *Subject Matter and Jurisdiction.* Similar to GDPR the CCPA looks to apply to the collection, storage, processing, and/or sale of data belonging to natural persons who are residents of California.[111] Unlike GDPR, there does not seem to be a requirement of marketing specifically to California residents in order for the Act to apply. However, like the drafters of GDPR, it seems as though the drafters of CCPA intentionally excluded data not from a natural person.[112] As discussed earlier, this makes sense because such data would normally fall under other regulations such as Intellectual Property Rights and trade secrets.

   Also, like GDPR, CCPA establishes certain rights of natural persons, who are CA residents including, but limited to (1) the right to opt-out of data collection just like under

[110] Pam Greenberg, *Trends in State Cybersecurity Law & Legislation*, NCSL.ORG (2016), https://www.ncsl.org/documents/taskforces/StateCybersecurityLawsLegis.pdf; Mitchell Noordyke, *US State Comprehensive Privacy Law Comparison*, THE INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS (IAPP) (Apr. 18, 2019), https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/; Jenni Bergal, *Every State Now Has a Data Breach Notification Law*, GOVERNING.COM (Apr. 3, 2018), https://www.governing.com/topics/mgmt/sl-alabama-data-breach-notification.html.

[111] CCPA, §1798.135(g), § 1798.140(e).

[112] *Id*.; GDPR, art. 1-3.

GDPR[113], (2) the right to opt-out of the sale of personal data, which is similar to the GDPR right to prevent others from profiting from data,[114] (3) the right to know, which is similar to the GDPR right to access and the GDPR right to know,[115] and (4) the right to be forgotten.[116] In contrast to GDPR, CCPA also includes a right to non-discrimination.[117] This right is similar to the concept in GDPR, which does not allow businesses to require data sale and collection not necessary to the service they are providing. [118] This particular provision of CCPA is fairly detailed regarding the types of discrimination that businesses may not engage in. The Act seems to go out of its way to ensure that businesses will not require consumers to share any more than the minimum amount of information necessary to conduct business with that consumer without the consumer's consent.[119]

Now that we understand the rights that the statute sets out, we should ask who will be governed and regulated by the statute? CCPA limits its scope to specific businesses and not just any CA business or any business transacting business with a CA resident. In order for a business to be governed by the statute it must also meet one of the following criteria: (1) get 50% or more of its revenues from the sale of consumer personal data, (2) have gross adjusted sales of $25 million or more, or (3) buys, sells, shares, receives, collects or does some sort of combination of buying, selling, sharing, receiving and collecting personal information of 50,000 or more consumers, households or devises annually.[120] In order to prevent companies from creatively structuring themselves out from being required to comply with CCPA and still

[113] CCPA, §1798.120.
[114] *Id*.; CCPA, §1798.115(d)
[115] CCPA, §1798.100, §1798.110
[116] CCPA, §1798.105
[117] CCPA, §1798.125
[118] GDPR, art. 5.
[119] CCPA, §1798.125
[120] CCPA, §1798.140(c)(1)

collect data from California residents, the act includes businesses that share common branding with a business that meet one of the three above started criteria or any business that controls or is controlled by a business that meets one of the three CCPA criteria.[121] The act also does not apply to government agencies and non-profits.[122] The effect of this is to provide an exception for small businesses and non-profits as well as the security and safety exceptions. This narrows the scope of this regulation dramatically from the scope of GDPR in terms of the businesses it applies to.

Unlike GDPR, CCPA does not seem to require customization of the site targeting California residents or marketing, branding, or advertising targeting California residents in order for CCPA to apply.[123] It does also state that if the required disclosures under the Act regarding data collection, sale, use, and consumer rights are in a California resident specific section of a website that the business must design the website such that any potential California resident will be directed to those pages and provision before sharing their data.[124]

Data collection under CCPA is defined broadly to include "buying, renting, gathering, obtaining, receiving, or accessing any personal information pertaining to a consumer by any means. This includes receiving information from the consumer, either actively or passively, or by observing the consumer's behavior."[125] Interestingly, this broad definition is not limited to automated forms of data collection which is in contrast to that of GDPR, which makes a point of directly targeting certain means of data collection by stating, "the processing of personal data wholly or partly by automated means and to the processing other than by automated means

[121] CCPA, §1798.140(c)(2)
[122] CCPA, § 1798.145(n)(1)
[123] Gabel & Hickman, *supra* note 42 at 1.
[124] CCPA, §1798.130(a)(5), §1798.135(a)(2)(B), §1798.135(b).
[125] CCPA, §1798.140(e)

of personal data which form part of a filing system or are intended to form part of a filing system."[126]

Of particular note is the non-regulation of de-identified data. The CCPA defines such data as data that could not possibly be associated with in any way either directly or indirectly to a particular consumer where a business has done the following: used technical safeguards preventing reidentification of the consumer, used a business process prohibiting reidentification, used a process preventing inadvertent release of said data and never attempted reidentification. [127] Deidentification is often more commonly referred to data anonymization. This allows for the collection of and use of consumer data, without the data being used for specifically targeting those consumers individually with their own data. For example, if a company collects data on your purchases and uses it to target advertising of related products back to you specifically. It would allow the company to track consumer trends, likes, dislikes, and other patterns amongst groups of consumers.[128] For example, consumers that buy a certain product or service are more likely to be vegetarian, or are more likely to be politically conservative, or more likely to like to color orange. This indicates the drafters were more concerned with drafting a personal data rights protection bill similar to GDPR. Neither bill is aimed at protecting consumers as a class, rather just consumers as individuals.

2. *Liabilities.* The CCPA provides that individuals may recover damages for any breaches of their unencrypted and nonredacted consumer information if breached by an unauthorized person or entity. Each such individual covered by the act (natural persons, who are California residents) may be entitled to damages in the amount equal the greater

[126] GDPR, art. 2(1).
[127] CCPA, §1789.140(h), (k)(3), §1789.145(a)(5), §1789.148.
[128] Jake Frankenfield, *Data Anonymization*, INVESTOPEDIA.COM (Dec. 5, 2020), https://www.investopedia.com/terms/d/data-anonymization.asp.

of one hundred dollars ($100.00) to seven hundred and fifty dollars ($750.00) per incident or actual damages. [129] Additionally, businesses may be subject to civil suits brought by the California Attorney General's office in the name of the State of California for any violations of the CCPA. Businesses will have 30 days from notice of noncompliance to cure violations if they can otherwise, they may be subject to civil penalties that can range from $2,500 for a non-intentional violation to $7,500 for an intentional violation.[130] These penalties appear to be far less than the penalties under GDPR.[131] Of course, GDPR governs and protects the rights of all EU citizens as opposed to CCPA, which just covers California residents. This might explain the disparity in the ranges of liabilities under their rules.

