DATA SNATCHERS: ANALYZING TIKTOK'S COLLECTION OF CHILDREN'S DATA AND ITS COMPLIANCE WITH MODERN DATA PRIVACY REGULATIONS

Samuel M. Roth*

I. Introduction

Between nationwide bans and high stakes data privacy settlements, modern social media applications face a considerable risk collecting the personal information of their younger users, and, as one of the fastest growing social media platforms, TikTok is no exception.[1] TikTok is a social-networking platform owned by ByteDance that allows users to create and share short-form mobile videos.[2] In 2020,

* J.D. Candidate, Suffolk University Law School, 2022.

[1] *See* Eldar Haber, *The Internet of Children: Protecting Children's Privacy in a Hyper-Connected World*, 20 U. ILL. L. REV. 1209, 1209 (2020) (noting the mass datafication of children in today's society as well as the heightened responsibility for companies to handle children's data more carefully). The move towards an "always-on" era, by which interconnected devices constantly collect data from users, regardless of their age, exposes children to grave privacy risks. *Id.* The dire consequences of children's interconnectivity on a global scale, and the mass data-collection the results from such interconnectivity, necessitates a comprehensive reform of the regulatory framework that governs such protection. *Id. See also* Sam Blake & Tami Abdollah, *TikTok Under Scrutiny From Child Privacy Advocates*, DOT.LA (May 14, 2020), *archived at* https://perma.cc/JM53-N3FW (stating that in the U.S., TikTok is currently fighting multiple class action lawsuits and receiving pressure from regulatory enforcement agencies).

[2] *See Our Products*, BYTEDANCE (2020), *archived at* https://perma.cc/2Z2X-R69W (describing the mission and use of TikTok). ByteDance's products mostly incorporate social media and interconnectivity, with offices and availability around the globe. *Id. See also* Joe Tidy & Sophia Smith Galer, *TikTok: The story of a social media giant*, BBC (Aug. 5, 2020), *archived at* https://perma.cc/6NSP-G5AG (detailing the story of TikTok as a social media giant); John Herrman, *How TikTok*

TikTok's mobile application reached two billion global downloads on the App Store and Google Play, a milestone for ByteDance and a record number of downloads for any application.[3] With its popularity and influence increasing rapidly during the COVID-19 pandemic, TikTok found success in its highly addictive and accessible format, attributing to the app's large percentage of predominantly young users.[4] Dances, lip-syncs, and comedy shorts comprise a majority of content on the platform, oftentimes bridging the cultural gap between its users through unprecedented access to a worldwide audience.[5] But,

Is Rewriting the World, THE N.Y. TIMES (2019), *archived at* https://perma.cc/MSF3-K29E (explaining the format and presentation of TikTok).

[3] *See* Craig Chapple, *TikTok Crosses 2 Billion Downloads After Best Quarter For Any App Ever*, SENSOR TOWER (Apr. 29, 2020), *archived at* https://perma.cc/5FXL-24AE (recognizing TikTok's exponential growth in downloads by quarter through the App Store and Google Play). In Q1 2020, TikTok generated the most downloads for any app ever in a quarter, accumulating more than 315 million installs across the App Store and Google Play. *Id.* Google Play has accounted for the vast majority of TikTok downloads, racking up more than 1.5 billion installs, or 75.5 percent of the total while the App Store has generated 495.2 million downloads, or 24.5 percent. *Id.*

[4] *See id.* (stating that while the app was already popular and backed by a large user acquisition campaign, TikTok's latest surge comes amid the global COVID-19 pandemic, which has seen consumers drawn to their mobile devices more than ever as they look for new ways to shop, work, and connect with others)*; see also* Irfan Sabir et al., *TikTok Addictions and Its Disorders among Youth of Pakistan*, 7 INT'L J. OF MULTIDISCIPLINARY & ALLIED STUDIES 140, 145 (2020) (concluding that TikTok addictions are affecting people who are inspired by TikTok videos and people making those videos causing depression and different kinds of complexes among youth); V. Dinesh Kumar & M. Shuriya Prabha, *Getting glued to TikTok[R] – Undermining the psychology behind widespread inclination toward dub-mashed video.*, 20 ARCHIVES OF MENTAL HEALTH 76, 76 (2019) (applying the core concept of self-comparison orientation theory that TikTok utilizes to create an illusionary complex process whereby an anonymous person is converted into a celebrity). TikTok recognizes the influence in portraying an anonymous users' exaggerated version of the self-identity in a confined virtual environment, combining celebrated virtual moments with the instant gratification of boosting up one's own "self-identity." Kumar & Prabha, *supra*. *See also* Rachel Waters, *Lessons From TikTok's Latest Privacy Trouble with Tweens*, IPWATCHDOG (June 7, 2020), *archived at* https://perma.cc/EV5M-YMNQ (suggesting that COVID-19 has been a boon to a growing group of entertainment-based apps and services, including Netflix, Amazon, Zoom, Instagram, and TikTok).

[5] *See* Herrman, *supra* note 2 (noting that TikTok's owner, ByteDance relies heavily on AI — not human editors, or a self-selected feed of accounts — to curate and create customized streams of largely user-and-partner-generated content tailored to each of its readers). TikTok is a landscape that evolved both alongside and at arm's length from the American tech industry. *Id.*

with TikTok's increasing number of users sharing and creating videos comes growing concerns about the app's safety.[6]

Social media companies, and their respective platforms, are frequently criticized and TikTok's rapid rise in popularity invited similar judgment.[7] Industry giants like Facebook, Twitter, and Snapchat have been subject to civil lawsuits, regulatory fines, and public opposition, yet the global number of social media users has doubled since 2015.[8] Notably, TikTok's swift expansion caught the

[6] *See* Tidy & Galer, *supra* note 2 (explaining the app's rapid growth has also put TikTok at the forefront of the minds of politicians). Accusations have been brought against TikTok and ByteDance from both the U.S. and India over the collection of sensitive data from users that could be used by the Chinese government for spying, but the accusations are vague. *Id. See* Geoffrey A. Fowler, *Is it time to delete TikTok? A guide to the rumors and the real privacy risks.*, THE WASH. POST (July 13, 2020), *archived at* https://perma.cc/PE5S-UD92 (elucidating that privacy concerns have been the most viral aspect of TikTok since July of 2020). *See* Coco Huang, *TikTok Challenged by More Than Trump in the US*, L.A. BUS. J. (Aug. 10, 2020), *archived at* https://perma.cc/CT8G-AMKA (stating that "[t]he primary concerns of the White House and lawmakers revolve around TikTok being used to collect personal data from U.S. citizens and to censor politically sensitive content"). Founder and former head of TikTok, Alex Zhu, told the *New York Times* in November of 2020 that TikTok does not share user data with its Beijing-based parent company, ByteDance, or the Chinese government. *Id. See* Chaim Gertenberg, *Reddit CEO says TikTok is 'fundamentally parasitic,' cites privacy concerns*, THE VERGE (Feb. 27, 2020), *archived at* https://perma.cc/Y2HQ-BY7J (quoting the CEO of Reddit, Steve Huffman, saying, "[TikTok is] so fundamentally parasitic, that it's always listening, the fingerprinting technology [it] use[s] is truly terrifying, and I could not bring myself to install an app like that on my phone," as well as warning others saying, "I actively tell people, 'Don't install that spyware on your phone.'").

[7] *See* Ingrida Milkaite & Eva Lievens, *Child-friendly transparency of data processing in the EU: from*
legal requirements to platform policies, 14 J. CHILD. & MEDIA 5, 10 (2020) (citing companies like Snapchat, Instagram, and TikTok as proven or potential offenders in the regulated data-collection industry); *see also* Waters, *supra* note 4 (providing that the privacy abuses leveled against TikTok serve as a guide for how those abuses arise and how they may be mitigated by any company building and growing a privacy compliance program).

[8] *See* Brian Dean, *Social Network Usage & Growth Statistics: How Many People Use Social Media in 2020?*, BACKLINKO (Aug. 12, 2020), *archived at* https://perma.cc/3BVU-ETPU (showing how social media companies rely on continuous growth in the number of people with internet access and smartphones). *See generally* Adi Robertson, *Social media bias lawsuits keep failing in court*, THE VERGE (May 27, 2020), *archived at* https://perma.cc/LQ83-AHLB (explaining the lawsuits that people file claiming they have been censored on social media, attributing this phenomenon to activism stunts, confusion of the law, and an exacerbated situation of politicians pushing misinformation).

attention of former president Donald Trump ("Trump") in July 2020, prompting a United States ("U.S.") ban by mid-September. [9] According to Trump, the hasty ban was due to the app's data-collection methods and the alleged national security threat U.S. citizens faced because of its Chinese ownership.[10] Whether Trump had the power to ban TikTok is currently being disputed, but the social and political impact of his declaration to do so places ByteDance at the center of an emerging issue in foreign relations.[11] With intensifying trade tariffs, diplomatic escalation, and Trump's politicized scrutiny of China's failure to contain COVID-19, Chinese technology corporations like

[9] *See* Whitney Robinson, *Trump Orders ByteDance to Divest TikTok's U.S. Operations.*, BUS. L. TODAY (Aug. 2020), *archived at* https://perma.cc/JK5H-6THQ (noting that on August 6, 2020, Trump issued an initial Executive Order outlining the threat posed by TikTok and stated that all transactions with ByteDance would be prohibited within 45 days of the order). *See* David Shepardson, Echo Wang, & Alexandra Alper, *Trump to shut off TikTok, WeChat to new U.S. users on Sunday*, REUTERS (Sept. 18, 2020), *archived at* https://perma.cc/3NFM-K2JU (providing context for the TikTok ban in the U.S.). *See* David Yaffe-Bellany & Edvard Pettersson, *TikTok Sues Trump Administration to Block U.S. Ban*, BLOOMBERG (Sept. 19, 2020), *archived at* https://perma.cc/RH8A-4ATF (discussing Trump's ban on TikTok, as well as TikTok's planned retaliation through the court system). *See* Tali Arbel, Matt O'Brien & Matt Ott, *US bans WeChat, TikTok from app stores, threatens shutdowns*, AP NEWS (Sept. 18, 2020), *archived at* https://perma.cc/BNQ6-VF5Z (revealing TikTok's reaction on the day the ban went into effect while providing detail on the potential cyber security concerns voiced by U.S. politicians). China's ministry of commerce condemned the ban and urged the U.S. to stop what it called bullying behavior and wrongdoing. *Id.* Similar concerns apply to U.S.-based social networks such as Facebook and Twitter, but Chinese ownership adds an extra wrinkle because the Chinese government could demand cooperation from Chinese companies. *Id.*

[10] *See id.* (stating that Trump has pressured the app's Chinese owner to sell TikTok's U.S. operations to a domestic company to satisfy U.S. concerns over TikTok's data-collection and related issues). *See also U.S. Relations With China 1949-2020*, COUNCIL ON FOREIGN RELS. (2020), *archived at* https://perma.cc/RPN2-T4SB (documenting China-U.S. relations throughout history, specifically noting the 2020 trade wars and Trump's growing Chinese trade blacklist).

[11] *See* Katy Stech Ferek, *U.S. Likely Exceeded Authority in TikTok Ban, Judge Says*, THE WALL ST. J. (Sept. 28, 2020), *archived at* https://perma.cc/UJ7W-VLWE (sharing that the federal judge who stopped the Trump Administration's download ban on TikTok determined that the government likely overstepped its authority under national security law); *see also* Yaffe-Bellany & Pettersson, *supra* note 9 (stating TikTok's belief that Trump exceeded his authority and did so for political reasons rather than to stop an "unusual and extraordinary threat" to the U.S., as the law requires). TikTok said the ban violates its First Amendment free-speech rights. Yaffe-Bellany & Pettersson, *supra* note 9.

TenCent, Huawei, and ByteDance were impeded by the U.S. government for their supposed encroachment into U.S. market and business operations.[12] Questions arose regarding ByteDance's data-collection practices and TikTok's use became a divisive topic for many Americans, prompting policy makers to investigate the lack of transparency from TikTok's data-collection practices.[13]

Like most companies that collect data on a global scale, TikTok is subject to prominent European Union ("E.U.") and U.S. privacy regulations governing the collection of civilian personal information and data.[14] With a third of TikTok's U.S. users being fourteen-years

---

[12] *See* Arbel, O'Brien & Ott, *supra* note 9 (discussing TenCent and ByteDance's disagreement with the U.S. government and disappointment with its treatment in the country); *see also* Sean Keane, *Huawei ban timeline: UK says there's 'clear evidence of collusion' between Huawei and China*, CNET (2021), *archived at* https://perma.cc/7LTC-XZ2F (providing a timeline of the eventual Huawei ban in the U.S.).

[13] *See* Dean DeChiaro, *House Republicans press TikTok on use of kids' data, ties to Beijing*, REUTERS (May 21, 2020), *archived at* https://perma.cc/66WW-7354 (noting, in May 2020, House Representatives Greg Walden, the top Republican on the House Energy and Commerce Committee, and Cathy McMorris Rodgers, the ranking member of a consumer subcommittee, asked TikTok what information was collected about American users, what data is shared with the Chinese Communist Party or other state-owned entities, and whether information on Americans is stored in China). *See* Chris Mills Rodrigo, *Schumer, Cotton request TikTok security assessment*, THE HILL (Oct. 24, 2019), *archived at* https://perma.cc/GPM9-KNC6 (reporting Senate Minority Leader Chuck Schumer (D-N.Y.) and Sen. Tom Cotton (R-Ark.) asking U.S. intelligence officials to assess whether Chinese-owned social media platform TikTok poses "national security risks"). Bipartisan U.S. questions were asked about the security risks of TikTok, including urged investigations from Senator Marco Rubio (R-Fla.) and the Open Markets Institute, an antitrust advocacy organization with close ties to Senator Elizabeth Warren (D-Mass). *Id.* In response to the new attention on their business practices, ByteDance registered to lobby the U.S., putting "general issues affecting internet companies" as one of its priorities and hiring American law firm Covington & Burling to provide advice on tech policy issues. *Id*. *See also* Mary Atamaniuk, *Which Company Uses the Most of Your Data?*, CLARIO (Oct. 14, 2020), *archived at* https://perma.cc/YT3S-TJNU (providing a chart showing the percentage of data gathered by Clario).

[14] *See* Alex Hern, *TikTok under investigation over child data use*, THE GUARDIAN (July 2, 2019), *archived at* https://perma.cc/8HN5-UKXW (reporting the UK's intention to investigate TikTok amidst GDPR noncompliance concerns); *see also* Robert Chesney, *TikTok and the Law: A Primer (In Case You Need to Explain Things to Your Teenager)*, LAWFARE INST. (Aug. 2, 2020), *archived at* https://perma.cc/QJ72-5F6C (recognizing that for purposes of CFIUS review, a covered "U.S. business" is any entity that engages in interstate commerce in the United States—even if that entity is a foreign corporation).

old or younger, ByteDance must meet a higher standard of care when collecting data.[15] Predominantly, the General Data Protection Regulation ("GDPR"), Children's Online Privacy Protection Act of 1998 ("COPPA"), and California Consumer Privacy Act ("CCPA") each play a part in regulating the data-collection methods of TikTok in the E.U. and U.S.[16]

Due to the emergence of the Internet of Things ("IoT"), vulnerable age groups are conditioned to allow apps like TikTok to collect and retain massive amounts of data in their routine functions, oftentimes without younger users recognizing the implications of doing so.[17] Fortunately, the publicization of TikTok's data-collection has uncovered significant flaws in the U.S.'s protection of children's privacy, highlighting the regulatory gaps in both federal law and public policy.[18] To curb the excessive collection of children's data, the U.S.

---

[15] *See* Raymond Zhong & Sheera Frenkel, *A Third of TikTok's U.S. Users May Be 14 or Under, Raising Safety Questions*, THE N.Y. TIMES (Aug. 14, 2020), *archived at* https://perma.cc/L9ME-VNKL (describing the youngest demographics of TikTok's users likely being even younger than their accounts claim). In July 2020, TikTok classified that more than a third of its 49 million daily users in the United States were fourteen-years old or younger, a figure reviewed by the *New York Times*. *Id.* One former TikTok employee said company workers had previously pointed out videos from children who appeared to be even younger than 13, yet they were allowed to remain online for weeks. *Id.*

[16] *See* General Data Protection Regulation, 2016 O.J. (L 119) 82–83 (regulating privacy and compliance standards set by the E.U. imposing crippling fines for every improper data processing practice). *See* California Consumer Privacy Act of 2018, CAL. CIV. CODE § 1798.198(a) (2018) (applying to California consumers, the CCPA resembles the GDPR in its protection of online privacy rights). *See* Children's Online Privacy Protection Act of 1998, 16 C.F.R §§ 312.6(c)–312.8 (2020) (setting limitations on gathering data from children, giving the parents the right to delete and alter the information, having the companies report their data-collection from minors, not conditioning a child's participation on the child disclosing more personal information than is reasonably necessary for participation, and maintaining the security and confidentiality of children).