3. *Enforcement.* To examine CCPA's implementation we can look at the major cases that are currently pending under the statute. In comparison to GDPR CCPA is relatively new and much of its short life has been shadowed by the COVID-19 pandemic, which has dramatically slowed courts, litigation, and civil enforcement cases. Some of the most noteworthy current pending cases include:

    A. *Cullen v. Zoom Video Communications, Inc.,* Case No. 5:20-cv-02155 (N.D. Cal.) This case is still pending. The central issues are whether Zoom's data-sharing policies violated the CCPA's "adequate notice" requirement by collecting and using the personal data of users without implementing and maintaining reasonable security procedures as required by the statute. Additionally, the plaintiff's alleged that Zoom committed fraud in violation of California's Unfair Competition Law, by collecting

[129] CCPA, §1798.150.
[130] CCPA, §1798.155.
[131] GDPR, art. 83.

personal information and misrepresenting its privacy capabilities. [132]

B. *I.C., a minor by and through his natural parent, Nasim Chaudhri and Amy Gitre v. Zynga, Inc.,* Case No. 3:20-cv-01539 (N.D. Cal.); *Carol Johnson and Lisa Thomas v. Zynga, Inc.*, Case No. 3:20-cv-02024 (N.D. Cal.). Plaintiffs in this case claimed that video game company Zynga, Inc. failed to adequately protect the personally identifiable information of its users. This suit was specifically instigated by the fact that Zynga, Inc. was hacked and the personally identifiable information of over 218 million were compromised. Among various claims for fraud and misrepresentation are also claims for violating FTC regulations and state regulations regarding protection of personally identifiable information including the CCPA.[133]

C. *Barnes v. Hanna Andersson LLC and Salesforce.com Inc.,* Case No. 4:20-cv-00812 (N.D. Cal.). This lawsuit stemmed from a data breach that included unencrypted credit card and consumer information of customers. Plaintiffs sued both Hanna Anderson LLC and Salesforce.com. Though the lawsuit references CCPA, the plaintiffs in the case are actually suing under California's Unfair

[132] *Cullen v. Zoom Video Communs., Inc.*, No. 20-CV-02155-LHK, 2020 U.S. Dist. LEXIS 78745 (N.D. Cal. Apr. 24, 2020); Alysa Zeltzer Hutnik et al., *CCPA Litigation Round-Up*, AD LAW ACCESS (Apr. 7, 2020), https://www.adlawaccess.com/2020/04/articles/private-litigants-have-already-started-to-file-direct-claims-under-the-ccpa/; Cathy Cosgrove, *CCPA Litigation: Shaping the Contours of the Private Right of Action*, IAPP.ORG (June 8, 2020), https://iapp.org/news/a/ccpa-litigation-shaping-the-contours-of-the-private-right-of-action/.

[133] *I.C. v. Zynga Inc*., No. 20-cv-01539-YGR, 2021 U.S. Dist. LEXIS 2227 (N.D. Cal. Jan. 6, 2021); Hutnik et al., *supra* note 132.

Competition Law, Cal. Bus. & Prof. Code §17200 ("UCL") and for negligence.[134]

D. *Sheth v. Ring LLC*, Case No. 2:20-cv-01538 (C.D. Cal.). In this case plaintiff's alleged Ring Security doorbell company made unauthorized disclosers of personally identifiable information to third parties and also failed to adequately protect customer personal information. Additionally, plaintiffs allege that personal data was collected without authorization. These claims did not spring out of any specific data breach event. Alongside claims under CCPA, there are claims of negligence, breach of warranty, and various other state statutes.[135]

E. *Burke v. Clearview AI, Inc.*, Case No. 3:20-cv-00370 (S.D. Cal.). In this case, the plaintiffs allege that Clearview AI, Inc. improperly collected and sold personally identifiable information including biometric data the company scrapes the internet for images and information. Then it sells that information to law enforcement agencies. Scraping is a process of using bots to extract content and data from a website. Plaintiffs allege that in this process the defendants collect personal identifiable information in their database. The plaintiffs also claim that this type of collection and sale of their personally identifiable data was unauthorized and therefore in violation of CCPA.[136]

4. *Central Provisions.* So far CCPA's central provisions in terms of enforcement are once focusing on notice, permission, and reasonable protection. There also does not

[134] *Barnes v. Hanna Andersson LLC and Salesforce.com Inc.*, Case No. 4:20-cv-00812 (N.D. Cal.); Hutnik et al., *supra* note 132; Cosgrove, *supra* note 132.
[135] *Sheth v. Ring LLC*, Case No. 2:20-cv-01538 (C.D. Cal.); Hutnik et al., *supra* note 132; Cosgrove, *supra* note 132.
[136] *Burke v. Clearview AI, Inc.*, Case No. 3:20-cv-00370 (S.D. Cal.); Hutnik et al., *supra* note 132; Cosgrove, *supra* note 132.

seem to be a need for an actual data breach for the creation of a claim just as under GDPR.

A. Notice to consumers regarding what information is collected, the purpose for collection, and how it will be used:

Section 1798.100(b) places a requirement on businesses covered by CCPA to provide notice to consumers prior to collection of personal information and data. The section also states that this notice should disclose the purposes of the data collection and the manner in which it will be used.[137] The definitions portion under CCPA Section 1798.140 provides some specific examples such as sharing information with a service provider that would require disclosure under Section 1798.100.[138] It also states the obligations of the business when information is subject to a sale or merger consumer personal information is subject to different use and purpose.[139]

Section 1798.120(b) then goes further than 1798.100 by explicitly requiring that notice be given for the sale of customer information to third parties.[140] Additionally, Section 1798.115(d) then expounds upon this by stating that if that information is sold to a third party not only would the sale of that information have to be disclosed under Section 1798.100(b), but if that third party wanted to sell that data to yet another party such sale would also have to be explicitly disclosed to the consumer prior to sale and then that said consumer would have to be

[137] CCPA, §1798.100(b).
[138] CCPA, §1798.140, §1798.100.
[139] CCPA, §1798.140(t)(2)(D).
[140] CCPA, §1798.120(b).

given the opportunity to opt-out prior to the third party selling the information.[141]

Moreover, Section 1798.185 (6) of the CCPA stresses the importance of notices to consumers being "provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities and are available in the language primarily used to interact with the consumer."[142]

B. The requirement to obtain prior permission from consumers to collect, use or store their personal data is often referred to as the right to opt-out. Under the CCPA we see the spirit of this right protected by way of a prohibition in Section 1798.120 (D) which states that if a business fails to receive consent from a consumer then the sale of that consumer's information is expressly prohibited. [143] Other sections, such as 1798.120 (6) and Section 1798.125(b)(3), provide exceptions for not deleting data in certain circumstances and for entering into a financial incentive program with a consumer provided that the consumers have consented. [144] Similar to the requirement to provide notice, the right to opt-out is also referenced several times within the definitions portions under Section 1798.140 CCPA.[145]

More than just getting permission businesses must offer the right to opt-out under Section 1798.120, which also states that in the case of minors this is actually the right to opt-in. [146]

[141] CCPA, §1798.115(d).
[142] CCPA, §1798.185(6).
[143] CCPA, §1798.120(D)
[144] CCPA, §1798.120(6), §1798.125(b)(3).
[145] CCPA, §1798.140.
[146] CCPA, §1798.120.