[17] *See* Dave Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, CISCO INTERNET BUS. SOLS. GRP. (Apr. 2011), *archived at* https://perma.cc/DR8K-F2L2 (explaining the Internet of Things to better understand its potential to change everything we know to be true today). *See also* Stacy-Ann Elvy, *Commodifying Consumer Data in the Era of the Internet of Things*, 59 B.C. L. REV. 423, 424–25 (2018) (raising significant concerns for consumers in the new economic age brought on by the IoT). "If an IoT company does not have a privacy policy, it is likely free to monetize consumer data without concern for potential privacy policy violation claims." *Id.* at 439.

[18] *See also* Damin Park, *Mining for Children's Data in Today's Digital World*, 38 J. NAT'L ASS'N ADMIN. L. JUDICIARY 320, 339 (2018) (stating that despite the FTC's

must strengthen the enforcement power and broaden the scope of COPPA by incorporating elements of both the GDPR and CCPA to properly hold infringing data collectors accountable. Simultaneously, the U.S. must work to deter the harmful collection of children's data from a policy standpoint, reinforcing a positive social attitude towards data privacy and providing tools to educate the public's understanding of the modern privacy landscape.

II. History

A. Prominent Global and U.S. Data Protection Regulations

1. GDPR

In the E.U., the right to privacy is a part of the 1950 European Convention on Human Rights, which was remodeled to meet the modern necessities of technological progression.[19] In 2018, the E.U. revamped its personal data-collection and processing standards by passing the GDPR.[20] The GDPR is a set of safeguards and principles aimed at protecting the data privacy rights of E.U. citizens by holding data collectors responsible for their actions and attributing rights to data subjects.[21] One of those rights is based on the notion that people

work in implementing COPPA, providing amendments, and enforcing the law, COPPA still has limitations that fail to protect children from devious data-collection and marketing ploys).

[19] *See What is GDPR, the E.U.'s new data protection law?*, GDPR.E.U. (Oct. 13, 2020) [hereinafter *What is the GDPR?*], *archived at* https://perma.cc/6E7U-H8MJ (stating the GDPR in plain terms to allow for easier comprehension for E.U. citizens).

[20] *See* 2016 O.J. (L 119) 1 (validating the protection of natural persons in relation to the processing of personal data as a fundamental right). *See also* Milkaite & Lievens, *supra* note 7, at 6 (recognizing GDPR as a recent addition to the framework for collecting and processing personal data in the E.U.). "'Processing' is any operation which is performed on personal data, such as, for instance, collection, recording, organization, structuring, storage, use, disclosure, dissemination, erasure or destruction of data (article 4 (2) of the E.U. General Data Protection Regulation (GDPR))." *Id.* at 18 n.1. *See Data protection by design and default*, INFO. COMM'R'S OFF. (Apr. 23, 2021), *archived at* https://perma.cc/6JR9-2XJF (instructing data collectors on how to best collect data from their users, providing a checklist and helpful resources for doing so).

[21] *See* Milkaite & Lievens, *supra* note 7, at 7–10 (analyzing articles 12, 13, and 14 of the GDPR in relation to children's privacy rights). *See also* Henry H. Eckerson,

should be informed of and able to control what is happening with their personal information.[22] Other data subject rights include the right to access, rectify, or erase one's data, the right to restrict the processing of one's data, the right to have portability over one's data, and the right to object to the collection of one's personal data.[23] In recognizing such rights, the GDPR cast a wide net over global data-collection, threatening high fines for any entity that improperly processes the personal data of E.U. citizens or residents, or offers services to such people.[24] Today, the GDPR remains a leader in protecting E.U. citizens' data, influencing almost every major global regulation with similar goals.[25]

GDPR Reference Guide: All 99 Articles in 25 Minutes, ECKERSON GRP. (Nov. 28, 2017), *archived at* https://perma.cc/KNZ3-CQTM (describing that Article 12 requires data collectors to provide information in a concise, transparent, intelligible, and easily accessible form, using clear and plain language, and the controller needs to provide information on action taken on request by and to the data subject within one month). Article 13 requires data collectors to provide certain information to data subjects when personal data is collected from subjects, including the subject's rights, the period for which the data will be stored, and other pertinent information. *Id.* Like Article 13, Article 14 requires data collectors to provide certain information to the data subject when personal data is not being collected as well. *Id.*

[22] *See generally* Milkaite & Lievens, *supra* note 7, at 6 (listing the requirements of transparency and control in the GDPR). "These requirements of transparency and control include (1) provision of clear information about data processing, (2) communication from data controllers to data subjects on the rights available to the latter and (3) facilitation of the exercise of data subject rights in practice . . . ." *Id.*

[23] *See generally What is the GDPR?*, *supra* note 19 (defining the principles and key regulatory terms set in the GDPR).

[24] *See id.* (explaining who the GDPR applies to and the penalties associated with improper data processing of those individuals). "There are two tiers of penalties, which max out at €20 million or 4% of global revenue (whichever is higher), plus data subjects have the right to seek compensation for damages." *Id. See also 20 biggest GDPR fines so far [2019, 2020 & 2021]*, DATA PRIV. MANAGER (Feb. 8, 2021), *archived at* https://perma.cc/X5F5-JZMV (listing the biggest GDPR fines by February of 2021).

[25] *See* 2016 O.J. (L 119) 7 (contributing that children merit specific protection).

> Children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data. Such specific protection should, in particular, apply to the use of personal data of children for the purposes of marketing or creating personality or user profiles and the collection of personal data with regard to children when using services offered directly to a child.

Children are also recognized as specialized citizens under Recital 38 of the GDPR, noting that children merit specific protection because they are less aware of the potential risks and personal rights they have in regards to data processing.[26] Similarly, in an attempt to increase information transparency, Recital 58 requires privacy information addressed to children to be written in clear and plain language.[27] Article 8 sets a parental consent requirement for all children under the age of sixteen when online services are offered directly to them, requiring data collectors to obtain prior parental consent before processing children's personal data under Recital 38.[28]

Id. See also Sarah Hospelhorn, *California Consumer Privacy Act (CCPA) vs. GDPR*, VARONIS (2020), *archived at* https://perma.cc/EP6R-3PRB (comparing the influence of the GDPR on the first comprehensive U.S. online privacy regulation, the CCPA, and the differences the CCPA has from the E.U. regulation). "While the GDPR was created to protect citizens of the E.U., its impact spans much farther. The CCPA is an outcome of the GDPR's reaching influence, shifting government priorities and making them more willing to protect individual privacy." *Id.*

[26] *See* 2016 O.J. (L 119) 7 (recognizing that children merit special protection). *See* Milkaite & Lievens, *supra* note 7, at 8–9 (referencing Recital 38 of the GDPR). "Recital 38 GDPR explicitly states that 'children merit specific protection with regard to their personal data, as they may be less aware of the risks, consequences and safeguards concerned and their rights in relation to the processing of personal data.'" *Id.* at 8.

[27] *See* 2016 O.J. (L 119) 11 (discussing the principle of transparency and the importance of providing transparent communication with children). *See* Milkaite & Lievens, *supra* note 7, at 8–9 (specifically citing Recitals 38 and 58 of the GDPR). The requirement linked to Recital 58, is within the core principles of article 13 in the United Nations Convention on the Rights of the Child ("UNCRC") which aims to safeguard the child's right to seek, receive, and impart information and ideas of all kinds). *Id.* at 9. "'[A]ny information and communication where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand.'" *Id.*

[28] *See* 2016 O.J. (L 119) 37–38 (outlining the conditions applicable to a child's consent in relation to information society services). *See* Haber, *supra* note 1, at 1238 n.166 (discussing Article 8 of the GDPR and its mandated parental consent for minors under the age of 16 for valid processing of a child's data). *See also What if we want to target children with marketing?*, INFO. COMM'R'S OFF. (Apr. 23, 2021), *archived at* https://perma.cc/4JG7-ZH4M (outlining how targeted marketing at children heightens chances of violating Recital 38 of the GDPR, and advertising standards in the E.U.). "If they are also unable to critically assess the content of the marketing then their lack of awareness of the consequences of providing their personal data may make them vulnerable in more significant ways." *Id. See* Virginia A. M. Talley, *Major Flaws in Minor Laws: Improving Data Privacy Rights and Protections For Children Under the GDPR*, 30 IND. INT'L & COMP. L. REV. 127, 142 (2019) (providing that the GDPR regulation does not offer practical methods or

Furthermore, Article 12(1) of the GDPR requires data controllers to take appropriate measures to provide information in a concise, transparent, intelligible, and easily accessible form for all data subjects, especially children.[29] The specific methods of data processing that data collectors are compelled to use when dealing with the data of children not only encourages them to be transparent, but explicitly require them "to present the information efficiently and succinctly in order to avoid information fatigue."[30]

2. COPPA

Unlike the broader data privacy focus of the GDPR, COPPA is a U.S. federal regulation governing the online collection, use, and

solutions for obtaining verifiable and reliable parental consent for the processing of children's data).

[29] *See* 2016 O.J. (L 119) 39 (requiring transparent information, communication, and modalities for the exercise of the rights of the data subject).

> "[C]ontroller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Id. at 33. *See* Milkaite & Lievens, *supra* note 7, at 7 (imposing an obligation on data controllers to provide transparent information to data subjects). Article 12(1) of the GDPR requires controllers to "'take appropriate measures to provide any information . . . relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.'" *Id.* at 9. Additionally, the GDPR includes a provision that prohibits a collector from subjecting a minor's data to automated processing or profiling, compelling collectors to indicate the presence of automated decision making when used while processing data. *Id.* at 15. *See also* Nicole O., *Minors and Your Privacy Policy*, PRIV. POLICIES (Jan. 5, 2021), *archived at* https://perma.cc/C98P-DMU7 (noting that a data collector must be using reasonable efforts to verify that the minor is of the age of consent and that if the parent gives consent, that it was really the parent who consented).

[30] *See* Article 29 Data Protection Working Party, *Guidelines on transparency under regulation* 2016/679 7 (requiring data controllers to present information efficiently to avoid information fatigue); *see also* Milkaite & Lievens, *supra* note 7, at 9 (quoting Article 29). *See also Data protection by design and default*, *supra* note 20 (discussing GDPR Article 25 requirements). "The controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed." *Id.*

disclosure of personal information from children under the age of thirteen.[31] Enacted in October 1998, COPPA implements laws through the Federal Trade Commission's COPPA Rule (the "Rule"), giving the Federal Trade Commission ("FTC") general oversight and enforcement authority.[32] The Rule prohibits data collectors from engaging in unfair or deceptive acts and practices when collecting personal information from children on the Internet.[33] More

[31] *See* 16 C.F.R. §§ 312.1– 312.2 (noting how the U.S. federal regulation protects the control and processing of data for children under the age of 13). *See generally* Jeffrey D. Neuburger & Jonathan P. Mollod, CHILDREN'S ONLINE PRIVACY: COPPA COMPLIANCE, Westlaw 1-555-6526 (providing an overview of COPPA, the Federal Trade Commission, implementing regulations such as the COPPA Rule, including criteria affecting whether a website or online service operator must comply with COPPA, specific notice, verifiable parental consent, and other key requirements and practice tips for complying with COPPA or avoiding its scope).

[32] *See* 16 C.F.R. §§ 312.1–312.13 (providing the entire scope of the Children's Online Privacy Protection Rule); *see also* Neuburger & Mollod, *supra* note 31 (detailing the FTC COPPA Rule). *See also* Bethany Brown, *Children's Right to Privacy on the Internet in the Digital Age*, 20 UNIV. J. TECH. L. & POL'Y 223, 224–25 (2020) (introducing the role of the COPPA rule in the debate on whether the FTC sufficiently protects the rights of minors). "A major problem with the Rule, in light of the recent development of technology, is highlighted in both FTC settlements with Google and YouTube as well as the public comments regarding the review of the Rule: how to determine whether certain content is child-directed." *Id.* at 229. *See also* Shannon Finnegan, *How Facebook Beat the Children's Online Privacy Protection Act: A Look Into The Continued Ineffectiveness of COPPA and How to Hold Social Media Sites Accountable in the Future*, 50 SETON HALL L. REV. 827, 830 (2020) (noting that in the eighteen years since the enactment of COPPA, the internet has grown and the way data is stored, collected, and disseminated over the internet has become more complex and more prominent).

[33] *See* 16 C.F.R. § 312.1 (stating the scope of the COPPA regulations). COPPA "prohibits unfair or deceptive acts or practices in connection with the collection, use, and disclosure of personal information from and about children on the Internet." *Id. See* Brown, *supra* note 32, at 230 (stressing that the FTC needs to better define what it means for content to be child directed). *See* Andy Green, *Complete Guide to Privacy Laws in the US*, VARONIS (Mar. 29, 2020), *archived at* https://perma.cc/QC5Y-QDM7 (stating that "COPPA's regulatory rules . . . effectively expanded the reach of the law and broadened the type of personal information to be protected, including screen names, email addresses, video chat names, as well as photographs, audio files, and street-level geo coordinates."). *See also* Park, *supra* note 18, at 342 (describing the significant dangers children face when sharing personal information online from such a young age).

> Children who are born into the digital world may have intimate information about them tracked digitally as early as ten with a trend towards even younger ages. The significance of this is that these children, who are old enough to use and benefit from the

specifically, the Rule outlines five regulations: (1) operators must provide notice on their website about what information they collect and how they use this information, (2) operators must obtain verifiable parental consent prior to collecting or disclosing any child's personal information, (3) operators must provide a reasonable means for a parent to review the personal information collected from a child and provide the option to permit its further use, (4) operators may not make children give out more personal information than is reasonably necessary in order to play a game or participate in an online activity, and (5) operators must have reasonable procedures in place to protect the confidentiality, security, and integrity of personal information collected from children.[34] In addition to the five provisions, COPPA provides definitions for clarity and comprehension.[35] According to COPPA, a child is anyone under the age of thirteen, while an operator is anybody who operates a website and "collects or maintains personal information" from the website's users.[36]

In terms of enforcing COPPA, the FTC monitors the Internet and encourages complaints from parents on its website, imposing civil penalties in the form of fines, injunctive relief, and consumer redress for improper operation.[37] Additionally, a state attorney general may

> technology, may not grasp the weight of privacy issues at such a young age, and they likely have an even weaker grasp of why it is so important to protect those privacy rights as soon as they start using these technologies. This is because children, at such a young age, do not have the know-how, wisdom, or experience to appreciate what privacy entails and why it is important to preserve data and privacy in this digital age.

Id.

[34] *See* 16 C.F.R. § 312.1 (stating COPPA's general requirements). *See* Brown, *supra* note 32, at 226 (outlining the 5 regulations in the Rule).

[35] *See* 16 C.F.R. § 312.2 (stating definitions under the Rule).

[36] *See* Brown, *supra* note 32, at 225 (distinguishing the relevant definitions of "child" and "operator"); *see also* Neuburger & Mollod, *supra* note 31 (offering a more detailed explanation of how the FTC evaluates who is marked as an operator and when that operator's service is directed to children). *See also* Dan Feldman & Eldar Haber, *Measuring and Protecting Privacy in the Always-On Era*, 35 BERKLEY TECH. L. J. 197, 215 (2020) (arguing that children's information needed as much protection before the internet era as it did before COPPA was enacted).