> Section 1798.135 further elaborates the exact manner in which businesses must make these rights obvious, clearly and easily accessible, and easy to understand. [147] Similarly, Section 1798.185, demonstrates the importance of this right being "provided in a manner that may be easily understood by the average consumer, are accessible to consumers with disabilities, and are available in the language primarily used to interact with the consumer."[148]
>
> Additionally, section 1798.192 strengthens these provisions by stating that these rights to opt-out cannot be contractually waived. [149]

C. Duty of reasonable protection and limits to damages: Perhaps the most central provision for understanding the duty to reasonably protect data is Section 1798.150. This section states that any actual breach, "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information," [150] creates a cause of action under which the consumer or consumers affected may sue for damages. The damages are however limited to $750 per incident unless the consumer or consumers can prove actual damages.[151] From a practical point of view quantifying actual damages would typically be difficult to prove. Thus, the $750 per incident fine makes it financially impractical for any individual consumer to bring a lawsuit. This is undoubtedly why most of the CCPA cases so far are being

[147] CCPA, §1798.135.
[148] CCPA, §1798.185.
[149] CCPA, §1798.192.
[150] CCPA, §1798.150
[151] *Id*.

approached as class actions. The statute does also allow for injunctive and declaratory relief. It is unclear what types of damages a consumer would be entitled to for failures to disclose or failure to provide an opt-out/opt-in. This will be clearer once some of the cases actually start working their way up the court system.

Section 1798.155. does provide "a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation."[152] However, this fine would go to the Consumer Privacy Fund to help offset the costs of the Attorney General for participating in these cases. It would not go to the consumer or consumers to compensate them for damages they may have suffered as an individual.[153]

5. *Implementation/Trends.* Many of the same arguments against GDPR could also be levied against CCPA: (A) there is no need for regulation, (B) high cost of implementation creating market stagnation, barriers to entry, loss of innovation, and relatedly loss of jobs; (C) opt-in fatigue and poor customer service; (D) roadblock to blockchain technology; and (E) less privacy. As the two statutes are so similar the arguments to debunk these concerns are also the same here as they were for GDPR. Interestingly, because GDPR was already in force at the time CCPA came into effect, much of the fear and opposition vocalized prior to GDPR was not as pronounced with CCPA.

CCPA is still in its very nascent stages of enforcement. So, far we can see that CCPA is almost never used as the sole claim. This may be in part for two reasons. The first reason being that CCPA does not allow for large damages. This

[152] CCPA, §1798.155.
[153] *Id*.

> necessitates the creation of larger classes in order for the amounts to be worthwhile, which of course is a more costly type of litigation. When we couple this with the second reason, which is that CCPA is still unproven in the course, this means that plaintiffs are wise to include other claims for more easily and tried and true causes of action. So far, we see FTC regulations, fraud, and California's Unfair Competition laws to be the ones that are coupled with CCPA claims. We will have to wait to see how these cases play out in order to really know what the future trends for CCPA might be.[154] In the meantime, many other states have proposed similar regulations to CCPA, and it would not be surprising to see that sometime in the future each state will have its own version of a data privacy act.

**Data Privacy Specific Regulations at the Federal Level:**

There are a few data privacy regulations at the federal level. However, unlike GDPR, most are industry-specific and do not serve the same function of regulating internet commerce, the internet of things, or organizations collecting data that are outside of healthcare and finance. These regulations would include HIPAA (Health Insurance Portability and Accountability Act of 1996), FCRA (Fair Credit Reporting Act of 1970), RFPA (Right to Financial Privacy Act of 1978), GLBA (Gramm–Leach–Bliley Act, also known as the Financial Services Modernization Act of 1999), EFTA (Electronic Funds Transfer Act of 1978) and FINRA (Financial Industry Regulatory Authority).

Outside of these regulations, there are national security regulations aimed at protecting sensitive government information from getting into the wrong hands and posing a threat to national security as well as federal law enforcement agencies focused on fighting criminal activity online. These regulations are not intended to regulate normal personal data transactions online. Unlike data privacy laws that regulate entities collecting, storing, and processing data these

[154] Hutnik et al., *supra* note 132; Cosgrove, *supra* note 132.

agencies and regulations are aimed at catching and prosecuting hackers, terrorists, spies, and criminals. This would include regulations and agencies such as ECPA (Electronic Communications Privacy Act of 1986), SCA (Computer Security Act of 1987), USA PATRIOT Act (Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001), CISA (Cybersecurity and Infrastructure Security Agency Act of 2018), HSA (Homeland Security Act of 2002), FIMSA (Federal Information Security Management Act of 2002), The Federal Bureau of Investigation's National Cyber Investigative Joint Task Force (NCIJTF), and other similar acts and programs.

It is necessary to look outside of these types of regulations to truly understand how ordinary legal data collection, storage, processing, and privacy is regulated at the national level in the U.S. in the absence of a federal data privacy act.

**Data privacy rules outside of GDPR, CCPA, and other Data Privacy Specific Regulations:**

While it is true that CCPA is the closest to a GDPR like regulation that we have here in the U.S. it is no surprise that most of the CCPA lawsuits we looked at above are coupled with claims under the Federal Trade Commission Act (FTC Act). Prior to these types of state data privacy regulations, U.S. consumers would have relied on FTC Act claims for remedies. In particular, Section 5 of the FTC Act, which regulates unfair or deceptive acts or practices in interstate commerce, and ironically is not a specific data privacy or data security regulation.[155] Most states do have data privacy rules and regulations, but few are as robust as the CCPA, with most only have data breach notification requirements. [156] In those states,

[155] FTC Act, § 45.

[156] *Cybersecurity Legislation 2019*, National Conference of State Legislatures, https://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx (last visited July 21, 2019); Hardeep Singh, *A Glance At The United States Cyber Security Laws*,

Section 5 of the FTC Act and state laws governing fraud or deceptive practices or breach of fiduciary duty are the best sources for causes of action against abuse of user data. Arguably, the FTC's regulation in this area has been more impactful than other data privacy regulations. Since the FTC comes into play with interstate commerce and since most internet or web-based commerce and communication is interstate, the FTC has been in large part the major and only federal level player in this space. Therefore, it would be meritorious to look at Section 5 of the FTC Act and related regulations under the FTC Act.

1. *Subject Matter and Jurisdiction.* Subject matter and jurisdiction are fairly simple and clear. The act governs any unfair or deceptive acts or practices in interstate commerce. The only requirement being that it involves one or more parties from different states.[157] Since most companies collecting consumer data online would be operating in more than one state, this statute applies to many more organizations and businesses than CCPA and arguably GDPR. Also, since this statute was not drafted or designed solely with online data collection in mind, this act would in fact apply to any unfair or deceptive act or practice even if it did not involve the internet at all.

2. *Liabilities.* On February 14, 2019, the maximum civil penalty amount under this regulation increased from $41,484 to $42,530 for violations of Sections 5(l), 5(m)(l)(A) and 5(m)(l)(B) of the FTC Act per incident.[158] Penalties of course can be much higher, such as the FTC imposing a $5 billion penalty against Facebook for violating its 2012 order where the company had been warned about deceiving

APPKNOX.COM (Jan. 27, 2016), https://www.appknox.com/blog/united-states-cyber-security-laws; Bergal, *supra* note 110.

[157] FTC Act, § 45.

[158] Federal Trade Commission, *FTC Publishes Inflation-Adjusted Civil Penalty Amounts*, FTC.GOV (Mar. 1, 2019), https://www.ftc.gov/news-events/press-releases/2019/03/ftc-publishes-inflation-adjusted-civil-penalty-amounts.

customers about the degree of privacy settings on the platform which allowed users to control the privacy of their personal information.[159] This fine was related to recent FTC investigations that most famously stemmed from Facebook's interactions with allowing British political consulting firm Cambridge Analytica to have access to user information during the 2016 U.S. presidential election. These investigations have resulted in a separate lawsuit filed by the FTC against Cambridge Analytica and in the settlement of claims against their app developer Aleksandr Kogan and former Cambridge Analytica CEO Alexander Nix.[160] The $5 billion fine against Facebook for violation of the FTC's 2012 order was the largest one in history at least so far.[161] Results of the case against Cambridge Analytica itself remain to be seen as the company has filed for bankruptcy.

3. *Enforcement.* As of 2018, FTC has brought more than 65 cases regarding Data Security and Identity theft and more than 25 cases for violations of the Children's Online Privacy

[159] Federal Trade Commission, *FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook- FTC settlement Imposes Historic Penalty, and Significant Requirements to Boost Accountability and Transparency*, FTC.GOV (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

[160] Federal Trade Commission, *FTC Sues Cambridge Analytica, Settles with Former CEO and App Developer- FTC alleges they deceived Facebook users about data collection*, FTC.GOV, (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-sues-cambridge-analytica-settles-former-ceo-app-developer; Federal Trade Commission, *FTC Issues Opinion and Order Against Cambridge Analytica For Deceiving Consumers About the Collection of Facebook Data, Compliance with EU-U.S. Privacy Shield*, FTC.GOV (Dec. 6, 2019), https://www.ftc.gov/news-events/press-releases/2019/12/ftc-issues-opinion-order-against-cambridge-analytica-deceiving.

[161] Federal Trade Commission, *supra* note 159; Somini Sengupta, *F.T.C. Settles Privacy Issue at Facebook*, NYTIMES.COM (Nov. 29, 2011), https://www.nytimes.com/2011/11/30/technology/facebook-agrees-to-ftc-settlement-on-privacy.html.

Protection Act (COPPA).[162] The agency seemingly is bringing more and more resources towards crimes involving data security as it has determined these types of crimes to be directly part of the agency's mandate.[163] Particularly in the absence of specific federal legislation in the area. This section will take a moment to examine a few of the more pivotal cases involving data security and FTC regulations.

A. *FTC v. Wyndham Worldwide Corp. 799 F.3d 236 (3d Cir. 2015).* While the FTC has been in the data cybersecurity space since 2005 it wasn't until Wyndham that its authority to regulate in the area under 15 U.S.C. § 45 was challenged in a court. The case involved Wyndham Worldwide Corp., a company in the hotel and hospitality industry that between 2008 and 2009 had been hacked three times. Over the course of these hacks, 619,000 accounts containing unencrypted information were compromised resulting in approximately $10.6 million in fraud damages. Even after the first attack, Wyndham failed to use any firewalls, any encryption techniques, or place any restrictions on certain IP addresses. Wyndham brought 4 separate arguments challenging the authority of the FTC to bring any actions against them. (1) the FTC lacked authority, (2) the FTC's Section 45(a)(1)'s "unfairness" prong did not include unreasonable data security measures, (3) the FTC had not given sufficient notice of how data security measures could be deemed an unfair trade practice, and (4) the FTC consumer injury claims were inadequate. All of the defendant's arguments were upheld by the trial court. Of these four, two were considered by the 3rd Circuit Court of Appeals. First, that the FTC lacked authority under

[162] Federal Trade Commission, *2018 Privacy and Data Security Update*, FTC.GOV (2018), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.
[163] Denny, *supra* note 20.

the unfairness prong of § 45(a) to regulate issues of data security. Second, did Wyndham have fair notice that specific data security practices, or lack thereof, would be in violation of the unfairness provision. The 3rd Circuit found in favor of the FTC on both arguments.[164] One central point on this issue of notice was that there had been many previous settlements with private companies and the FTC for data security violations under this prong of Section 45 already, and also that the FTC had published a Guidebook about cybersecurity and data privacy matters.[165] Perhaps one of the most important takeaways from Wyndham is the flexibility that the FTC was granted. By the court not insisting on specific rules and guidance the FTC can adapt to the everchanging landscape of cybersecurity without being pinned down to standards that would be quickly outdated. In the absence of other federal cybersecurity regulations, such flexibility allows the FTC the bandwidth necessary to be somewhat effective in protecting consumer information and privacy.[166]

B. *Spokeo, Inc. v. Robins, 578 U.S. ___ (2016).* In *Spokeo*, the Supreme Court addressed issues of standing for violations of the Fair and Accurate Credit Transaction Act (FACTA), as well as Fair Credit Reporting Act (FCRA). The court held that

[164] *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015); Denny, *supra* note 163; Lydia F. de la Torre, *FTC v. Whyndham: Authority to regulate cyber security under FTC Act*, MEDIUM.COM (May 19, 2019), https://medium.com/golden-data/case-study-ftc-v-whyndham-c838bd7f5bd8; *FTC v. Wyndham Worldwide Corp.: Third Circuit Finds FTC Has Authority to Regulate Data Security and Company Had Fair Notice of Potential Liability*, 129 Harv. L. Rev. 1120 (2016).