[37] *See Children's Online Privacy Protection Act (COPPA)*, ELEC. PRIV. INFO. CTR. (2020), *archived at* https://perma.cc/TYY6-P5JB (highlighting the enforcement standards in place to ensure compliance with the Rule up to $11,000 per violation). *But see* Park, *supra* note 18, at 339 (stating that "[d]espite the FTC's work in implementing COPPA, providing amendments, and enforcing the law, COPPA still has limitations that fail to protect children from devious data collection and

bring a civil action for a violation of the Rule, which may include, but is not limited to, an injunction, enforced compliance, damages, restitution, or other compensation.[38] To date, all resolved FTC and state enforcement actions have resulted in settlements involving either an assessment of fines or constraining future conditions for collecting and handling information from children.[39]

3. CCPA

Although the U.S. established general data privacy rights for its citizens in 1974 with the U.S. Privacy Act, and later formulated the Health Insurance Portability and Accountability Act ("HIPAA"), California enacted the CCPA to extend consumer-privacy protections to modern day standards.[40] Under the comprehensive internet-focused CCPA, consumers in California have the right to access the specific pieces of collected information held by businesses while reserving the right to opt-out of third-party data sales.[41] Modeled after the GDPR, the CCPA is similar in that it includes a right to delete data gathered by collectors and includes a broad definition of "personal

marketing ploys."). Two significant examples of COPPA's failures to adequately protect children spawn from the confusing legalese advertisers are permitted to use within their privacy policies regarding parental consent, and in addition, the common practice of children lying about their age online with no verification requirements. *Id.* *See also* Elvy, *supra* note 17, at 487 (citing that scholars have noted that the FTC "has not followed the empirical evidence [regarding consumers' failure to read or understand privacy policies and 'how consumers form their expectations'] to the fullest extent.").

[38] *See Children's Online Privacy Protection Act (COPPA)*, *supra* note 37 (discussing, "[a]t the state level, COPPA authorizes state attorneys general to bring actions in federal district court to enforce compliance with the FTC regulations and to obtain damages or other forms of compensation and relief."). *See* Neuburger & Mollod, *supra* note 31 (expanding on the included relief an action on behalf of a state attorney general may bring).

[39] *See id.* (referencing the list of federal and state enforcement actions brought against COPPA violators).

[40] *See* CAL. CIV. CODE § 1798.100 (2018) (noting the California state data privacy legislation enacted in 2018). *See generally* Green, *supra* note 33 (providing a comprehensive and informative timeline of U.S. data privacy regulations during 2020 and the potential future of an increased amount of state data privacy legislation).

[41] *See id.* (describing the California consumer's right to access their own data through data subject access requests, or DSAR).

information."[42] However, the CCPA differs from the GDPR in that it does not require data collectors to have a legal basis for processing personal information.[43] Instead, the CCPA places the onus on the consumer, utilizing an opt-out system to encourage California consumers to take control of their own data processing.[44] Additionally, the CCPA gives consumers a limited right of action to sue if they're the victim of a data breach, including a general avenue for the state Attorney General to sue on behalf of California residents as well.[45] The CCPA set a trend within the U.S. to pass state data protection regulations, prompting states like Virginia, Maine, and Nevada to follow suit, and encouraging a slew of other states to consider privacy legislation of their own.[46]

In 2020, California governor Gavin Newsom vetoed a bill requiring parental consent for children under thirteen to create social media accounts.[47] The bill proposed an update for the CCPA to

[42] *See id.* (recognizing that the GDPR grants consumers a right to correct or rectify incorrect personal data while the CCPA does not, as well as requiring explicit consent at the point when consumers hand over their data). CCPA carries a broad definition of personal information, providing, "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." *Id.* "[T]he CCPA also contains a long list of identifiers it considers personal information, including biometric, geolocation, email, browsing history, employee data, and more." *Id. See* Hospelhorn, *supra* note 25 (providing a "big picture" view of the CCPA and its foundation on GDPR principles).

[43] *See* Green, *supra* note 33 (including the CCPA security provisions as an indication of the Center of Internet Security's top 20 controls and the NIST Critical Infrastructure Security Framework as baselines). *See* Hospelhorn, *supra* note 25 (noting who the CCPA applies to and the clear differences in each regulations' definition of terms and rights granted).

[44] *See* Green, *supra* note 33 (clarifying the U.S. approach to data privacy law by stating, "[t]he U.S. instead has vertically focused data federal privacy laws for finance (GLBA), healthcare ([HIPAA]), children's data (COPPA), as well as a new wave of state privacy laws with California Consumer Privacy Act (CCPA) being the most significant.").

[45] *See id.* (highlighting the potential action for the state Attorney General to sue collectors).

[46] *See id.* (listing the states with data regulations in place like the CCPA, as well as the states drafting their own versions). Other states considering their own privacy bills include Massachusetts, Maryland, Hawaii, North Dakota, and New York, each of which is expected to pass regulations of their own. *Id.*

[47] *See* Cynthia J. Larose, *California Update: Governor Signs One Privacy Bill and Vetoes Another*, MINTZ (Oct. 1, 2020), *archived at* https://perma.cc/VC4C-2GJA (providing information on how "Assembly Bill 1138 would have applied to sites and

incorporate the restrictions set forth in COPPA, but was rejected for its regulative redundancy.[48] Governor Newsom's veto was, in part, due to California's existing Senate Bill 568 ("SB 568") which aims to specifically protect California minors online by holding websites accountable for their data-collection methods if they are directed towards minors or have knowledge that minors are using their site.[49] SB 568 has two main provisions: the first is aimed at preventing exploitative online advertisements towards minors while the second provision focuses on a minor's right to "erase" his or her online posts.[50] California's state legislation protects minors' privacy rights far beyond any other state in the U.S., giving parents the opportunity to refuse to consent to an operator's further collection of information from their child.[51]

applications like Snapchat, Instagram, TikTok, Facebook, Twitter, etc., and would have taken effect July 1, 2021.").

[48] *See id.* (proffering that "Governor Newsom said in his veto message that states have the authority to enforce COPPA, and AB 1138 would only create 'unnecessary confusion' given its overlap with federal law.").

[49] *See* CAL. BUS. & PROF. CODE § 22580 (2019) (determining the privacy rights for California minors in the digital world). *See* Emily DiRoma, *Kids Say the Darndest Things: Minors and the Internet*, CARDOZO L. REV. DE NOVO 43, 46 (2019) (noting "California's enactment of SB 568 focuses on expanding the online safeguards that the Federal Trade Commission (FTC) put in place for minors and children with COPPA"). "California's legislation expanded the age of protection and the definition of a minor as promulgated under COPPA from under thirteen years old to under eighteen years old; thus broadening the age range of children and the scope of the law's protection." *Id.* at 46. *See also* Laura Arredondo-Santisteban & Randy Shaheen, *California Enacts Law Protecting Minors' Digital Privacy Rights*, VENABLE LLP (Nov. 24, 2014), *archived at* https://perma.cc/S9WN-CDZR (recognizing that under SB 586, "a website 'directed to minors' means a site 'that it is created for the purpose of reaching an audience that is predominantly comprised of minors, and is not intended for a more general audience comprised of adults.'"). "The bill also states that web operators which employ third party advertising services can comply with SB 568 by notifying the advertising service that the site is 'directed to minors.'" *Id.*

[50] *See* DiRoma, *supra* note 49, at 46 (discussing the two provisions of SB 586). "California's new eraser button law contains two key elements: it gives teens the right to delete social-media posts and prohibits certain types of advertising from targeting them." *Id.* at 56.

[51] *See id.* at 63–64 (arguing that "'[u]nlike COPPA, SB 568 is narrowly focused on giving minors the right to [request] the removal of information they post online and preventing online marketers from targeting [minors] with
offers for [prohibited] products and services.'"). Some believe that SB 568 creates an entirely new class of specially-protected minors not covered by COPPA, those teenagers older than thirteen, but under the age of eighteen. *Id.* at 64. "[A]dvocates

Recently, however, voters in California strengthened the CCPA's reach in the 2020 elections by passing Proposition 24, commonly referred to as the California Privacy Rights Act of 2020 ("CPRA").[52] Among a wide variety of updates, the CPRA provides new data privacy rights to California consumers that strengthen the CCPA's effectiveness, establishes a new enforcement agency, increases compliance burdens for covered businesses, and requires new standards for data minimization and retention.[53] Opt-out rights were also expanded under the CPRA to include "sharing" of personal information, which is defined as "the transfer or making available of a consumer's personal information by the business to a third party for cross-context behavioral advertising, regardless of monetary or other valuable consideration."[54] Notably, the CPRA also imposes triple fines for violations of children's privacy under the CCPA; fines that a covered business may face in addition to violations of COPPA.[55]

hope that the passage of SB 568 will continue to incentivize and push Congress to continue expanding protection for minors' privacy online," empowering kids, teens, and their families by providing the important option to delete their data. *Id.*

[52] *See generally* Brian H. Lam, *California Privacy Rights Act Passes - Dramatically Altering the CCPA*, MINTZ (Nov. 6, 2020), *archived at* https://perma.cc/ZYB4-C68Z (describing the CPRA, its provisions, and compliance burdens). "The CPRA becomes effective on January 1, 2023. Provisions that apply to covered business collection of personal information will apply to personal information collected on or after January 1, 2022." *Id.*

[53] *See id.* (noting the creation of the California Privacy Protection Agency ("CalPPA") which will have administrative authority and the ability to enforce the CPRA, including updated audit rights and the additional enforcement of the CPRA beyond the CCPA). Qualification for businesses that are considered as a "covered business" will be modified to include a broader range of data collectors than the CCPA previously considered. *Id.* The CPRA also includes a new category of personal information referred to as "sensitive personal information" which includes financial information, account log-in credentials, a consumer's identification numbers, precise geolocation, racial and ethnic information, personal communications, information about one's sex life or sexual orientation, and generic data, biometric, or health information. *Id.*

[54] *See id.* (explaining the added opt-out rights and user control provisions included in the CPRA).

[55] *See* Lam, *supra* note 52 (mentioning the triple fines for Children's Privacy where the collecting and selling information of children under the age of 16 violates the CCPA).

B. TikTok's Rise

As a media powerhouse valued at more than $100 billion by Bloomberg, TikTok's impressive rise to fame was neither accidental nor surprising.[56] TikTok's earliest incarnation existed as the Shanghai social media service, Musical.ly.[57] Initially designed to be a short-form educational app, Musical.ly was launched in 2014 as a new social media service in both China and the U.S.[58] Musical.ly allowed users to create and share short, 15-second lip-sync videos with other users on the platform, a popular feature still used on TikTok.[59] Through a blend of smart design choices and modest download rates, Musical.ly quickly accumulated a strong user base, expanding globally and reaching 70 million users by 2016.[60] Later that year, Coca-Cola launched its #ShareACoke campaign on Musical.ly, initializing Musical.ly's "user-generated" advertisement model.[61]

Meanwhile, in the same year, Chinese tech giant ByteDance launched a similar service in China called Douyin, attracting 100 million users in China and Thailand within one year.[62] In 2017,

---

[56] *See* Lulu Chen et al., *TikTok Owner's Value Exceeds $100 Billion in Private Markets*, BLOOMBERG (May 20, 2020), *archived at* https://perma.cc/LC3D-TG2H (detailing recent private share transactions for ByteDance's valuation rose at least a third to more than $100 billion); Herrman, *supra* note 2 (proffering TikTok is far from an evolutionary fluke); Tidy, *supra* note 2 (highlighting TikTok's origins as different to the fairytale start-up story we have heard before).

[57] *See* Tidy, *supra* note 2 (describing Musical.ly, and their strong U.S. business links due to a healthy audience in that key market).

[58] *See* Biz Carson, *How a failed education startup turned into Musical.ly, the most popular app you've probably never heard of*, BUS. INSIDER (May 28, 2016), *archived at* https://perma.cc/4YY3-KPNS (tracking the early history of TikTok, discussing its initial intent and popularity as told by the co-founder and former CEO of Musical.ly, Alex Zhu). *See Our Products*, *supra* note 2 (referencing ByteDance's social media services). *See* Herrman, *supra* note 2 (explaining Musical.ly and its careful progress into the AI generated content entertainment app TikTok).

[59] *See* Carson, *supra* note 58 (describing the typical videos made by TikTok content creators using top hits to boost popularity).

[60] *See id.* (quoting Zhu's stated number of Musical.ly users registered in 2016).

[61] *See SHARE A COKE: TURNING LYRICS INTO LANGUAGE*, SHORTY AWARDS (Oct. 17, 2020), *archived at* https://perma.cc/FT3A-P69Y (providing the impact of the #ShareaCoke campaign by showing 953,000 Musical.ly video submissions generating 134 million views, viewership figures far above the likes of YouTube and Instagram).

[62] *See* Tidy, *supra* note 2 (referring to Douyin as TikTok's Chinese "sister app," attracting 100 million Chinese and Thailand users with a year of launch in 2016); Herrman, *supra* note 2 (asserting that Douyin is one of the most popular of many

ByteDance acquired Musical.ly for $1 billion, globally reinventing the app as TikTok and keeping Douyin as an identical Chinese social media service.[63] Publicly traded, and positioned to overtake the likes of Facebook, Snapchat, and other social media super giants, TikTok grew rapidly thanks to its popularity with younger demographics and advertising capabilities.[64] In 2019, TikTok hired former high-profile Disney executive Kevin Mayer as CEO, who subsequently quit the position just four months later after the Trump Administration expressed concern about the company's ties to China.[65] Currently, TikTok retains roughly 800 million active users, an all-time high for social media applications.[66]

Despite its rapid growth, TikTok, while still known as Musical.ly, was involved in a $5.7 million settlement over allegations that the company illegally collected personal information from children.[67] The U.S. Department of Justice, on behalf of the FTC, filed

short-video-sharing apps in China, a landscape that has evolved at arm's length from the American tech industry).

[63] *See* Liza Lin & Rolfe Winkler, *Social-Media App Musical.ly Is Acquired for as Much as $1 Billion*, THE WALL ST. J. (Nov. 9, 2017), *archived at* https://perma.cc/S6U6-9BQX (reporting the $1 billion deal struck between Musical.ly Inc. and ByteDance to acquire the popular app in 2017); *see also* Kevin Tran, *Social video app Musical.ly acquired for up to $1 billion*, BUS. INSIDER (Nov. 13, 2017), *archived at* https://perma.cc/B2K3-5A6U (offering that the acquisition deal between Musical.ly Inc. and ByteDance is believed to be anywhere between $800 million and $1 billion).

[64] *See* Chen, *supra* note 56 (reciting TikTok's private trading reaching $140 billion). Andrea Walne, a partner at Manhattan Venture Partners claims, "[t]he trading of ByteDance is reflective of the global wave of consumers who agree that ByteDance can displace Facebook as the leading social network." *Id.* TikTok is in the ballpark of the market capitalizations of some of the world's biggest public companies, ahead of rivals such as Twitter Inc. and Snap Inc. but still behind Facebook Inc. *Id.*

[65] *See id.* (mentioning TikTok poaching the American Disney streaming star, Kevin Mayer, as CEO); *see also* Bloomberg, *TikTok CEO Kevin Mayer quits after 4 months*, FORTUNE (Aug. 27, 2020), *archived at* https://perma.cc/54F6-D8J8 (describing the reason for the former Disney executive's short exit from TikTok, citing the Trump Administration's criticism and potential U.S. ban as a significant factor in his departure).

[66] *See* Tidy, *supra* note 2 (showing TikTok's active user increase from 500 million to 800 million within a year).

[67] *See* Neuburger & Mollod, *supra* note 31 (stating the settlement case filed as *United States v. Musical.ly, Corp.* and the complaint alleging the app's violation of the Rule). *See* Jen Thorpe, *Musical.ly Fined $5.7 Million for Collecting Personal Information from Children*, GEEK NEWS CENT. (Feb. 27, 2019), *archived at* https://perma.cc/3JLT-HV8Y (providing background to the privacy settings that led to the alleged violation, resulting in the $5.7 million settlement).

a complaint alleging that the operators of the Musical.ly app were unaware that a significant percentage of users were younger than thirteen and received thousands of complaints from parents that their children under thirteen-years of age had created Musical.ly accounts.[68] Furthermore, the FTC alleged that Musical.ly violated the Rule by failing to notify parents about the app's collection and use of personal information from users under the age of thirteen, failing to obtain parental consent before such collection and use, and failing to delete personal information at the request of parents.[69] In addition to the $5.7 million settlement, Musical.ly agreed to comply with COPPA moving forward and to take all videos, made by children under the age of thirteen, offline.[70]

III. Facts

A. Common Data-Collection Practices

As business technology advances, data-collection methods evolve to outdate the limitations set in place by regulatory law.[71] With

[68] *See id.* (suggesting two lessons to learn from the TikTok settlement). It is important to remember that companies must take steps to ensure that the data from children is kept private and parents should not assume that an app will protect their child's data – or keep their child's profile private. *Id.*

[69] *See* Neuburger & Mollod, *supra* note 31 (stating that to register for the TikTok app, it required users to provide an email address, phone number, username, first and last name, a short biography, and a profile picture).

[70] *See id.* (summarizing the additional terms of the settlement).

[71] *See* Elvy, *supra* note 17, at 500 (criticizing the limitations of existing privacy frameworks).