[165] Federal Trade Commission, *Protecting Personal Information: A Guide For Business*, FTC.GOV (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[166] *Supra* note 164.

for a plaintiff to prove they had standing under a current case or controversy, they must show injuries were both concrete and particularized. The Court also stated that intangible injuries such as to free exercise and free speech could meet these standards. The case was then remanded to the 9th circuit, which found that the statute was to prevent consumers from having false credit information about them being disseminated and that the dissemination of such false information provided the plaintiff with concrete and particularized injury sufficient for standing. While this case did not stem from 15 U.S.C. § 45, it did establish that plaintiff could have standing to bring claims under FTC statutes for the dissemination of their data. This in turn strengthened the FTC's ability to have standing to protect consumers whose data has been compromised by showing such dissemination of personal data is injury sufficient to have standing.[167]

C. *Facebook.* Changes to the way in which Facebook handled information in 2009 led to an FTC investigation culminating in the FTC reaching the conclusion that Facebook's practices violated the unfair and deceptive practices portions of 15 U.S.C. §45. The commission asserted the following were deceptive practices: Facebook (1) made public information that users had classified as private information, such as their friend's list, without getting the users consent or providing them with

[167] *Spokeo, Inc. v. Robins*, 578 U.S. ___ (2016); Denny, *supra* note 20; Jennifer M. Keas & Kathryn A. Shoemaker, *Supreme Court Will Not Look at Spokeo Again, Leaving Lower Courts to Grapple with Article III Uncertainties*, FOLEY.COM (Feb. 18, 2018), https://www.foley.com/en/insights/publications/2018/02/supreme-court-will-not-look-at-spokeo-again-leavin.

notice; (2) allowed third party Aps installed by users to access to all user personal information instead of limiting these APs to only the information they needed as platform's policies stated they would, (3) conveyed to users that they could restrict data sharing to specific groups, such as "friends only" when in fact that data was accessible to any third party Aps that said user's friends might install, (4) claimed to users they verified the security of Aps participating in their verified Aps program when they did not do so, (5) stated to users that their information would not be shared with advertisers and then shared user information anyway, (6) did not delete user information, photos, videos, etc. when users deleted their accounts even though the platform claimed that they did, and (7) stated that they conformed with the U.S.- EU Safe Harbor Framework when they did not.[168] In 2011 the FTC settled with Facebook. The settlement was then memorialized into a 2012 FTC order.[169]

The terms of this settlement included: (1) barring Facebook from making misrepresentations to users regarding the privacy and security of user information and data, requiring Facebook to obtain affirmative consent prior to changing or overriding privacy settings for users, (2) requiring Facebook to bar anyone from having access to any user information 30 days after the user has deleted their account, (3) a mandatory that Facebook must establish and maintain a comprehensive privacy

[168] Federal Trade Commission, *Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises*, FTC.GOV (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep; *In re Facebook, Inc.*, C-4365, 2012 FTC LEXIS 136 (F.T.C. July 27, 2012).
[169] *Id*.

> program which protects the privacy and confidentiality of consumers' information and addresses privacy risks associated with the development and management of new and existing products and services, and (4)
> stipulates that every two years for the next 20 years, Facebook must obtain third-party independent audits to certify its privacy program meets or exceeds the requirements of the FTC order, and ensures the privacy of consumers' information is being protected.[170]

With the 2016 election, new investigations were initiated to look into the relationship between Cambridge Analytica and Facebook as it became apparent the consulting company Cambridge Analytica was able to harvest the information of millions of Facebook users through the Facebook platform. FTC also stated that Facebook had failed to comply with the promises it made in the 2011 agreement (2012 order)[171].

Specifically, the FTC findings reported that Facebook violated the settlement order in the following ways: (1) Facebook misrepresented in their privacy policy that users would need to opt-in to enable facial recognition on their accounts, when in fact the "Tag Suggestions" feature, which uses facial recognition was automatically turned on for

[170] Federal Trade Commission, *FTC Gives Final Approval to Modify FTC's 2012 Privacy Order with Facebook with Provisions from 2019 Settlement*, FTC.GOV (Apr. 28, 2020), https://www.ftc.gov/news-events/press-releases/2020/04/ftc-gives-final-approval-modify-ftcs-2012-privacy-order-facebook; *United States v. Facebook, Inc.*, Civil Action No. 19-2184 (TJK) (D.D.C. Apr. 23, 2020), https://www.courthousenews.com/wp-content/uploads/2019/07/facebook-complaint.pdf.

[171] Federal Trade Commission, *supra* note 159.

tens of millions of users. (2) Facebook lied to users when they shared the data of users' friends with 3rd party apps, despite that those friends had in fact opted for more restrictive settings supposedly not authorizing the sharing of their information with 3rd parties. (3) In 2014, Facebook announced that it would stop allowing 3rd party developers to access information and collect data from friends of app users. However, they not only failed to mention that they were grandfathering-in existing developers allowing them access through April of 2015, but they also actually failed to stop allowing this data collection till after June 2018. (4) Facebook removed a disclosure under its privacy setting notifying users that their information could be shared with apps that their friends are using. This was 4 months after the 2012 order was issued despite that the information was still being shared. (5) That Facebook failed to notify users that they would be using their phone numbers for advertising when they asked users for phone numbers to initiate 2-factor authentication. (6) Facebook failed to adequately police 3rd party developers. Facebook did not screen developers prior to giving the access to vast amounts of user data, did not enforce its own administrative policies regarding violations, often based enforcement on financial benefits to Facebook for allowing developers to continue their relationship with Facebook, and only required developers to agree to terms and conditions at the time of registering their app with Facebook. Together with other actions, the FTC alleged this failed the requirement to maintain a reasonable privacy program. (7) Many of Facebook's "Privacy shortcut" programs failed to disclose that even the most restrictive settings would allow for sharing of information with 3rd party apps

> through their friends unless they additionally when to the "Apps Settings Page" and made the appropriate selections to opt-out of sharing. These violations of the 2011 settlement coupled with others are what led to the hefty fine.[172]
>
> Because Facebook violated the 2011 agreement the FTC was able to slap Facebook with a $5 billion fine. The largest FTC data security fine in history. While this amount might at first seem staggering it is important to note that Facebook made $55.8 billion in revenues in 2018 through just targeted advertising.[173]
>
> In addition to the monetary penalty, the FTC ordered Facebook to comply with a new 20-year settlement order, which covers WhatsApp and Instagram as well. This new order included the following far more detailed and restrictive requirements: (1) A requirement for Facebook to appoint compliance officers responsible for Facebook's privacy program. Officers will be approved by a new privacy committee. Once appointed and approved the officers will only be removed by the privacy committee and Facebook's CEO or employees will not have the authority to remove them. This is so their independence remains intact. The officers along with Facebook CEO, will submit to quarterly certifications to the FTC. These will certify Facebook's compliance with the privacy program mandate in the FTC order. An annual certification will be submitted for the entire company. False