> The limitations of existing privacy frameworks that rely excessively on a notice and choice model and the terms of a company's privacy policy, combined with the exponential growth and proliferation of new types of highly sensitive IoT consumer data, necessitate new discussions and solutions on how best to ensure the protection of consumer privacy and data in the IoT setting.

Id. See also Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), *archived at* https://perma.cc/XLH6-T9T9 (concluding that about half of Americans feel as if they have no control over who can access their online searches, and roughly eight-in-ten or more U.S. adults say that they have very little control over the data that government (84%) or companies (81%) collect about them). "79% of adults assert they are very or somewhat concerned about how companies are using the data they collect about them, while 64% say they have the

computerized algorithms and high-powered data processors, companies and websites can capture a wide array of consumer data in a variety of ways.[72] Although the GDPR, COPPA, and CCPA each define their own characterization of data, businesses classify and collect consumer data in four overarching categories: personal data, engagement data, behavioral data, and attitudinal data.[73] Personal data includes information that personally identifies a consumer such as Social Security numbers, race, health, and biometric data, as well as non-personally identifiable information like IP addresses, web browser cookies, and device IDs.[74] Engagement data traces how consumers interact with a business's digital property including websites, mobile apps, social media pages, emails, advertisements, and customer

same level of concern about government data collection." *Id. See also Netherlands fined TikTok over English-only privacy terms*, DEUTSCHE WELLE (July 22, 2021), *archived at* https://perma.cc/4EX2-2LTZ (reporting "[T]hat by not offering their privacy statement in full in Dutch, 'TikTok failed to provide an adequate explanation of how the app collects, processes and uses personal data' that younger children could readily understand.").

[72] *See* Jathan Sadowski, *When data is capital: Datafication, accumulation, and extraction*, 6 BIG DATA & SOC'Y 1, 2 (2019) (recognizing the economic relationship between data and capitalism known as "surveillance capitalism"). Both datafication and financialization seek to maximize value extracted "using innovative methods of capital creation and circulation, whether through complex financial instruments or complex information technologies." *Id.* at 9. *See also* Max Freedman, *How Businesses Are Collecting Data (And What They're Doing With It*), BUS. NEWS DAILY (June 17, 2020), *archived at* https://perma.cc/9UJ3-QW54 (noting how data analytics is a powerful field, "breaking down the sea of data into manageable tidbits of actionable insights."). *See also* Louise Matsakis, *The WIRED Guide to Your Personal Data (and Who Is Using It)*, WIRED (Feb. 15, 2019), *archived at* https://perma.cc/PU2F-PXXJ (describing how apps like Instagram, Messenger, Gmail, and Google Maps do not cost money, but you pay with your personal data instead, which they use to target you with ads).

[73] *See* Indrajeet Deshpande, *What Is Customer Data? Definition, Types, Collection, Validation and Analysis*, TOOLBOX (May 26, 2020), *archived at* https://perma.cc/JU6F-7UHU (providing that "[c]ustomer data is the behavioral, demographic and personal information about customers collected by businesses and marketing companies to understand, communicate and engage with customers."). *See generally* Freedman, *supra* note 72 (indicating the four types of consumer data businesses collect: personal data, engagement data, behavioral data, and attitudinal data).

[74] *See* David Lyon, *Everyday Surveillance: Personal data and social classifications*, 5 INFO., COMM., & SOC'Y 242, 251 (2002) (explaining personal data as data that is specifically manipulated to extract individual profiles of likely targets that is not otherwise publicly available). *See generally* Freedman, *supra* note 72 (defining personal data).

service.[75] Behavioral data records transactional information such as purchase history, product usage, repeated actions and habits, and qualitative data such as mouse movement information.[76] Finally, attitudinal data encompasses metrics on consumer satisfaction, purchase criteria, product desirability, and more.[77] Despite the potentially limitless methods available to businesses to capture consumer data, there are three generally recognized avenues for doing so.[78] According to Liam Hanham, a data science manager at Workday, consumer data can be collected by directly asking customers, by

[75] *See id.* (defining engagement data); *see also What is Engagement Data in Gainsight?*, GAINSIGHT (July 27, 2020), *archived at* https://perma.cc/VP2K-DJEL (explaining that "[e]ngagement data generally falls into four basic categories: product usage, brand and marketing engagement, support engagement, and success engagement.").

[76] *See* Freedman, *supra* note 72 (defining behavioral data). *See also* Shane Greenstein, *Behind the Buzz of Behavioral Data*, DIGITOPOLY (May 14, 2015), *archived at* https://perma.cc/BQ2S-7CS4 (explaining that "[b]ehavioral data refers to information produced as a result of actions, typically commercial behavior using a range of devices connected to the Internet, such as a PC, tablet, or smartphone, tracking sites visited, apps downloaded, or games played."). "Behavioral data contributes to two valuable activities — risk assessment and targeted advertising." *Id.* *See also* Deshpande, *supra* note 73 (defining that behavioral data helps you identify underlying patterns that customers reveal during their purchase journey, combining transactional data, product usage, and qualitative data). *See also* LAWRENCE LESSIG, FREE CULTURE: THE NATURE AND FUTURE OF CREATIVITY 130–35 (Penguin Books, 2004) (suggesting that there are four modalities that could regulate behavior: market, social norms, technology, and law).

[77] *See* Freedman, *supra* note 72 (defining attitudinal data); *see also* Michael J. Demetsky, *Behavioral Demand Modeling and Valuation of Travel Time: Attitudinal Data*, 1 TRANSP. RSCH. BD. 21, 21 (1974) (finding attitudinal data "arose from a consensus that behavioral analysis of travel choice has a much broader potential with psychological data than merely with subjective dimensions of modal attributes."). *See also* Desphande, *supra* note 77 (providing that attitudinal data is usually collected through surveys, interviews, focus groups, feedback, customer complaints, reviews, and other forms of direct consumer interaction). In short, "[a]ttitudinal data is driven by the feelings and emotions of your customers. It is how they perceive your brand and offerings." *Id.*

[78] *See* Freedman, *supra* note 72 (outlining how company data-collection methods vary, with some being highly technical and others being more deductive in nature). *See* Sadowski, *supra* note 72, at 1 (determining that "[t]he imperative to capture all data, from all sources, by any means possible influences many key decisions about business models, political governance, and technological development."). "Rather than data collection being seen as simply a way of producing and obtaining commodities that are somehow converted into monetary value, datafication takes shape as a political economic regime driven by the logic of perpetual (data) capital accumulation and circulation." *Id.* at 2.

indirectly tracking customers, and by appending other sources of customer data through data transfers and brokerage deals.[79]

Machine learning algorithms and other forms of Artificial Intelligence ("AI") are also powerful resources for data processing, flagging anomalies and providing automated recommendations to contextualize vast swaths of information.[80] The purpose and benefit of acquiring such information then informs businesses on how to optimize customer experience, refine company marketing strategies, profit from sales to data brokers and data service providers, and ultimately, secure more data.[81] The never-ending cycle of collect, sell, and repeat is an attractive incentive for businesses to capitalize on, with most modern companies making a majority of their profit from engaging in the data processing industry.[82] Yet, the question still remains whether sufficient regulatory law exists to prevent businesses from exploiting vulnerable consumers; a legitimate concern for parents in the IoT era.[83]

---

[79] *See* Freedman, *supra* note 72 (quoting Liam Hanham on the three ways customer data can be collected).

[80] *See id.* (recognizing the proliferation and improvement of data analytics due to machine learning algorithms and other forms of AI); *see also* Adam Uzialko, *How Artificial Intelligence Will Transform Business*, BUS. NEWS DAILY (Apr. 22, 2019), *archived at* https://perma.cc/63CS-N9B5 (explaining the role of AI in business today as a supportive tool by processing and analyzing troves of data more quickly than a human brain could).

[81] *See* Sadowski, *supra* note 72, at 4 (proffering that the value derived from data is a very important form of capital). Data is used to profile and target people, optimize systems, manage and control things, model probabilities, build digital systems, and grow the value of assets. *Id.* at 5. *See also* Freedman, *supra* note 72 (noting examples of how businesses use collected data).

[82] *See* Sadowski, *supra* note 72, at 8 (noting that data-collection is driven by the perpetual cycle of capital accumulation). *See* Brian X. Chen, *What We Learned From Apple's New Privacy Labels*, THE N.Y. TIMES (Jan. 28, 2021), *archived at* https://perma.cc/AE9G-BGE2 (focusing on Apple's recent decision to implement data privacy "nutrition labels" on their App Store, displaying the type of data collected on each app's product page for users to view).

[83] *See* Haber, *supra* note 1, at 1209 (asserting that children's privacy is at great risk due to the emergence of IoT). The IoT world is growing rapidly, leading to a potential, but likely, increase in surveillance. *Id.* at 1215. The potential negative impact on individuals' civil rights and liberties—and perhaps mostly on their right to privacy—could be direr for some vulnerable populations than others, as technology does not generally differentiate between users. *Id.* Children are a vulnerable population, easily influenced and vulnerable to risks and harms that parents need to be aware of, yet children today are watched over more than any other generation in history. *Id.* at 1222.

B. TikTok Age Demographics

Within the U.S., teenagers account for a large percentage of TikTok's active users.[84] According to the New York Times, more than a third of TikTok's 49 million daily users in the U.S. are fourteen-years old or younger; a concerning statistic considering the app's age minimum is thirteen-years old.[85] When users download TikTok onto a personal device and register for an account, the app asks for their birth date to verify whether they are eligible to use its service.[86] In the U.S., users ages thirteen and younger are only permitted to use a restricted mode within the app in which they are able to browse TikTok content, but cannot share personal information or videos.[87] Like most social media, TikTok can expose younger age groups to harmful situations like inappropriate content, social anxiety, cyberbullying, and predatory users.[88] Specifically, TikTok's AI curated "For You" page is controversial, as its comprehensive curation capabilities can suggest

[84] *See* J. Clement, *Distribution of TikTok users in the United States as of June 2020, by age group*, STATISTA (Nov. 6, 2020), *archived at* https://perma.cc/KB4W-QK2U (reporting that 32.5% of TikTok users are between the ages of 10–19 and that 29.5% of users are ages 20–29).

[85] *See* Zhong & Frenkel, *supra* note 15 (stating that the estimated number of American users that are 14 or younger is 18 million).

[86] *See id.* (claiming that there are concerns that some under-thirteen users may lie to get around the age restrictions, and that the platform is not obtaining the required consent from those users' guardians). *See also For Parents: Safety Center*, TIKTOK (2020), *archived at* https://perma.cc/6Z7X-YCV2 (stating on TikTok's safety information page, "[t]he full TikTok experience is intended for users age 13 and over. If you learn that your child under the age of 13 has registered for a 13+ TikTok account, contact us at: https://www.tiktok.com/legal/report/privacy. We will promptly take appropriate action.").

[87] *See* Zhong & Frenkel, *supra* note 15 (discussing the age-restricted "walled-off" mode available to TikTok users under the age of 13). *See also* Julia Alexander, *TikTok will pay $5.7 million over alleged children's privacy law violations*, THE VERGE (Feb. 27, 2019), *archived at* https://perma.cc/H762-7K7K (stating that TikTok's trust and safety team created the age-restricted version of the app in response to a $5.7 million settlement for violating COPPA).

[88] *See* Haley Zapal, *How TikTok Predators Are Interacting With Kids*, BARK (July 24, 2019), *archived at* https://perma.cc/LR5M-GL3H (describing TikTok's "For You" feature). According to Bark, a children's online safety tool, pedophiles take full advantage of the "For You" page, using it to curate an ever-growing collection of their favorite young singers. *Id. See also* Brandon Doyle, *TikTok Statistics – Updated June 2021*, WALLAROO (June 14, 2021), *archived at* https://perma.cc/F65P-XH7N (reporting that 83% of TikTok users post videos).

and display underage content creators for predators to follow, record "duets," and message.[89]

In response to safety concerns for underage users, TikTok unveiled a "Family Safety Mode" in which parents can manage screen time, restrict content, and limit direct messages or turn off the feature completely.[90] Further, on January 13, 2021, Elaine Fox, TikTok's Head of Privacy in Europe, published a blog post on TikTok's website outlining the company's updated approach to strengthen privacy and safety for youth on TikTok.[91] The updates to children's safety included changing the default TikTok privacy setting for all registered

[89] *See* Zapal, *supra* note 88 (criticizing TikTok's use of flattery to exploit younger users). Utilizing validation as a tool is common across social media, but with TikTok, the comments are often centered around one's singing ability or physical appearance, making compliments seem extra special and making it easier for predators to exploit kids who are eager to impress their online audience. *Id. See* Herrman, *supra* note 2 (describing "duets" as a type of "response" video where users can duplicate content from other users and add themselves alongside). *See also* Nicole Sakin, *TikTok settlement highlights power of privacy class actions to shape US protections*, IAPP (Mar. 23, 2021), *archived at* https://perma.cc/UES4-LJBQ (adding to the list of pending class actions lawsuits against TikTok, specifically referring to its settlement in the U.S. District Court for the Northern District of Illinois Eastern Division regarding the Biometric Information Privacy Act ("BIPA")). The complaint, amongst other claims, states that TikTok violated BIPA in several ways: (1) collecting, storing, and using users' face geometry scans (a biometric identifier under BIPA Section 10) without notifying or receiving written releases from users, (2) possessing and profiting from users' biometric identifiers "by using them for targeted advertising, improvements to artificial intelligence technologies, patent applications, and the generation of increased demand for and use of other products," and (3) impermissibly disclosing and disseminating users' biometric data without consent and without an allowed reason under BIPA, such as a subpoena. *Id.* TikTok agreed to pay a total of $92 million to settle the claims, agreeing to have TikTok employees and contractors complete annual data privacy compliance training and hiring a third party "to review the data privacy law compliance training for a period of three years and to provide verification of this review." *Id.*

[90] *See* Maressa Brown, *Is TikTok Safe for Kids?*, PARENTS (Feb. 20, 2020), *archived at* https://perma.cc/8YRJ-K2NE (discussing the dangers of letting a child explore TikTok on their own and the safety measures parents can take to reduce risk). *See also* Carmen Keenan, *Introducing Family Safety Mode and Screentime Management in Feed*, TIKTOK (Feb. 19, 2020), *archived at* https://perma.cc/D7JZ-39UK (unveiling TikTok's new feature to help parents and guardians keep their teens safe on TikTok).

[91] *See* Elaine Fox, *Strengthening privacy and safety for youth on TikTok*, TIKTOK (Jan. 13, 2021), *archived at* https://perma.cc/D5Y8-DVKZ (announcing changes for users under age 18 aimed at driving higher default standards for user privacy and safety).

accounts under the age of sixteen to private, tightening the options for commenting on videos for users under the age of sixteen by removing the "everyone" comment setting, changing the default duet settings to "friends only," only allowing downloads of videos that have been created by users sixteen and over, and setting the "suggest your account to others" feature to "off" for users under sixteen.[92] In addition, TikTok updated its default settings by restricting direct messaging and hosting live streams to accounts of users ages sixteen and older, restricting the buying, sending, and receiving of virtual gifts to users eighteen and over, and enabling parents and caregivers to set guardrails on their teens' TikTok accessibility through Family Pairing features.[93]

C. TikTok Data-Collection Practices and Government Bans

It is unclear to what extent TikTok collects its users' data, but government bans across the globe indicate international concern and frustration with the app's lack of transparency.[94] Among ongoing

[92] *See id.* (revealing the additional changes that TikTok is rolling out to promote a safe experience for younger users).

[93] *See id.* (noting TikTok's adjusted default account settings supporting stronger privacy measures for users and restating the company's commitment to keeping younger users safe).

[94] *See Penetrum Security Analysis of TikTok versions 10.0.8 – 15.2.3*, PENETRUM (Nov. 13, 2020), *archived at* https://perma.cc/22LC-MTU8 (finding that "[a]fter extensive research, TikTok is not only a massive security flaw waiting to happen, but that its ties to Chinese parties and Chinese ISP's make it a very vulnerable source of data that still has more to be investigated."). "Data harvesting, tracking, fingerprinting, and user information occurs throughout the entire application, collecting unneeded information like a phone's IMEI number, screen resolution, sim card provider, GPS tracking, and more." *Id. See* Craig Giles, *TikTok Investigation Should Prompt More Data Transparency*, LAW360 (Feb. 21, 2020), *archived at* https://perma.cc/7MYZ-4G25 (discussing the U.S. response to TikTok as a "counterintelligence threat" by recounting the investigations underway). "So while the investigation into TikTok is a positive step in the direction of recognizing early on the consequences of misused personal information, it also serves as a reminder that privacy and national security can often fall within the same sphere." *Id. See* Fowler, *supra* note 6 (writing that Jackson, from Disconnect, said the app sends an "abnormal" amount of information from devices to its computers). When Jackson opened TikTok, he found approximately 210 network requests in the first nine seconds, totaling over 500 kilobytes of data sent from the app to the Internet: equivalent to half a megabyte, or 125 pages of typed data. *Id.* Many of the requests TikTok was making was information about the phone (like screen resolution and the

investigations into children's privacy from the Committee on Foreign Investment in the United States ("CFIUS"), the UK's Information Commissioner's Office ("ICO"), and France's Commission Nationale de l'Informatique et des Libertés ("CNIL"), TikTok's data-collection practices are at the root of a rapid shift in data privacy and security.[95] Fortunately, a multitude of security consultants and reverse-engineers attempted to track TikTok's data-collection methods to determine the app's hidden framework, ultimately revealing information about the app's high security risks and formidable data processing functionality.[96] Countries such as India and Pakistan banned TikTok

Apple advertising identifier) that could be used to "fingerprint" your device even when you are not logged in. *Id. But see* Eva Xiao, *TikTok Doesn't Pose Overt Threat to U.S. National Security, Researchers Say*, THE WALL ST. J. (Mar. 22, 2021), *archived at* https://perma.cc/K6VF-YTF9 (claiming that experts have verified TikTok's data-collection relative to other social media giants like Facebook, finding no major differences in collection practices that should be a cause for concern).

[95] *See* Shining Tan, *TikTok on the Clock: A Summary of CFIUS's Investigation into ByteDance*, CTR. FOR STRATEGIC AND INT'L STUD. (May 13, 2020), *archived at* https://perma.cc/YDM9-DRM6 (stating that if CFIUS rules against ByteDance, the U.S. government would most likely force ByteDance to either sell TikTok or cease operations in the United States). "As ByteDance is tangled up in U.S. national security, the U.S. economy and popular culture, it will be hard for CFIUS to balance all three pressures." *Id. See also* Elizabeth Schulze, *TikTok is under investigation in the UK over children's data privacy rights*, CNBC (July 3, 2019), *archived at* https://perma.cc/U9WW-KDYJ (recounting head of the UK's ICO, Elizabeth Denham's opened investigation).

> "We are looking at the transparency tools for children," Denham said. "We're looking at the messaging system, which is completely open, we're looking at the kind of videos that are collected and shared by children online. So we do have an active investigation into TikTok right now, so you can watch that space."

Id. See also Natasha Lomas, *TikTok is being investigated by France's watchdog*, TECHCRUNCH (Aug. 11, 2020), *archived at* https://perma.cc/M53V-Q7VV (discussing the potential investigation of a French "watchdog" for GDPR). The fines levelled against TikTok, if it is found to not be in compliance with the GDPR, could be up to 4% of their annual revenue. *Id. See* Geoffrey Gertz, *Is TikTok a Threat to national security?*, THE WASH. POST (Nov. 11, 2019), *archived at* https://perma.cc/WY72-89EJ (recalling ByteDance's entry into the U.S. market by acquiring Musical.ly, prompting CFIUS review).

[96] *See* Andy Shane, *Zimperium Analyzes TikTok's Security and Privacy Risks*, ZIMPERIUM (Oct. 30, 2019), *archived at* https://perma.cc/B4FN-ESWG (reporting that in regard to TikTok, the Android version has high privacy and security risks, and iOS has high privacy and medium security risks). Zimperium z3A, a popular mobile security service, evaluates risks posed by mobile apps to help users manage security threats and breaches of privacy. *Id. See generally* bangorlol, *Not new news, but tbh if you have tiktiok, just get rid of it*, REDDIT (July 2020), *archived at*

from their mobile app stores as a result of their own analyses confirming the app's rampant data mining.[97] Despite such events, Pakistan's TikTok ban was rescinded shortly after with new assurances

https://perma.cc/Q7LY-MCVW (discussing the hidden data-collection methods of TikTok's application, gathered from the personal tests run by a Reddit user with the ability to reverse engineer phone applications to reveal their data-collection methods). The comment refers to TikTok as "a data collection service that is thinly-veiled as a social network," citing the application's ability to collect phone hardware and the owner's usage outside of the app, information on other application data, internet IP and router information, GPS pinging, "clipboard" access, the ability to set up a local proxy server with no authorization, and other hidden collection methods. *Id.* According to the reverse engineer, the Instagram, Facebook, Reddit, and Twitter apps do not collect anywhere near the same amount of data that TikTok does and are not trying to hide exactly what data is being tracked like TikTok is. *Id. But see generally TikTok Transparency Report 2019 H2*, TIKTOK (July 9, 2020), *archived at* https://perma.cc/X83C-NDUU (offering TikTok's efforts to comply with the public's call for transparency by releasing a detailed privacy report for the second half of 2019). Restricted content and government requests to delete content are given in the transparency report, notably discussing TikTok users' privacy in relation to other users, but not in relation to TikTok itself. *Id.*

[97] *See India bans TikTok, WeChat and dozens more Chinese apps*, BBC (June 29, 2020), *archived at* https://perma.cc/R86K-BL2H (noting "India's Ministry of Information Technology said it was banning 59 Chinese apps after receiving 'many complaints from various sources' about apps that were 'stealing and surreptitiously transmitting users' data in an unauthorized manner."). The ministry stated, "'The compilation of these data, its mining and profiling by elements hostile to national security and defense of India, which ultimately impinges upon the sovereignty and integrity of India, is a matter of very deep and immediate concern which requires emergency measures . . . .'" *Id. See also* Maria Abi-Habib, *India Bans Nearly 60 Chinese Apps, Including TikTok and WeChat*, THE N.Y. TIMES (June 30, 2020), *archived at* https://perma.cc/2X5P-EMPP (reporting the tense situation at the border between India and China, as well as India's valid concerns for its citizens' digital privacy). Christopher Ahlberg, the chief executive of Recorded Future, a cybersecurity company in Massachusetts that analyzes and collects threat intelligence, believes

> India's concerns aren't overblown, they are valid. China would not be above using these apps for large scale data collection. I don't expect that the government is running all these apps, but they may make an agreement with the companies that they have to cooperate once in a while. And it's easy under Chinese law to require them to do so.

Id. See Oliver Yeh, *India's TikTok Ban Cost the App At Least 15 Million New Users There—and Its Biggest Month Yet*, SENSOR TOWER (May 1, 2019), *archived at* https://perma.cc/2S5X-XEYQ (claiming that nearly two weeks after it was removed from the App Store and Google Play in India, ByteDance's social video app TikTok is available again in India, its largest market).

that the app's content would be moderated in accordance with local laws.[98]

Nevertheless, TikTok's potential ban in the U.S. placed the video sharing app in a unique position; one that balanced losing access to the American market with a forced corporate buy-out.[99] Scrutiny against TikTok began in 2017 when it was acquired by ByteDance, resulting in a CFIUS review and potential U.S. ban.[100] Although CFIUS is an interagency of the executive branch, Trump's "simple ban" on TikTok was derived from the executive branch's power under the International Emergency Economic Powers Act ("IAAPA").[101] In response, TikTok claimed that the Trump Administration's ban exceeded its authority by violating TikTok's free-speech rights and failing to relate to any "unusual and extraordinary threat," which is

[98] *See* Salman Masood, *Pakistan Rescinds TikTok Ban*, THE N.Y. TIMES (Oct. 19, 2020), *archived at* https://perma.cc/6LDR-GTUX (noting "[a] decision outlawing the social media app in Pakistan was overturned after 10 days with assurances from the Chinese owners that content would be moderated according to local laws.").

[99] *See* Proclamation No. 13,942, 85 R 48,637 (U.S. Dep't of Com. Aug. 11, 2020) (prohibiting TikTok from commercially existing in the U.S.). *See* Yaffe-Bellany & Pettersson, *supra* note 9 (stating that TikTok asked a federal judge to block the Trump Administration's ban on their app's usage in the U.S.).

[100] *See* Chesney, *supra* note 14 (writing that although Musical.ly was a foreign corporation at the time of its acquisition, it had a robust U.S. presence and qualified for CFIUS review under 31 CFR 800.252(a)). TikTok never sought approval from CFIUS at the time of their acquisition, likely due to low-risk national security implications. *Id.* TikTok's popularity in the U.S. and CFIUS's retroactive review of prior transactions prompted Trump to formally review the ByteDance-Musical.ly deal of 2017. *Id.* If CFIUS concludes that ByteDance should not have been able to complete the acquisition, ByteDance would be forced to divest itself of Musical.ly, or else cease operations in the United States. *Id.*

[101] *See* Proclamation No. 13,942 85 R 48,637 (U.S. Dep't of Com. Aug. 11, 2020) (ordering that "additional steps must be taken to deal with the national emergency with respect to the information and communications technology and services supply chain . . . ."). "Specifically, the spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States." *Id. See* International Emergency Economic Powers Act, 50 U.S.C. §§ 1701–1706 (outlining the executive branch's powers enumerated under the Act). *See* Chesney, *supra* note 14 (discussing the IEEPA as the executive branch's constitutional control over foreign commerce through embargos and targeted sanctions for a broadly defined set of circumstances to protect U.S. national interests). Under the IEEPA, the president can investigate, regulate, or ban an array or commercial activity, but the president must also declare a national emergency before doing so. *Id.*

required by the law.[102] TikTok sued to block Trump's order in a California federal court, but dropped the suit in order to file a separate claim in Washington against a second executive order carried out by the U.S. Department of Commerce ("DOC").[103] The second presidential order threatened to ban TikTok in the U.S. unless it could complete a takeover deal that allayed the government's national security concerns; an ultimatum that piqued the interest of potential U.S. buyers like Microsoft, Oracle, and Wal-Mart.[104] After the DOC

[102] *See* Yaffe-Bellany & Pettersson, *supra* note 9 (explaining the order targeting multiple Chinese businesses, not only TikTok). TikTok claimed that the U.S. government has "ignored evidence" and initiated the ban for political reasons. *Id. See also* Adi Robertson, *How the Trump administration could 'ban' TikTok*, THE VERGE (Aug. 1, 2020), *archived at* https://perma.cc/JT26-77JQ (describing how the Trump Administration could repeat a tactic it used with Huawei and have the Commerce Department put TikTok on the "entity list," limiting the app's commercial ties to U.S. companies by essentially flagging companies that U.S. businesses should use caution dealing with). The Trump Administration does not need congressional approval to place a company on the entity list and can cite any U.S. company that does business with it (barring special exemptions) for violating sanctions, a tactic that stopped Google from working with Huawei on Android phones and would likely influence Apple from keeping TikTok in the app store as well. *Id.* James Lewis, director of technology policy at the Center for Strategic and International Studies, says putting TikTok on the list would be "extreme, unusual, and legally dubious" because the Trump Administration "could sanction [it], but usually the sanction is tied to trade violations or espionage or proliferation or intellectual property theft. You can't just do it because you're mad at a company." *Id. See also* Alaina Lancaster, *Two Covington Litigation Veterans Will Take on Trump for TikTok*, LAW.COM (Aug. 24, 2020), *archived at* https://perma.cc/AZ6B-6PUG (announcing that TikTok, represented by Covington & Burling, sued the Trump Administration over an executive order banning the social media platform in the U.S.).

[103] *See* Complaint for Injunctive and Declaratory Relief at 3–4, TikTok Inc. v. Trump, C.D. Cal. R. (Aug. 24, 2020) (No. 2:20-cv-7672) (claiming Trump's ban on TikTok as an overreach of the president's authority and a violation of the company's First Amendment right to free speech). *See* Yaffe-Bellany & Pettersson, *supra* note 9 (reporting TikTok's willingness to strike a deal with a U.S. business and Trump's preliminary approval of an Oracle agreement).

[104] *See Order Regarding the Acquisition of Musical.ly by ByteDance Ltd*, THE WHITE HOUSE (Aug. 14, 2020), *archived at* https://perma.cc/EY6S-FMW7 (ordering TikTok to divest in the U.S.). *See generally* Kate Cox, *Everything we know so far about Oracle not actually buying TikTok*, ARS TECHNICA (Sept. 21, 2020) [hereinafter Cox, *Everything we know*], *archived at* https://perma.cc/8TKM-8LPL (discussing the Oracle and Wal-Mart deal). About 40% of ByteDance itself is held by U.S. investors. *Id.* Supporters of the proposed Oracle deal claim that ownership would translate to about 53% of TikTok's new U.S.-friendly formation, TikTok Global, being held by U.S. investors, thus giving the U.S. majority control. *Id.*

extended TikTok's U.S. takeover deadline, and the federal court in Washington granted an injunction to suspend the ban, TikTok's updated security framework and takeover proposal stalled due to the White House's failure to pursue a final judgement on the ban past the final deadline.[105] Despite the media attention TikTok's U.S. ban received, the app's dominance over the global market may be at an even greater risk considering its heightened supervision and looming penalties for misusing children's data.[106]

ByteDance clarified that not only is Oracle not getting its core assets, but Oracle is also not gaining control of the company; TikTok Global would create a wholly owned subsidiary where Oracle would only have the authority to check the source code of "TikTok USA" for security reasons. *Id.* Trump approved of the deal "in concept," and Chinese experts classify the deal as reasonable, leaving CFIUS to approve the deal. *Id.*

[105] *See* Kate Cox, *Trump admin puts a hold on TikTok ban it seems to have forgotten about*, ARS TECHNICA (Nov. 12, 2020) [hereinafter Cox, *Trump admin*], *archived at* https://perma.cc/6W6Z-PQZS (reporting that the deadline passing with no enforcement is a tacit admission that the proposed ban is not actually particularly important to the Trump Administration any longer). The Department of Commerce stated the orders against TikTok are on hold "pending further legal developments" in multiple lawsuits. *Id.* While ByteDance has not divested any portion of TikTok yet, it does have a deal of sorts in place with Oracle that the White House seemed more or less content with after it was announced in September. *Id. See* David McCabe, *TikTok Is Poised to Outlast Trump, and to Test Biden*, THE N.Y. TIMES (Jan. 15, 2021), *archived at* https://perma.cc/MP2D-BF5C (mentioning the stalled Trump battle against TikTok and the likelihood of Biden rescinding the executive order and commanding ByteDance to sell the app). *See also* Mike Isaac, *U.S. Appeals Injunction Against TikTok Ban*, THE N.Y. TIMES (Oct. 8, 2020), *archived at* https://perma.cc/AZM8-PXPQ (reporting the government's decision to appeal the injunction, which delayed TikTok from being banned in U.S. app stores, further escalating the battle between the White House and ByteDance).

[106] *See* Giles, *supra* note 94 (calling on all social media apps, including TikTok, to provide more transparency displaying their data-collection practices). *See* Kitty Donaldson et al., *TikTok Faces Government Restrictions on U.K. Expansion Drive*, BLOOMBERG (Aug. 26, 2020), *archived at* https://perma.cc/2ZFQ-5ETM (noting that U.K. restrictions on TikTok possibly occurring in the near future as Boris Johnson's party looks to stunt TikTok's reach into their country). *See also* Kristin L. Bryan et al., *Election 2020: Looking Forward to What a Biden Presidency May Mean for Data Privacy and Data Privacy Litigation*, NAT'L L. REV. (Nov. 12, 2020), *archived at* https://perma.cc/7KWF-UJ38 (referencing the Biden Administration's likely path forward with data privacy legislation given Vice President Kamala Harris's part in pushing forward California's efforts to manage state residents' data protection). "For obvious reasons, one of the main priorities of the Biden Administration will be to revitalize the U.S. economy. This priority will run up against global data privacy considerations, however, in light of developments" in late 2020. *Id.* "Many

C. TikTok Conflicts with Data Regulations

Potential violations of far-reaching privacy regulations such as GDPR, COPPA, and CCPA prompted numerous investigations into TikTok's data-collection practices, sparking nations worldwide to question TikTok's intentions.[107] Notably, in 2019, TikTok settled for $5.7 million dollars with the FTC over accusations that the company's app violated COPPA by illegally collecting personal information from children under the age of thirteen.[108] The FTC investigation was prompted by various news reports, claiming that even in a cursory review of the app, the FTC found a large portion of users under the age of thirteen, as well as numerous cases where parents were not notified or asked for permission.[109] It is important to note that COPPA regulates websites that either target children under thirteen or have actual knowledge that children under that age are using their services, compelling such website providers to obtain parental consent in order to safely process personal data of younger children.[110] Additionally, TikTok is currently dealing with multiple class action lawsuits concerning similar issues, one of which recently settled for $1.1

observers have also predicted that the Biden Administration will re-establish a cybersecurity coordinator position within the White House." *Id.*

[107] *See* Jennifer Hassan & Ruby Mellen, *It's not just the United States: These governments also see TikTok as a problem.*, THE WASH. POST (Sept. 18, 2020), *archived at* https://perma.cc/R3NV-4JB4 (listing the countries investigating and considering bans on TikTok).