[172] *Id.*

[173] *Id*.; Brad Kutner, *Facebook to Pay $5 Billion Penalty for Privacy Violations*, COURTHOUSENEWS.COM (July 24, 2019), https://www.courthousenews.com/ftc-fines-facebook-5-billion-for-privacy-violations/.

certification will subject the Officers and/or CEO to personal civil and criminal penalties. This is significant because we are seeing personal civil and criminal liability for data security measures of a large private company. (2) An expanded third-party assessor biennial assessment program. As part of the program, the third party must make this assessment to the new privacy committee and report to them on a quarterly basis. This assessment shall be based upon independent sampling, testing, and fact-gathering to test Facebook's privacy program and not on assertions or attestations by Facebook and its management. The FTC may approve or remove the assessor and the order specifically prohibits making misrepresentations of misstatements to the assessor. Additionally, the FTC's ability to enforce the order is beefed up hear by authorizing the FTC to use discovery methods under the Federal Rules of Civil procedure to monitor compliance. (3) A requirement that Facebook conduct a privacy review for every new practice, service, new product, or product change/modification. This review must be completed before implementation and the results and decisions regarding user privacy must be documented. (4) A mandate to document any incidents where the data of 500 users or more had their information or privacy compromised including what efforts Facebook has made to address the issue. This mandatory documentation must be delivered to the FTC within 30 days of the triggering incident coming to Facebook's attention. (5) Each quarter the designated compliance officers shall generate a privacy report to be shared with the independent accessor, the CEO, and upon request with the FTC. (6) A prohibition from advertising using telephone numbers provided by users to enable security

features like two-factor authentication, (7) A requirement to establish, use, and maintain a comprehensive data security program (8) An obligation to provide improved oversite of third-party apps which must include the elimination of app developers that fail to support their need for specific user data or that fail to certify compliance with the platform policies. (9) A requirement to provide clear notice to its use of facial recognition technology in a conspicuous way to users. (10) A mandate to routinely scan and detect if passwords are stored in plain text and to encrypt user passwords. (11) A requirement that any time use of user data exceeds its prior disclosure to users to obtain affirmative and express consent from users before doing so. (12) A prohibition against asking for or requiring passwords to services from users signing up for Facebook services.[174]

D. *YouTube.* In 2019, Google LLC and its subsidiary YouTube, LLC settled a case with the FTC regarding violations of the Children's Online Privacy Protection Act (COPPA). This case was initiated by New York Attorney general against YouTube for sharing information and data collected from minors without their parent's consent as COPPA requires all child-directed websites and online services to do. YouTube not only collected the data, but also used cookies to deliver targeted ads to these minors (children under 13), thereby making millions of dollars in advertising.[175] As part of the investigation,

[174] Federal Trade Commission, *supra* note 159.
[175] Federal Trade Commission, *Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law: FTC, New York Attorney General allege YouTube channels collected kids' personal information without parental consent*, FTC.GOV (Sept. 4, 2019), https://www.ftc.gov/news-

> it was revealed that YouTube executives knew that the content was directed towards minors. Among other pieces of evidence was proof that both Google and YouTube asserting to Mattel, one of the world's largest toy companies, that "YouTube is today's leader in reaching children age 6-11 against top TV channels," and representing to its competitor Hasbro, that it is the "#1 Website regularly visited by kids."[176] Such evidence was particularly damming since COPPA applies to any website that has knowledge that it will be collecting personal information or data from children.[177]
>
> The settlement required YouTube to pay a $170 million judgment and agree to a new set of policies when it comes to child-oriented programming. Among the requirements, YouTube was required to develop, implement, and maintain programs that has channel owners identify their child-related content on the platform and then create a method by which YouTube can ensure it complies with COPPA. Additionally, it required YouTube to notify channel owners that their child-directed content may be subject to COPPA as well as provide annual training about COPPA compliance to any YouTube employees that interact with channel owners.[178]

4. *Central Provisions.*
   A. 15 U.S.C. § 45 ("Section 5"): At its heart, the act is one that governs "unfair or deceptive acts or

events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations.

[176] *Id*.
[177] *Id*.
[178] *Id*.

practices in or affecting commerce (15 U.S.C. § 45 (a)(1))."

The "unfair" part of Section 5 is invoked when an act meets all of the elements of their three-part test: an act is unfair if it (1) causes or is likely to cause substantial injury (can be monetary) to consumers, (2) cannot be reasonably avoided by consumers, and (3) is not outweighed by countervailing benefits to users or to the competition. It is important to note that issues of public policy may also be considered but will not affect the outcome if all three factors are not met.

Similarly, "deceptive practices" also must satisfy a three-part test: the representation, omission, or practice must: (1) mislead or be likely to mislead the consumer, (2) the consumer's interpretation of the representation, omission, or practice must be reasonable under the circumstances, and (3) must be material. Notably, unlike with unfairness, deceptive practices do not require proof that the consumer could not avoid and there is no balancing test against potential benefits. Therefore, in most cases, it may be easier for the FTC to bring causes of action under deceptive practices rather than unfairness.

B. Children's Online Privacy Protection Act ("COPPA"): COPPA "prohibits unfair or deceptive acts or practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet".[179] COPPA is enforced under the same provisions of 15 U.S.C. § 45 for unfair and deceptive trade practices. One part

[179] COPPA, 16 C.F.R. § 312.1.

that makes it unique is that websites/organizations may actually have the FTC review and pre-approve their websites, policies, and practices under Section 312.12 of COPPA.[180] Specifically, Section 312.3 of COPPA states that any website or online service directed to children or have knowledge that it will be collecting and/or maintaining the personal information of children to do the following: (1) provide notice and clear disclosure of what information is being collected from the minor, how such information will be collected and how will be used, (2) must obtain verifiable parental consent prior to the collection of any such data from a minor, use of the data or disclosure of it, (3) provide a method for the parent to review the information being collected and then also to refuse further use or maintenance of said data, (4) create reasonable procedures and safeguards for protecting the security, confidentiality, and integrity of the data. [181] Additionally, that website or service may not make participation in an activity, game, or prize conditioned upon the receipt, use, or disclosure of personal information of a minor.[182]

C. 15 U.S.C. § 46(b) ("Section 6(b)") and 15 U.S.C. § 46(f) ("Section 6(f)"): These provisions of the code provide the FTC broad subpoena like powers to require any company or organization engaged in commerce to compile and file reports answering questions regarding their practices. They also allow to then take this information from various companies

[180] COPPA, 16 C.F.R. § 312.12.
[181] COPPA, 16 C.F.R. § 312.3.
[182] *Id*.

and organizations to conduct studies and publish reports for the public interest.[183]

5. *Implementation Trends.*

The FTC has demonstrated as an agency to make data privacy a major part of its agency mandate. This can be seen through the sheer number of lawsuits it has brought under 15 U.S.C. § 45 and COPPA.[184] Also, with the large monetary penalties the FTC has imposed on companies like Facebook, the agency has demonstrated a willingness to make it financially relevant in order for companies to comply with its requirement ensuring that companies take reasonable data security measures seriously.[185] While the FTC has been accused of overreach and overly burdensomeness, it has mostly escaped the open critical analysis seen with GDPR. This is because the FTC's authority to regulate has come from the courts rather than through the legislature.