[108] *See* Complaint of Civil Penalties, Permanent Injunction, and Other Equitable Relief, United States v. Musical.ly, Corp., C.D. Cal. R. (Feb. 27, 2019) (No. 2:19-cv-1439) (claiming TikTok's business practices violate COPPA). *See* Cecilia Kang, *F.T.C. Hits Musical.ly With Record Fine for Child Privacy Violation*, THE N.Y. TIMES (Feb. 27, 2019), *archived at* https://perma.cc/6UNX-9CG9 (claiming the settlement as a record fine for child data privacy violations and reminding all online and service providers the FTC's lack of tolerance for COPPA violations).

[109] *See* Kang, *supra* note 108 (recounting the ease in which the FTC determined TikTok's inactivity in regulating the age of its U.S. users). The FTC claimed that when some parents asked to have the data of their children deleted, TikTok deleted a child's account but retained videos and personal account information about those users on its servers. *Id.* After the settlement, TikTok instituted its restricted version of the app for thirteen-year-olds and implemented parental controls for users' parents to moderate accounts. *Id.*

[110] *See* Milkaite & Lievens, *supra* note 7, at 10 (stating that COPPAs strict regulation over younger age groups led global social media companies, such as Instagram, Snapchat, Facebook, and Google, to exclude the use of their services by children 13-year-old or younger in order to avoid having to obtain parental consent).

million dollars.[111] TikTok's public response to both settlements resulted in a bi-yearly transparency report, as well as the creation of a U.S. restricted-mode, announcing updated default settings for children under the age of eighteen and parental locks aimed towards shifting the liability of children's TikTok activity to their parents.[112]

CNIL, the French "watchdog" investigating TikTok for GDPR compliance, claimed that its investigation was complaint-triggered, probing issues related to data transparency, users' data access rights, transfers of user data outside the E.U., and the app's inadequate steps taken to ensure the data of minors was protected.[113] Furthermore, the

---

[111] *See* Blake, *supra* note 1 (stating that a coalition of child privacy protection advocacy groups filed a complaint with the U.S. Federal Trade Commission against TikTok). In May of 2020, a bipartisan group of senators urged the FTC to investigate the "collection and processing practices" of companies that market to children on the internet as it reviews the COPPA rule to ensure privacy safeguards are effective for kids online today. *Id.* Pleaded by U.S. senators, the urgency to review the COPPA rule received support from the argument believing that "children are a uniquely vulnerable population that deserve heightened privacy protections," and that "the FTC should take extreme caution not to weaken – either purposefully or inadvertently – privacy protections under COPPA." *Id. See* Chris Mills Rodrigo, *TikTok settles with Illinois family over children's data case*, THE HILL (Dec. 5, 2019), *archived at* https://perma.cc/YL4S-YT7P (noting that as a part of the Illinois settlement, a fund of $1.1 million was created to be distributed to the claimants, with each getting an estimated $10). *See also* Charlie Gasparino, *TikTok faces claim for billions in London child privacy lawsuit*, FOX BUS. (Apr. 20, 2021), *archived at* https://perma.cc/Z4E6-UNY7 (alleging that TikTok violated UK and European Union data protection laws by processing youngsters' data without adequate security measures, transparency, the consent of guardians, or legitimate interest). Anne Longfield, the former Children's Commissioner for England and so-called "litigation friend," or public face, of an anonymous 12-year-old girl leading the class action, alleges that every child that has used TikTok since May 25, 2018, may have had private personal information illegally collected by ByteDance through TikTok for the benefit of unknown third parties. *Id.*

[112] *See TikTok Transparency Report 2019 H2*, *supra* note 96 (offering government compliance statistics and deleted material at the request of users, including underage user posts). *See* Thorpe, *supra* note 67 (reporting that TikTok will split users into age-appropriate TikTok environments, in line with FTC guidance for mixed audience apps, where younger users will not be permitted to share personal information and places limits on content and user interactions). The two lessons to be learned from the $5.7 million fine is that companies should take extra steps to be more careful when dealing with children's data, and parents should not assume that the app will protect their children's data or keep their profile private. *Id.*

[113] *See* Lomas, *supra* note 95 (stating TikTok's compliance with the GDPR as a top priority and that it was aware of CNIL's investigation and was fully cooperating with them). Previously, CNIL successfully fined Google $57 million dollars, imposing GDPR fines of up to 4% of a company's annual revenue. *Id.*

ICO's ongoing TikTok investigation in the UK focuses on available child transparency and safety tools, the messaging system which allows adults to text children, and the app's general standards of child data processing, displaying a collective concern for TikTok's use of children's personal information on a global scale.[114] Similarly, Dutch market research and information group SOMI believes TikTok's public response to the accusatory findings of EU privacy watchdogs was insufficient, failing in its obligation to protect children who regularly use its service and likely violating the GDPR.[115]

Recently, the Italian Data Protection Authority ("Italian DPA") has also brought forth comprehensive proceedings against TikTok, announcing its urgency to initiate a formal proceeding against the social networking app after an Italian investigation began in March of 2020.[116] The Italian DPA found that TikTok paid poor attention to the

[114] *See* Milkaite & Lievens, *supra* note 7, at 11 (discussing the ICO's efforts to protect children's data by enforcing GDPR and a consultation code of practice design for children accessible apps to utilize). *But see* Donaldson, *supra* note 106 (claiming regulators across Europe have opened probes into TikTok, but politicians appear to be in no hurry to ban it). "France has no plans to do so, and [n]either does Germany, according to spokespeople for their respective governments." *Id.*

[115] *See* Alex Scroxton, *TikTok's GDPR compliance probed amid accusations of data misuse*, COMPUTER WEEKLY (Aug. 21, 2020), *archived at* https://perma.cc/NV5H-ZMJ6 (quoting SOMI claiming that the only way to build a strong claim against TikTok and its violative data-collection practices is to conduct thorough research). In the past, TikTok spokespersons have highlighted the importance of parental control on the app, shifting the responsibility to protect children onto the parents and away from TikTok. *Id.* "SOMI's principle complaint is that TikTok was warned [in 2019] that children are not being adequately protected against online contact with adults who are not known to them, and that parental supervision of the service may be 'wholly insufficient.'" *Id.*

[116] *See Tik Tok, a rischio la privacy dei minori: il Garante avvia il procedimento contro il social network* [*TikTok Endangers Children's Privacy: Italian Dpa Initiates Proceedings Against the Social Network*], GARANTE PER LA PROTEZIONE DEI DATI PERSONALI (Dec. 22, 2020) [hereinafter *TikTok Endangers Children's Privacy*], *archived at* https://perma.cc/Q99T-P393 (claiming that the information issued to TikTok users is standardized and does not take into specific consideration the situation of minors, while normally, it would be necessary to create a special section dedicated to children, written in a simpler language, and with alert mechanisms that report the risks to which they are exposed). TikTok's data retention times are indefinite with respect to the purposes for which it is collected, similar to the anonymization methods that the social network claims to apply. *Id.* The same lack of clarity concerns TikTok's transfer of data to non-E.U. countries, since those to which the company intends to transfer data are not specified, nor is the adequacy of such transfer indicated. *Id. See also* Melody M. Terras & Judith Ramsay, *Family Digital Literacy Practices and Children's Mobile Phone Use*, FRONTIERS IN PSYCH.

protection of children by continuing to implement (1) signup mechanisms that do not protect children adequately, (2) easy-to circumvent signup restrictions for kids, (3) poor transparency and clarity in user information, and (4) unfriendly privacy default settings.[117] The CCPA has also been cited in at least one class action suit, which was consolidated with several other lawsuits in a multi-district lawsuit in September 2020.[118] In response to TikTok's growing global and U.S. privacy concerns, data privacy experts expect to see more U.S. states adopting stricter privacy regulations to protect their own state citizens, potentially fast-tracking a spiral of ongoing litigation over privacy rights in the U.S.[119]

IV. Analysis

A. The Importance of Protecting Children's Data Privacy

At its core, the protection of children's online data stems from a simple risk: vulnerability.[120] In today's modern digital age, children spend increasingly more time on digital devices with each passing year, subjecting themselves to a flood of online activity and near limitless information.[121] Although the potential risks of such

(Dec. 23, 2016), *archived at* https://perma.cc/EX7Z-7SSX (balancing the importance of a children's digital literacy development with parenting).

[117] *See TikTok Endangers Children's Privacy*, *supra* note 116 (noting how TikTok pre-sets the user's profile as "public," allowing maximum visibility to the contents published therein). *See generally* Fox, *supra* note 91 (responding indirectly to the Italian DPA's concerns with TikTok's protection of children's data, proposing solutions that mirror the privacy-related shortcomings outlined by the Italian DPA).

[118] *See* Marisol C. Mork et al., *The California Consumer Privacy Act ("CCPA") - 2020 Year in Review*, SQUIRE PATTON BOGGS (Dec. 22, 2020), *archived at* https://perma.cc/5JQ5-N64L (recapping developments in the CCPA throughout 2020 and TikTok's class action lawsuits that were merged with an Illinois class action lawsuit to include over 30 plaintiffs).

[119] *See* Blake, *supra* note 1 (noting that although the FTC can fine up to $42,350 per violation under COPPA, the CCPA poses a "pretty significant motivation for states to bring their own actions.").

[120] *See* Haber, *supra* note 1, at 1215 (stating that under this datamining-by-default paradigm, constant surveillance could be direr for some vulnerable populations more than others).

[121] *See* Park, *supra* note 18, at 324 (showing how many five-to-eight year-olds have smart devices and how 84% of children eight or under have used a mobile device; amongst other examples, it is evident that children seem to like mobile devices just as much as or even more so than adults do). *See also* Elvy, *supra* note 17, at 438

engagement are discernible, the importance of fostering online competency, self-expression, and social development are fundamental building blocks for navigating a digital landscape.[122] Through online activity, children have the ability to freely explore their identities and search out their interests, participating in a wide array of social networks and adjusting to the norms of a technologically reliant society.[123] However, there is a caveat to such exploration.[124] Whether it be a lack of experience, know-how, understanding, or a combination of the three, children may not grasp the value of privacy at younger ages, making youth a demographic susceptible to exploitive data-collection methods.[125] Without regulatory guard rails, a child's free exploration in a digital landscape can quickly lead to manipulative data mining, online addiction and overuse, interaction with dangerous

(discussing how IoT devices collect large amounts of health-related data about children, including a biometric-tracking onesie for babies that monitors sleep patterns and an IoT pacifier that can track an infant's temperature). *See* Milkaite & Lievens, *supra* note 7, at 5 (claiming that 1-in-3 internet users worldwide is a child and "online" at increasingly younger ages).

[122] *See* Park, *supra* note 18, at 345 (offering the moral argument for protecting privacy, adding that there is something inherently valuable and precious about privacy that we attribute it as a basic standard for what it means to be human). The legal argument for children's privacy is both a constitutional and statutory right, derived from a reading of the Fourth Amendment, and expanded to modern times to include data privacy as a protectable search under the Constitution. *Id.* at 344. *See* Haber, *supra* note 1, at 1212 (discussing the importance of including children into the IoT, as it may become inventible for them to make use of IoT devices).

[123] *See* Milkaite & Lievens, *supra* note 7, at 7 (noting the importance of the right to receive information and be heard as pre-requisites for children's online participation; rights closely associated with development, human autonomy, sense of control, and choice).

[124] *See* Feldman & Haber, *supra* note 36, at 215 (stating that the ease of conveying information to websites, especially those directed at children, has made the protection of children's information more relevant and crucial than ever before – leading to COPPA).

[125] *See* Park, *supra* note 18, at 342 (discussing how children do not fully understand complicated business or advertising functions or their exposure to potential future risks online). *See* Finnegan, *supra* note 32, at 829 (highlighting concerns about children's weakened ability to understand the harms of providing personal information to third parties through the internet and about children being less privy to marketing techniques and more susceptible to the tactics of online marketers and their deceptive trade practices). *See also* Elvy, *supra* note 17, at 447 n. 126 (quoting, "it is simply too easy for advertisers to obtain the personal information of children for marketing purposes"). "Given the rapid level at which technology is evolving, there may be risks associated with the collection and disclosure of consumer data that consumers may never become aware of or fully understand." *Id.* at 448–49.

individuals, exposure to graphic content, and will likely reinforce harmful habits of neglecting one's own privacy.[126]

Consequently, the difficulty associated with regulating children's data concerns how to best balance children's privacy and protection without stunting their digital literacy.[127] Although there is no concrete solution for this balance, an effective way to moderate a child's online behavior, data output, and presence within the IoT is to promote the guidance of parental oversight.[128] Requiring parental consent for a child's data to be processed is a key aspect of emerging data privacy law, allowing parents to protect the vital interests of their child however they see fit with little to no government intervention.[129] Nevertheless, even with parental consent requirements in place,

---

[126] *See* Milkaite & Lievens, *supra* note 7, at 8 (touching on the significant concerns associated with children's data aggregation).

> A significant concern relates to the potential impact of data aggregation, profiling, and automated decision-making processes. These techniques, which are very difficult to monitor and challenge, capture specific details about children's lives and may "sort" children in certain categories and attribute them a certain "profile". This may lead to a situation where children are stuck with a certain profile and experience opportunities, suggestions, information and choices *within* that profile *only* without having the opportunity to receive information which an algorithm would consider uninteresting or irrelevant to that particular child, thus, hindering the child's development and opportunity to experiment throughout.

Id. *See also* Kumar & Prabha, *supra* note 4, at 76 (concluding that psychological-neurobiological models have shown that addiction to social networking sites involves an interaction of sensitized reward processing and cue-reactivity with diminished prefrontal inhibitory control, indicating when an addicted adolescent would not refrain from posting sensitive videos largely from the desire to get viewed).

[127] *See* Feldman & Haber, *supra* note 36, at 199 (offering that protecting privacy in the law always necessitates rethinking sectoral approaches to regulation altogether, but before doing so, policymakers must carefully balance the legitimate interests of IoT companies and users).

[128] *See* Talley, *supra* note 28, at 146–47 (stating that obtaining "verifiable consent" from a parent means to make a reasonable effort to ensure that, prior to collecting information about a child, a parent of the child receives notice of the website or service's collection, use, and disclosure practices of personal information, and that the parent authorizes the use of the personal information).

[129] *See* Haber, *supra* note 1, at 1245 (articulating the IoT necessitating some form of legal intervention for children's protection, but that the solution to online issues of care, custody, and control, are left to caregivers, and thus parents are a crucial way to responsibly protect children).

massive amounts of data can still be gathered from unassuming minors through various means.[130] Whether it be a child lying about their birthdate, imitating their parent's consent, or struggling to read a confusing privacy policy, the shortcomings of current regulatory law reveal dangerous gaps in the standards we use to protect children's data; and more specifically, question whose responsibility it is to ensure such gaps are eliminated.[131]

B. TikTok's Responsibility as a Data Collector

Social media companies account for vast amounts of personal data-collection, which allows them to store, process, and sell data to third-party brokers for immense amounts of profit.[132] By design, every social media company participates in gathering personal information, so it is important to note that TikTok's data-collection is not entirely different or any less questionable than the common practices of

[130] *See id.* (addressing that "[w]hile parents are accustomed to guarding their children from risks that might arise from television and other familiar media, the internet can result in a "regulation gap" between parental willingness and parental competence. Adding a layer of IoT to the mix only broadens this gap."). *See* Talley, *supra* note 28, at 142 (suggesting, as a solution, that controllers take proportionate approaches to ensuring that users are receiving parental consent by considering "low risk" and "high risk" processing to require more or less information from the parent ranging from a simple email address to a nominal payment linked to a bank transaction).

[131] *See* Park, *supra* note 18, at 339 (commenting that children may simply lie about their age online, which research shows is a common practice among children). "[A]lthough COPPA requires parental consent before collecting certain personal information from children, data collectors or deceptive advertisers may still use complicated and confusing legalese in their policies to confuse lay people who are not familiar with complex privacy policies." *Id.* at 339. *See also* Milkaite & Lievens, *supra* note 7, at 10 (evaluating the privacy policies of Instagram, TikTok, and Snapchat on whether they present information in a concise and intelligible manner according to article 12 GDPR and whether they provide all items of information that are required on the basis of article 13 and 14 GDPR). *See also* Finnegan, *supra* note 32, at 835 (outlining that kids will often lie about their age—often with parental consent—to create an account). The reality of age misrepresentation undermines the suggestion that simply asking for a user's age and accepting the user's response is sufficient for COPPA compliance. *Id.* Despite frequent age misrepresentation, the FTC has not challenged this practice. *Id.*

[132] *See* Elvy, *supra* note 17, at 435 (stating that it was estimated that by 2020, companies would be able to earn more profits transferring and disclosing IoT data than by selling IoT devices to consumers); *see also* Dean, *supra* note 8 (noting the 3.81 billion people using social media worldwide in 2020, continuing to grow and source data from users).

Facebook, Instagram, Snapchat, Twitter, or other media giants.[133] But when considering a combination of TikTok's rapid and recent success, frequent investigations, lack of internal transparency, numerous settlements, and concerningly high rates of U.S. users barely meeting the app's minimum age, TikTok's history displays a rarity within the social media industry.[134] TikTok is one of the only major social media sites in recent history to have been publicly targeted by regulatory enforcement agencies around the world, violating COPPA and likely facing steep fines from the GDPR in the near future.[135] Within the U.S., TikTok's main demographic of younger users necessitates a greater responsibility when collecting their data, a responsibility TikTok has been slow to conform to, but began to take more seriously after an influx of high-profile investigations were launched.[136]

---

[133] *See* Milkaite & Lievens, *supra* note 7, at 15 (noting the similarities in data gathering practices, given the information available to the public, between Snapchat, TikTok, and Instagram, touching on the lack of transparency between the three and the lack of details provided on the exchange of users' information); *see also* Fowler, *supra* note 6 (stating, "[i]t doesn't appear that TikTok takes more data than Facebook but [it] do[es] take measures to hide what [it is] collecting."). *See also* Matsakis, *supra* note 72 (offering, "Today, Google and Facebook can target ads based on your name—exactly what people feared the digital ad giant DoubleClick would do two decades ago."). Large companies like Amazon, Apple, Facebook, and Google are banding together to push hard for federal digital privacy legislation, racing to supersede the CCPA law with more industry-friendly federal legislation. *Id. See also* Atamaniuk, *supra* note 13 (showing the percentage of data gathered by each company in the tech-industry, with Facebook, Instagram, Tinder, Grindr, Uber, and others gathering the most by far, and TikTok gathering very little in comparison).

[134] *See* Giles, *supra* note 94 (portraying the wider data processing concerns associated with TikTok above other media sites). *See* Zhong & Frenkel, *supra* note 15 (displaying the alarming amount of U.S. users under the age of thirteen, raising questions whether the company is doing enough to protect them). Even though a majority of U.S. users are likely under the age of thirteen, other countries reflect similar age demographics: in Britain, the share of daily users who were classified as fourteen or younger was around 43% this spring, in Germany, the share was more than 35%, and in France it was 45%. *Id.*

[135] *See* Waters, *supra* note 4 (citing TikTok's various privacy lapses as Musical.ly, settlements with COPPA, and a slew of lawsuits around the U.S.). *See* Donaldson, *supra* note 106 (referencing regulators across Europe that have opened probes into TikTok). *See also* Chesney, *supra* note 14 (mentioning CFIUS's investigatory review and the U.S. IEEPA executive orders). *See generally TikTok Endangers Children's Privacy*, *supra* note 116 (stating the recent complaints and inadequate data processing methods that TikTok is being investigated on by the Italian DPA).

[136] *See* Fox, *supra* note 91 (reflecting on the multiple investigatory complaints and offering TikTok's solution to protect its minor users). *See* Zhong & Frenkel, *supra* note 15 (citing in July of 2020, TikTok classified more than a third of its 49 million

While it may seem simple enough to blindly label TikTok as an ill-intentioned social media company preying on the lucrative data of vulnerable consumers, its responsibility to protect its users only goes as far as the law requires.[137] Consequently, the red flags concerning its questionable data-collection practices exist as a symptom of a larger policy issue, and its past transgressions set a clear example of where the U.S.'s regulatory limit exists in the current day and age.[138] By demonstrating how to operate within the deficits of U.S. data privacy regulation, TikTok unintentionally exposed how to determine what behavior simultaneously abuses children's vulnerabilities as data subjects while following legal guidelines.[139] Ethically, as a leading social media app popular amongst younger users, TikTok should be setting a strong example for similar sites; ideally, taking a stand against common invasive data-collection practices and forwarding technology to protect children on its app.[140] Instead, TikTok's actions set a far different precedent by pushing

daily users in the United States as being fourteen-years old or younger, according to internal company data and documents that were reviewed by the *New York Times*).

[137] *See* Waters, *supra* note 4 (claiming that it is fundamental to a privacy compliance program to follow applicable federal and state law, and after TikTok's failure to comply with data deletion requests under COPPA, it bears repeating that websites who serve children must comply with COPPA). "Further, complying with applicable privacy laws means the often-burdensome effort of keeping up with a rapidly evolving body of law." *Id.* This includes the CCPA, state data breach notification laws, and updating proposed privacy legislation. *Id.*

[138] *See* Finnegan, *supra* note 32, at 844–46 (placing TikTok and its regulatory violations within the scope of a larger data privacy issue online, including the implications on other popular media sites such as Facebook and YouTube).

[139] *See* Fowler, *supra* note 6 (concluding that there is a hole in our ability to verify all of what TikTok does because TikTok's app uses some technical measures to encode its activity, meaning some of it is hidden from independent researchers looking under the covers). "TikTok's privacy policy leaves a door open to responding to government requests — without specifying which governments. It reads: 'We may disclose your information to respond to subpoenas, court orders, legal process, law enforcement requests, legal claims, or government inquiries.'" *Id.*

[140] *See* Milkaite & Lievens, *supra* note 7, at 17 (concluding that "[i]t is time for service providers to make sure privacy policies reach their actual audience, including (young) children, and to invest in innovative ways to offer information, which may in the end lead to enhanced trust relationships with their users."). "An important guarantee for reaching this goal is actually including children in information design and evaluation processes." *Id.*

regulatory limits and gambling its exponential growth on its ability to endure the costs of violating data privacy law.[141]

C. TikTok's Demonstration of the Need to Heighten U.S. Children's Data Protections

TikTok's ongoing friction with the GDPR, COPPA, and CCPA indicates a universal need for strong data privacy policy, but the differences in enforcement, key provisions, and effectiveness between each regulatory act results in vastly different levels of protection for children.[142] The GDPR is a strong privacy bill that provides special protections for children's data, requiring children ages fifteen and younger to receive authorized consent from a parent to allow their data to be processed.[143] In addition, the GDPR includes provisions necessitating "kid-friendly" privacy policies, reasonable efforts to verify the age of the minor, and automated data processing conditions, ultimately aiming for a more transparent and safe online environment for children.[144]

---

[141] *See id.* (providing, "[t]he analysis of privacy policies of Instagram, Snapchat and TikTok shows that there is much room for improvement for moving from text based, long policies to more engaging formats and understandable language adapted to different ages of users.").

[142] *See* Green, *supra* note 33 (comparing the differences between E.U. and U.S. privacy laws, as well as various state data privacy laws). *See also* Finnegan, *supra* note 32, at 852 (noting that "[t]he GDPR requires that any data-collection of a user under sixteen must be with parental consent or authorization, and Facebook, Inc. currently allows users between thirteen and sixteen on its website.").

> [U]nless Facebook, Inc. effectively locks all European accounts of users under sixteen, it must necessarily implement protocols that would be COPPA compliant in an effort to comply with the GDPR, as this mandate is more inclusive than the mandates in COPPA. As Facebook, Inc. is tailoring its practices to conform with the GDPR, there is no reason why it should not simultaneously address the gaps in its COPPA compliance.

Id.

[143] *See* Talley, *supra* note 28, at 140 (distinguishing that under the GDPR, if a child is younger than the age of sixteen, processing may be lawful "only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child."). *See* Finnegan, *supra* note 32, at 852–53 (recognizing that the GDPR is a strong start and that it has taken measures to provide individuals with stronger protections and control over their privacy rights and personal data).

[144] *See* Nicole O., *supra* note 29 (noting the inclusion of Recital 58 in the GDPR that reads "Given that children merit specific protection, any information and communication, where processing is addressed to a child, should be in such a clear

Although the GDPR may control the behavior of every major international data processor, its effect on U.S. citizens is largely indirect.[145] TikTok has a separate privacy policy for E.U. citizens to specifically conform to the standards of the GDPR, opting to keep a less transparent privacy policy for U.S. users.[146] Yet, investigations from the CNIL, Italian DPA, SOMI, and other E.U. watchdogs are adamant that TikTok's data processing methods and privacy policy still lack transparency; a gap in data privacy protection that can be closed off through proper investigation and GDPR enforcement.[147] TikTok's data privacy standards, even at their most strict under the GDPR, are evidently questionable and subject to scrutiny.[148]

---

and plain language that the child can easily understand."). "In addition to requiring advanced consent measures, the GDPR says you cannot subject their data to automated processing or profiling." *Id.*

[145] *See* Finnegan, *supra* note 32, at 852–53 (recognizing how Facebook, a U.S. social media company, is tailoring its practices to conform with the GDPR, informing its COPPA compliance as well). The GDPR applies to all companies or organizations that offer goods or services to, monitor the behavior of, or process or hold the personal data of E.U. data subjects. *Id.* at 852 n.175.

[146] *See* Milkaite & Lievens, *supra* note 7, at 13 (recognizing that TikTok has a separate privacy policy for E.U. residents).

[147] *See* Scroxton, *supra* note 115 (recounting the Amsterdam based non-profit organization advocating for data privacy and consumer issues in the Netherlands targeting TikTok). *See also TikTok Endangers Children's Privacy*, *supra* note 116 (criticizing TikTok's failure to adequately protect children after the easily circumvented age restriction is passed by simply lying). *See also* Tan, *supra* note 95 (noting that the TikTok-Musical.ly merger united the world's largest short-video apps, but TikTok did not seek clearance from CFIUS, likely because it did not perceive an obvious link to American national security, which is the basis for triggering CFIUS reviews). *See also* Schulze, *supra* note 95 (quoting the head of the UK's ICO, detailing the authority's focus on transparency tools for children, messaging systems, video sharing, and an active investigation into TikTok).

[148] *See* Talley, *supra* note 28, at 155 (offering that the GDPR could better protect children by implementing a system for screening online service users to ensure that data is not collected about children inappropriately or without the knowledge of the child, caretaker, or the service provider).

> While web services engaging in these direct marketing techniques are strongly encouraged to ensure children's data is specifically protected and that children are fairly informed about the ways in which their data could be used, the GDPR could better protect children if the governing bodies enforce stricter compliance with the Regulation.

Id. at 152. "Despite the GDPR's aims to harmonize data privacy laws across Europe and provide those who process data a simple framework to adhere to, the lack of a uniform age of consent affects children and businesses." *Id.* at 153.

Additionally, TikTok's attempt to publicize its latest "commitment to protecting younger user's privacy" shows that it is aware of the ethical doubt it garnered, publicly reflecting on its shortcomings and updating its default settings for minors; changes that were specifically cited by the Italian DPA investigation.[149] The shift in default settings is a strong step for TikTok's online safety, but should serve as an even stronger illustration for data privacy policymakers to consider regulating default application settings and user interconnectivity.[150] TikTok's changes in its default settings were a result of the combined pressure from the GDPR investigations and previous COPPA fines, but were never explicitly controlled by either data privacy act.[151] By improving default safety and accountability settings on apps like TikTok, data-collection can be more easily monitored, and modern day processors will have less room to operate in the blind spots of the law.[152]

Despite COPPA partially inspiring the conception of the GDPR, it is not nearly as robust on children's data privacy as its E.U. counterpart.[153] COPPA differs from the GDPR in two substantial

[149] *See* Fox, *supra* note 91 (discussing TikTok's commitment to transparency and safe data processing, stating, "We'll continue to evolve our policies, work closely with regulators and experts in minor safety, and invest in our technology and teams so that TikTok remains a safe place for everyone to express their creativity.").

[150] *See* Feldman & Haber, *supra* note 36, at 221 (advocating for the use of an approach termed Privacy by Design ("PbD"): a "systematic approach to designing any technology that embeds privacy into the underlying specification or architecture."). This concept of PbD could be interpreted as calling for structural support for privacy protection and advocating privacy protection by an organization's default mode of operation. *Id.*

[151] *See Data protection by design and default*, *supra* note 20 (summarizing Article 25's default requirements to only necessary personal data, a requirement that does not directly control data collectors from implementing exploitive default settings for minors). Data protection by default requires you to ensure that you only process the data that is necessary to achieve your specific purpose, linking to the fundamental data protection principles of data minimization and purpose limitation; a requirement easily achieved by data controllers on a regular basis by showing a necessary purpose for such collection. *Id.*

[152] *See* Feldman & Haber, *supra* note 36, at 228–33 (distinguishing other potential technology solutions to improve regulation through an always-on era, including methods like data anonymization, encryption, and other privacy mechanisms used to satisfy k-anonymity).

[153] *See* Park, *supra* note 18, at 339 (offering that "despite the FTC's work in implementing COPPA, providing amendments, and enforcing the law, COPPA still has limitations that fail to protect children from devious data collection and marketing ploys.").

ways: it exclusively regulates the data-collection of children in the U.S. and it only protects children under the age of thirteen.[154] Although COPPA set some important trends used in data privacy today, it is often criticized for containing a number of flawed provisions and an unfortunate lack of enforcement.[155] Specifically, a common complaint with COPPA is that the act's scope only goes so far as to protect children under the age of thirteen.[156] Due to COPPA's high toll on violators who process data from underage users, most social media sites opt to avoid COPPA scrutiny entirely by restricting users in that age group from connecting to their service.[157] However, the protection of users under the age of thirteen-years old is far too limited and arbitrary, and should be raised to either match the age constraints of the GDPR at sixteen-years old, or updated with research to reflect a more informed age limit.[158] The high level of risk associated with COPPA violations, and the common practice of companies avoiding thirteen year old's on their sites entirely, indicates the effectiveness of the act if it were to increase the age of those covered.[159]

---

[154] *See* Nicole O., *supra* note 29 (plainly stating the simplified, but key differences between COPPA and the GDPR).

[155] *See* Park, *supra* note 18, at 341 (noting that the FTC's problems in enforcing COPPA partly arise from the fact that until now, the FTC's enforcement has largely been limited to "responding to reported violations and suspicious behavior" instead of focusing more of its energy and time on investigating the apps). Even when the FTC does investigate violations, the process is far too slow and laborious involving manual testing methods. *Id.*

[156] *See* Finnegan, *supra* note 32, at 831 (addressing that most prominently, critics attack COPPA's limited scope by highlighting the fact that the definition of child is limited to those under thirteen-years of age).

[157] *See* Milkaite & Lievens, *supra* note 7, at 10 (explaining that COPPA requires website providers to obtain parental consent in order to legitimately process personal data of younger children, leading global social media companies, such as Instagram, Snapchat, Facebook, and Google, to exclude the use of their services by under 13-year-olds in order to avoid having to obtain parental consent).

[158] *See* Finnegan, *supra* note 32, at 831 n.36 (commenting "[A]ge thirteen appears to have been selected arbitrarily and developmentally illogically . . . using the age of thirteen . . . creates an irreconcilable conflict with the minority doctrine in contract law.").

[159] *See* Haber, *supra* note 1, at 1231 (considering how COPPA must be revisited and recalibrated to meet the challenges the IoT raises and its differences that need to be addressed since the evolution of the internet). "COPPA, for example, must promote awareness of caregivers to the risks of datafication, increase oversight and accountability on obtaining verifiable consent for the use of these devices, and adhere to stricter data minimization, and transparency requirements." *Id.*

In addition, modern technology connected to the IoT largely falls outside the scope of COPPA, with smart devices such as phones and tablets allowing children to access TikTok without COPPA considering such IoT devices as "child specific" targeted appliances.[160] Fortunately, the FTC has made it clear that TikTok substantially targets children as its audience, evident in the $5.7 million fine levied against TikTok for knowingly violating the act.[161] Despite the considerable fine, COPPA's plethora of enforcement actions are constrained by its failure to include a private right of action for parents, and relies on the FTC as the sole enforcer for any violations.[162] As a result, the overburdened, underfunded, and understaffed FTC often fails to apply the COPPA Rule it standardized, subsequently allowing data processors to freely benefit from younger data subjects more often.[163]

The CCPA may only impact California citizens, but its widespread influence over the rest of the U.S. has created a new

---

[160] *See id.* at 1232 (contending that recalibrating COPPA only means to meet the challenges of toys in the IoT and that children's datafication might very well continue though devices that fall under the radar).