It can also be seen by its recent use of 15 U.S.C. § 46(b). On December 14, of 2020, FTC used its authority under 15 U.S.C. § 46(b) to require the major tech giants including Amazon, Facebook, YouTube, WhatsApp, Snap, Twitter, Twitch, Reddit, Discord, and ByteDance Ltd. to turn over information regarding their data processing procedures. In its request, the FTC is specifically asking these companies "To compile data concerning the privacy policies, procedures, and practices of Social Media and Video Streaming Service providers, including the method and manner in which they collect, use, store, and disclose information about users and their devices, pursuant to

[183] FTC Act, 5 U.S.C. § 46(b), 15 U.S.C. § 46(f).
[184] Federal Trade Commission, *2018 Privacy and Data Security Update*, FTC.GOV, (2018), https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.
[185] Federal Trade Commission, *supra* note 159.

> Section 6(b) of the Federal Trade Commission Act, 15 U.S.C. § 46(b)."[186] This large scale effort to "lift the hood on the social media and video streaming firms to carefully study their engines. As concerns mount regarding the impact of the tech companies on Americans' privacy and behavior, this study is timely and important."[187] Even stating that there is greater concern that "despite their central role in our daily lives, the decisions that prominent online platforms make regarding consumers and consumer data remain shrouded in secrecy. Critical questions about business models, algorithms, and data collection and use have gone unanswered. Policymakers and the public are in the dark about what social media and video streaming services do to capture and sell users' data and attention. It is alarming that we still know so little about companies that know so much about us." [188] The FTC's goal being clearly to create increased transparency between the public and the companies profiting off of their data by bringing data practices of these large corporations into the light.[189]
>
> If the past is any indication, this investigation will probably lead to several things: (1) The possibility of further investigations and administrative suits against these companies for not taking reasonable security measures much like those we saw with Facebook and YouTube in the recent past with ever-increasing and stricter standards backed with more detailed and comprehensive orders.[190] (2)

---

[186] *See U.S. Before the F.T.C.*, Resolution Directing Use of Compulsory Process to Collect Information Regarding Social Media and Video Streaming Service Providers' Privacy Practices, FTC Matter No. P205402 (2020), https://www.ftc.gov/system/files/documents/reports/6b-orders-file-special-reports-social-media-service-providers/6b_smvss_resolution.pdf.
[187] *See* Statement of F.T.C., *supra* note 3.
[188] *Id*.
[189] *Id*.
[190] Federal Trade Commission, *supra* note 159; Federal Trade Commission, *supra* note 175.

The publication of not just a report of the FTC's findings[191], but also guidelines for companies regarding data security. Just as we saw with many publication in the past like The FTC Guidebook for Social Media Influences: Disclosers 101 for Social Media Influencers[192], the Children's Online Privacy Protection Rule: A Six-Step Complain Plan for Your Business, YouTube channel owners: Is your content directed to children[193], Cyber security for Small Business[194], Data Breach Response: A Guide for Businesses[195], Stick with Security: A Business Blog Series [196] , Careful Connections: Keeping the Internet of Things Secure[197], Start with Security: A guide for Business [198], and many more available on the FTC website. (3) There could be an administrative shift away from focusing on data security with the appointment of new appointees under the Biden administration, though this is unlikely given the terms of the

[191] Federal Trade Commission, *supra* note 162.
[192] Federal Trade Commission, *Disclosures 101 for Social Media Influencers*, FTC.GOV (Nov. 2019), https://www.ftc.gov/system/files/documents/plain-language/1001a-influencer-guide-508_1.pdf.
[193] Kristin Cohen, *YouTube channel owners: Is your content directed to children?*, FTC.GOV (Nov. 22, 2019), https://www.ftc.gov/news-events/blogs/business-blog/2019/11/youtube-channel-owners-your-content-directed-children.
[194] Federal Trade Commission, *Cybersecurity for Small Business*, FTC.GOV https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity.
[195] Federal Trade Commission, *Data Breach Response: A Guide For Business*, FTC.GOV (Apr. 2019), https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business.
[196] Federal Trade Commission, *Stick with Security: A Business Blog Series*, FTC.GOV (2017), https://www.ftc.gov/tips-advice/business-center/guidance/stick-security-business-blog-series.
[197] Federal Trade Commission, *Careful Connections: Keeping The Internet of Things Secure*, FTC.GOV (Sept. 2020), https://www.ftc.gov/tips-advice/business-center/guidance/careful-connections-keeping-internet-things-secure.
[198] Federal Trade Commission, *Start with Security: A Guide for Business*, FTC.GOV (June 2015), https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business.

current commissioners.[199] (4) The results may usher in comprehensive change to data regulations and legislation. However, unless we see a shift away in focus or some other federal regulation of the area it can be expected to see the FTCs presence in this area to continue its trend of expanding its regulatory authority to protect consumers that are now more and more heavily reliant on companies that are using their data.

**Global Data Privacy Trends:**

In recent history, data privacy regulations like GDPR and CCPA have made a large splash creating a trend of specific regulations over anyone collecting data, storing data, or processing data online in both Europe and California. Inspired by these laws, the latest very public data privacy scandals, and the current COVID-19 global pandemic other countries like China, Japan, South Korea, and India have started developing and modifying their own data privacy regulations to be like GDPR. Both Japan and Korea made major amendments in 2020. Japan amended its data privacy law Act on the Protection of Personal Information (APPI), to make it closer to GDPR[200] and South Korea amended its 3 major data privacy regulations the Personal Information Protection Act (PIPA); the Act on the Promotion of Information and Communications Network Utilization and Information Protection ('Network Act'); and the Act on the Use and Protection of Credit Information ('Credit Information Act') to incorporate pieces similar to GDPR. Other

[199] Mike Cowie, *The FTC in a Biden Administration Could Remain Republican Controlled for More Than 2 Years*, JDSUPRA.COM (Oct. 4, 2020), https://www.jdsupra.com/legalnews/the-ftc-in-a-biden-administration-could-67484/; John E. Villafranco et al., *What Happens to the FTC Under a Biden-Harris Administration?*, ADLAWACCESS.COM (Nov. 9, 2020), https://www.adlawaccess.com/2020/11/articles/what-happens-to-the-ftc-under-a-biden-harris-administration/.

[200] Scott A. Warren & Maika Kawaguchi, *New Amendments Passed to Japan's Data Privacy Law*, NATLAWREVIEW.COM (Aug. 19, 2020), https://www.natlawreview.com/article/new-amendments-passed-to-japan-s-data-privacy-law.

countries like China and India are developing their own versions of data privacy regulations. On October 21, 2020, China revealed its draft of a data privacy act called the Personal Information Protection Law (PIPL),[201] while in the wake of COVID-19 India has continued to delay its review of the Personal Data Protection Bill (PDPB), which was originally introduced in 2019 before the pandemic.[202]

Outside of Europe and Asia, we can also see some influences of this trend to have GDPR style data privacy acts. Interestingly Chile, Argentina, Uruguay, Mexico, Peru, and Columbia already had their own data privacy regulations, but after being inspired by GDPR, several other countries in Latin America like Barbados, Panama, and Brazil have quickly started following suit with statues modeled after GDPR.[203] Though it has taken a while for countries with earlier data privacy laws in Latin America to get enforcement agencies established, several countries like Mexico are taking significant strides towards enforcing their data privacy laws.[204] In Africa, we have seen a flurry of interest in data privacy regulations. African countries have played an interesting role as testing grounds for new technology especially in areas like biometric data use. Oddly enough, there seems to be a lack of consensus as to how many African countries have passed data privacy legislation versus how many have just proposed legislation with some sources ranging

[201] Gil Zhang & Kate Yin, *A look at China's draft of Personal Information Protection Law*, IAPP.ORG (Oct. 26, 2020), https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/.
[202] OneTrust, *India's Personal Data Protection Bill*, ONETRUST.COM, (July 24, 2020), https://www.onetrust.com/blog/indiias-personal-data-protection-bill/ and Diana Lee, Gabe Maldoff, & Kurt Wimmer, *Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR*, IAPP.ORG (Mar. 2020), https://iapp.org/resources/article/comparison-indian-personal-data-protection-bill-2019-vs-gdpr/.
[203] Katitza Rodriguez & Veridiana Alimonti, *A Look-Back and Ahead on Data Protection in Latin America and Spain*, EFF.ORG (Sept. 21, 2020), https://www.eff.org/deeplinks/2020/09/look-back-and-ahead-data-protection-latin-america-and-spain; Cynthia Rich, *Privacy Law in Latin America and the Caribbean*, 14 PVLR 730 (2015), https://iapp.org/media/pdf/resource_center/Privacy_Laws_Latin_America.pdf.
[204] *Id*.

from 17- 24 out of 53 countries have passed data privacy regulations in Africa.[205] South Africa being one of the latest African countries to enact data privacy legislation in 2020 with the Protection of Personal Information Act (POPIA)[206] which may be the mark of a continuing trend of data privacy regulation and enforcement finding political support in other neighboring African countries.

With the worldwide COVID-19 pandemic in 2020, the recent 2016 U.S. Cambridge Analytica scandal,[207] and the current SolarWinds Orion Russian hacking scandal estimated to have affected over 18,000 global customers, including many U.S. government agencies [208] there is likely to be more and more support for governments and legislators to more stringently regulate data privacy with data privacy specific legislation like GDPR, CCPA and others mentioned above. The pandemic has made citizens of the world more keenly aware of their dependence on large internet-based data collectors and processors than ever before. It would be reasonable to expect more information regarding the weaknesses of our regulations to comes to light in the near future. Specifically, information from the December 14, 2020 FTC Section 6(b) requests

---

[205] Privacy International, *2020 is a Crucial Year to Fight for Data Protection in Africa*, PRIVACYINTERNATIONAL.ORG (Mar. 3, 2020), https://privacyinternational.org/long-read/3390/2020-crucial-year-fight-data-protection-africa; Admire Moyo, *Only 17 out of 54 African States Have Data Privacy Laws*, ITWEB.CO.ZA, (Aug. 26, 2020), https://www.itweb.co.za/content/WnxpEv4gon4qV8XL; Jennigay Coetzer, *Africa's Lack of Data Protection and Cybercrime Laws Has Created Deep Vulnerabilities. But Is Change On The Way?*, LAW.COM (May 27, 2020), https://www.law.com/international-edition/2020/05/27/africas-lack-of-data-protection-and-cybercrime-laws-has-created-deep-vulnerabilities-but-is-change-on-the-way/.

[206] Nerushka Bowan, *After 7-year Wait, South Africa's Data Protection Act Enters into Force*, IAPP.ORG (July 1, 2020), https://iapp.org/news/a/after-a-7-year-wait-south-africas-data-protection-act-enters-into-force/; Hunton Andrews Kurth LLP, *South Africa's Protection of Personal Information Act, 2013, Goes into Effect July 1*, NATLAWREVIEW.COM (June 29, 2020), https://www.natlawreview.com/article/south-africa-s-protection-personal-information-act-2013-goes-effect-july-1.

[207] Ma & Gilbert, *supra* note 11.

[208] Marquardt et al., *supra* note 12.

to make public Amazon, Facebook, YouTube, WhatsApp, Snap, Twitter, Twitch, Reddit, and Discord's data collection, processing, and storage practices. This will give the FTC, and possibly the public, far more comprehensive information about what is being done with the private data of individuals than ever before. [209] As the public learns more about how their data and information is collected, stored, and used, it is reasonable to think that more data privacy regulation and enforcement will be demanded globally. Undoubtedly, data and cybersecurity will also play a pivotal role in investigating, finding, and charging individuals that recently breached the security of the U.S. Capitol building in D.C. In the days to come, the public will learn more about how much information can be uncovered about individuals by the amount of data available online about them. Already, many individuals have been identified and charged based on information and images posted online. [210] As a society, our understanding of data security and privacy may dramatically shift as all of this information comes to light.

While regulations like GDPR have gotten a lot more attention from the public doing a great deal to raise awareness, currently in the U.S., the FTC seems to be a more powerful tool at regulating the practices of big data internet-based organizations. It remains to be seen if such GDPR-style specific regulations will be more affective and more powerful in the future than FTC-style, less specific, Section 5 and Section 6, regulations have been; particularly when coupled with industry-specific regulations like COPPA, HIPAA, FCRA, RFPA, GLBA, EFTA, and FINRA.

[209] *See* Statement of F.T.C., *supra* note 3.
[210] Kevin Collier, *Selfies, social media posts making it easier for FBI to track down Capitol riot suspects*, NBCNEWS.COM (Jan. 16, 2021), https://www.nbcnews.com/tech/social-media/selfies-social-media-posts-making-it-easier-fbi-track-down-n1254522.