> In other words, while COPPA might apply to some IoT devices . . . it will fail to apply to many other IoT devices that will effectively be used by children under the age of thirteen. It thus fails to properly protect children against their datafication by various entities. It means that most IoT companies who potentially collect data from children under the age of thirteen and make use of such data are not required to adhere to safeguards that are granted by COPPA, and children are therefore left without legal safeguards for their information privacy.

Id.

[161] *See* Thorpe, *supra* note 67 (recounting TikTok's $5.7 million fine, which required TikTok to have been found as a website or online service that was directed to children and did not obtain parental consent before collecting personal information from children under the age of 13).

[162] *See* Finnegan, *supra* note 32, at 829 (addressing Congress's failure to create a private right of action under COPPA). *But see* Talley, supra note 28, at 146 (adding that COPPA does include a "safe harbor" provision which allows industry groups, if approved by the FTC, to create and implement the Rule's protections in a self-regulatory manner).

[163] *See* Finnegan, *supra* note 32, at 833 (stating generally, FTC's COPPA enforcement remains limited "[B]ecause COPPA grants no private rights of action to parents, enforcement of COPPA is the sole province of the FTC, which is . . . understaffed and overburdened.").

standard for state-run data privacy regulation.[164] Although TikTok's limited interaction with CCPA enforcement could imply its adherence to the California statute, data privacy experts believe that TikTok will likely face scrutiny from the CCPA under the act's inclusion of a parental private right of action.[165] With the further inclusion of the CPRA, the CCPA stands as a rigid model for state and federal data privacy law going forward, comprehensively protecting the rights of children and providing simplified enforcement actions against violators.[166] Additionally, the CPRA expansion extended CCPA fines for those who are collecting and selling information from children under the age of sixteen, following the GDPR's broad scope of protected ages.[167] The CPRA addition will be effective on January 1, 2023, but companies like TikTok will be held accountable for any violations on January 1, 2022, giving such companies ample time to predict, reform, and abide by the California state law.[168] Still, except for a few inconsequential bans, petty fines, and open investigations, TikTok has faced relatively little disciplinary action under the GDPR, COPPA, and CCPA; a phenomena that may not only require a change in the law, but a shift in policy as well.[169]

---

[164] *See* Green, *supra* note 33 (maintaining that with no federal answer to GDPR on the horizon, several other states are taking a page from California's book by drafting their own regulations to give citizens increased control over their personal data; notably, most of these bills using CCPA as a framework).

[165] *See id.* (summarizing that the CCPA also gives consumers a limited right of action to sue if they are the victim of a data breach).

[166] *See generally* Lam, *supra* note 52 (discussing in detail the new provisions included by the CPRA, or Proposition 24).

[167] *See id.* (articulating how the CCPA will now resemble the GDPR's level of threat by broadening liability, raising fines, covering a greater group of ages, and formulating a new administrative agency to enforce the law).

[168] *See id.* (providing a timeline for the CPRA's active application to businesses and their coverage date approaching faster than their enforcement date).

[169] *See* Waters, *supra* note 4 (stating that without admitting guilt, TikTok agreed to settle the FTC privacy charges for $5.7 million and entered into a consent order with the FTC). The amount paid by TikTok is dwarfed by both TikTok's current revenue and the FTC's $5 billion settlement with Facebook, but it was a record settlement for COPPA enforcement. *Id.* Considering the short amount of time since the TikTok settlement, it is not surprising that TikTok is back in the headlines with advocates and regulators alleging its blatant disregard of the consent order, yet no investigations have come to fruition. *Id.*

D. Reforming Policy Standards for TikTok's Collection of Children's Data

TikTok's controversial behavior is reprehensible, but unless a different approach to children's privacy protection is taken, TikTok's ability to exploit the law's vulnerabilities will persist.[170] Fortunately, the U.S. may be able to combat the questionable behavior of companies like TikTok by forming stronger public policy on data privacy and encouraging a social change in attitude towards children's online protection.[171] The first step to properly investigating TikTok is to shift the U.S.'s focus away from the Trump Administration's fixation on the company's Chinese ties and hone in on TikTok's domestic data processing methods.[172] The lack of transparency into TikTok's data-collection, of which is reportedly stored and processed in the U.S., is the largest threat TikTok poses to the U.S.'s safety; not the company's supposed loyalty to China or its presumed obligation to

---

[170] *See* Feldman & Haber, *supra* note 36, at 227 (offering a plethora of solutions to control unregulated entities under federal law). One such consideration hinges on the lack of external incentives for information protection and how market actors' self-regulation is bound to fail. *Id.* at 248.

> There must be some form of incentive for companies to adhere to these requirements. This could be achieved, for example, by obliging private companies to implement these technological measures ex ante in order to begin operating (e.g., by requiring licenses) or ex post (by imposing high fines for noncompliance or data breaches). It could also be achieved by granting a safe harbor from liability lawsuits on the fulfillment of these standards, which will be treated as evidence of compliance vis-a-vis liability or even combining the modalities of social norms and the market to drive consumers to demand that these companies protect their privacy better.

Id.

[171] *See* Haber, *supra* note 1, at 1239 (arguing that "[w]ithout adhering to an omnibus approach as reflected by the GDPR, perhaps the protection of children should rely less on regulation and more on other modalities of regulating behavior, like that of the market, social norms, and technology, either separately or combined.").

[172] *See* Arbel, O'Brien & Ott, *supra* note 9 (quoting Nicholas Weaver, a computer science lecturer at UC Berkeley, who "said the actions taking effect on [September 13, 2020] were short-sighted and suggested that 'the U.S. is not to be trusted and not a friendly place for business.'"). "'If there are direct national security threats, that information should be shared with the U.S. population,' said David Kennedy, CEO of cybersecurity firm TrustedSec, before the Commerce Department's regulations were announced. 'We're not ta[l]king about what needs to happen policy-wise, we're trying to hack this together to hurt China.'" *Id.*

transfer U.S. citizens' data to a foreign government.[173] Although those concerns could be substantial and may be worth an investigation, there is no evidence that such dire circumstances exist or that two separate executive orders were necessary to engage in such a short-sighted ban.[174] Banning TikTok in the U.S. was not an offensive decision, but rather an unsupported, distracting, and lethargic one, stirring up a much needed conversation on data privacy without the proper accountability.[175]

The next step to combat the gaps in U.S. data privacy should be to update social norms to reflect modern technology, providing IoT device users additional awareness into the inner workings of social media networks like TikTok.[176] Social norms are difficult to develop, but the capability of modern technology is not so complicated so as to

---

[173] *See* McCabe, *supra* note 105 (recognizing TikTok's claim that the "national security concerns of the U.S. are unfounded, noting that TikTok's data is stored in the United States with a backup in Singapore."). "While the talks between ByteDance and the government continue in private, TikTok has maintained its lobbying effort to convince government officials they have nothing to fear from the app, which uses the cheery slogan 'Make Your Day.'" *Id.* *See* Arbel, O'Brien & Ott, *supra* note 9 (reiterating that "TikTok says it does not store U.S. user data in China and that it would not give user data to the [Chinese] government, and does not censor videos per dictates from China.").

[174] *See* Fowler, *supra* note 6 (reminding not to excuse China's record of online repression — noting how it is possible that China will force TikTok to change its practices in the future, but for now, the issue comes down to whether users inherently distrust data mining from Chinese-owned companies more than data mining from U.S.-owned ones).

[175] *See* Robertson, *supra* note 102 (providing that the president of the United States cannot just sanction a company like TikTok because he or she is mad at it). Similar to Trump's threats of shutting down Facebook and Twitter, former Director of the CIA Mike Pompeo's discussion of banning TikTok obscures the real limits of U.S. government power, potentially foreshadowing genuinely troubling attempts to limit how Americans can use the internet. *Id.* *See* Cox, *Everything we know*, *supra* note 104 (noting that several Republican senators, including John Cornyn (R-Texas), Josh Hawley (R-Mo.), Marco Rubio (R-Fla.), Rick Scott (R-Fla.), Thom Tillis (R-N.C.), and Roger Wicker (R-Miss.) have all publicly objected to the proposed deal between TikTok and Oracle). "The Senators all urge CFIUS to reject the proposal, arguing that it is insufficient to prevent the national security threat for which a ban or sale was being required in the first place." *Id.*

[176] *See* Haber, *supra* note 1, at 1239 (providing that "[b]oth the market and social norms could potentially reduce the privacy risks of IoT to children . . . [because] [s]uch a scheme would rely mainly on consumer discontent with the practices that IoT manufacturers engage in which risk their children's privacy."). "[U]pon proper understanding of privacy risks, many, if not most, individuals might choose to at least abstain from purchasing devices that might pose a risk to their children." *Id.*

confuse the average consumer.[177] If the U.S. were to encourage operating systems, computers, and other data collecting devices to provide consumers with a clear and simple indication of an app's data-collection frequency and threat level, such notification could act as a buffer for parents to reassess their children's activity on a certain app.[178] This indicator, implemented on technology like tablets, smartphones, game consoles, and computers, could be akin to app-based privacy policies, with the difference being that the hardware manufacturer provides an additional layer of awareness for the user.[179]

---

[177] *See* Lessig, *supra* note 76, at 132–33 (proffering two substantial constraints of regulation, equal to that of the law, are social norm constraints and market constraints). Norms, like laws, punish individuals for violating a rule, but the punishment of the norm is imposed by a community and not by the state. *Id.* at 132. Market constraints are affected through conditions and are not independent of laws or norms, rather, the market imposes simultaneous constraints upon how an individual or group might behave due to a background of property and contract law. *Id.* at 133.

[178] *See* Park, *supra* note 18, at 348 (offering a similar mechanism to raise children's online protection through technology).

> For instance, an expansion of "do not track" mechanisms that have already been implemented by the FTC is one example of such a built-in protection. "Do not track" is a tool that allows consumers to show that they do not want to be tracked. Building this sort of "Privacy by Design" into new software products and services can substantially limit privacy intrusions. Although this may be effective, however, its enforcement will be long and arduous because it would require "industry buy-in" in addition to a regulatory scheme. This means that to legally require this protection to be programmed into software may require an entire restructuring of an industry. Although the FTC expressed its support for the "Do Not Track" program in 2010, it also stated that the agency alone would not be able to execute such a program. Moreover, some well-known websites such as Google and Facebook do not comply with "Do Not Track" requests, claiming that "it is unclear what the users really want" and that sometimes, since the default setting in the browser is to have "Do Not Track" enabled, it might not be clear whether it's the user's actual choice.

Id. at 348–49.

[179] *See id.* (noting that along with the "'do not track' mechanisms, another way to encourage transparency in mobile tracking, and thereby decrease abusive practices by third parties and app developers, is to identify and characterize third-party tracking services."). "Third-party service providers usually use the app permission method to collect information from users." *Id.* at 350. *See* Chen, *supra* note 82 (discussing Apple's bold decision to label apps in their App Store with privacy indicators but noting the heightened burden this puts on app developers and Apple to remain truthful). Although Apple intends to enhance their user's control over their

Whether or not that notification would include a comprehensive analysis of an app's data processing, a green-to-red color scale indicating an app's degree of privacy, or a simple icon flagging an app's collection rate, it's addition would be an appealing safety incentive for parents and would likely influence consumer app usage as well.[180]

Looking forward, the Biden Administration has signaled that it will pursue privacy legislation as a high priority and increase FTC enforcement as well, potentially foreboding trouble for TikTok.[181] Despite President Biden's increased support for data privacy protection and Vice President Harris's extensive history advocating for heightened privacy protections, TikTok will likely face less obtrusive scrutiny from the Biden Administration as opposed to the forthright criticism of Trump.[182] An indirect but effective way for the current

download choices, privacy researchers are not convinced that these labels are likely to be successful in their current form. *Id.* By comparing the privacy labels of apps like Spotify, Apple Music, WhatsApp, Signal, and MyQ, Chen concluded that some apps, which appear identical in function, can vastly differ in how they handle our information. *Id.*

[180] *See* Park, *supra* note 18, at 350 (recommending another option introducing a "whole new model for enforcing uniform privacy policy through something akin to 'nutrition labels.'").

> Yet another option is to introduce a whole new model for enforcing uniform privacy policy through something akin to "nutrition labels." The label would consist of a grid with the label "information we collect" on the vertical axis and "ways we use your information" on the horizontal axis. Each box in the grid would denote a certain type of data and what use that data is put to. Colors can be used to mark whether or not a company collects and uses your data for a specific purpose. This privacy grid would be a viable method to form a uniform privacy policy, because of its simplicity and practicality. It is simple because it removes the arduous task of having lay people reading complicated legalese which often make up a large portion of detailed policies, and practical because the grid allows for an effective and easy way to compare policies.

Id. at 350–51.

[181] *See* Bryan et al., *supra* note 106 (labeling data privacy as an anticipated high priority for the Biden Administration, taking up legal issues involving U.S. surveillance under Section 702 of the Foreign Intelligence Surveillance Act, Executive Order 12333, and the Presidential Policy Directive 28).

[182] *See id.* (noting that although data privacy is a high priority for the Biden Administration, one of their main priorities will be to revitalize the U.S. economy in light of the COVID-19 pandemic). *But see* McCabe, *supra* note 105 (noting how

U.S. administration to tackle the issues surrounding TikTok would be to moderately balance spreading awareness of the app's high security risks while shifting the conversation around its controversy to focus more on domestic privacy concerns.[183] Nonetheless, TikTok's future is still open ended, and although a multitude of major global powers have the social media app in their crosshairs, the U.S. is a significant market that has struggled to keep up with the company's subversive approach to data processing.[184]

V. Conclusion

The rapid advancement of IoT technology demands an equal response from regulatory enforcement agencies to protect children from unchecked data collectors. Although regulations such as the GDPR, COPPA, and CCPA play a major role in safeguarding children's privacy, the gaps in their coverage consistently benefit companies with subversive collection tactics. By preserving outdated methods of governmental supervision and perpetuating stifled enforcement opportunities for children, the U.S.'s ability to limit data collectors is inadequate in the face of the IoT. As a result, TikTok's data-collection practices consistently test the limits of the U.S.'s regulatory regime, frustrating enforcement agencies, citizens, and Trump to no avail. Fortunately, this frustration has led to an increased national concern for the dangers of rampant data-collection, marking the faults of current collection standards and how to address them.

Biden has said little about TikTok or the "broader, bipartisan concerns about the growing influence of Chinese technology companies.").

[183] *See id.* (indicating that TikTok's fate under Biden is far from certain). Biden could either take a hardline approach against TikTok or a softer approach, mitigating U.S. concern indirectly or forcing a sale outright. *Id.*

[184] *See* Bryan et al., *supra* note 106 (analyzing the possibility of a federal U.S. privacy bill in the near future, as conversation surrounding the Setting an American Framework to Ensure Data Access, Transparency, and Accountability ("SAFE DATA") Act and the Consumer Online Privacy Rights Act ("COPRA") raises concerns for data processors around the globe). "Based on the number of state privacy bills that are currently pending, it is conceivable that more than half of the states could enact divergent privacy laws over the next few years." *Id.* It is believed that the Biden Administration will also likely have a significant impact on the FTC's enforcement priorities, as it is anticipated there will be increased FTC enforcement activity. *Id.* "This increased enforcement may have ripple effects in privacy litigation, and with an increase in enforcement, the data privacy landscape for suits involving private parties may also shift." *Id.*

To heighten the responsibility for companies handling children's data, the U.S. must adopt stricter privacy guidelines for companies to adhere to, updating the current law by broadening the scope of protected ages and including stronger actions for enforcement. Similarly, the U.S. should consider developing a stronger public policy on combating harmful collection methods, reinforcing a positive social attitude towards data privacy, and providing tools to educate the public's understanding of the modern privacy landscape. In combination, U.S. regulation and public policy should be quick to adapt to changing trends, updating alongside each IoT advancement with children's privacy in mind. Subversive data-collection may persist throughout the U.S.'s inevitable privacy evolution, but by closely monitoring the behavior of companies like TikTok, the protection of children's data can successfully persevere.