Suffolk Journal of Trial and Appellate Advocacy

Volume 24 | Issue 1 Article 18

1-1-2019

The Fine Line between Identifiers Capable of Identifying and Identifiable Information

Aleksandra Popova
Suffolk University Law School

Recommended Citation
24 Suffolk J. Trial & App. Advoc. 255 (2018-2019)

THE FINE LINE BETWEEN IDENTIFIERS CAPABLE OF IDENTIFYING AND "IDENTIFIABLE INFORMATION"

I. INTRODUCTION

Most people do not understand the depths at which the Orwellian reality has materialized in today's highly digitalized world, by way of both continuously advancing "smart" technology and an ever-increasing need to be "connected."[1] The "internet of things" aims to create one swift motion through various means of being connected all working in tandem to accomplish a single lucrative goal: "capturing data that can then be used to measure and control the world around us" in order "to permit the user to accomplish commercial transactions with as little conscious thought as possible. . . ." because data explains "[t]he fewer steps there are in a transaction, the more likely people are to spend their money."[2] Though these devices appear harmless, the problem arises due to their "vacuuming up [of] information. . . ."[3] It is difficult to conceptualize the sheer volume of such Personally Identifiable Information ("PII"),[4] which is constantly being

---

[1] *See* Adam Greenfield, *Rise of the machines: who is the 'internet of things' good for?*, GUARDIAN.COM (June 6, 2017), https://www.theguardian.com/technology/2017/jun/06/internet-of-things-smart-home-smart-city (warning people to be skeptical and resist tracking as "internet of things" presents new possibilities). Greenfield explains "the internet of things" are a number of connected devices and services capable of gratifying and delivering convenience whether in the form of services for people, referred to as "quantified self," our homes, referred to as "the smart home" or public spaces, referred to as "the smart city." *Id.* He calls this process "the colonisation of everyday life by information processing." *Id.*

[2] *See id.* (discussing demand for instant gratification). The goal being a monetary one, it aims ". . . . to short-circuit the process of reflection that stands between having a desire and fulfilling that desire by buying something." *Id.*

[3] *See id.* (arguing that users do not know what is done with their information).

[4] *See Guidance on the Protection of Personal Identifiable Information*, U.S DEP'T OF LAB., https://www.dol.gov/general/ppii (last visited 2019) (quoting Department of Labor's definition of PII). According to the United States Department of Labor, PII is defined as:

> Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. Further, PII is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors). Additionally, information permitting the physical or online contacting of a

collected, analyzed, and packaged from consumers on every platform.[5] "It's not about what we know we're sharing, it's about what we don't know is being collected and sold *about us*."[6] Furthermore, the speed at which PII is being sold and transmitted as a commodity to second or third parties to increase sales without users' direct knowledge is alarming.[7] This collected data can fully identify "who you are on a day-to-day basis" by cataloging anything from simple personal information, such as name, IP address, or income, to who your best friend is, your sexual preference, and medical information relative to your medications or diseases, all in addition to tracking every step, interest, or decision you make along the way.[8] By combining PII and two types of cookies,[9] first and third party cookies, companies reach their ultimate goal: to deliver targeted ads to users in accordance with their specific interests as they surf the Internet, even when using multiple devices, in what appears to be a swift or "seamless" experience.[10] With the help of evolving technologies, companies use "device fingerprinting" to track users across "all kinds of internet-connected devices," such as smart phones, tablets, laptops, desktop computers, and other smart devices, creating the ultimate experience through mobile applications.[11]

---

specific individual is the same as personally identifiable information. This information can be maintained in either paper, electronic or other media.

Id.

[5] *See* Greenfield, *supra* note 1 (summarizing how information is being collected from consumers); *see also* Steve Kroft, *The Data Brokers: Selling Your Personal Information*, CBS NEWS, http://www.cbsnews.com/news/data-brokers-selling-personal-information-60-minutes/ (last updated Aug. 24, 2014) (expounding upon various data being collected through internet and mobile devices).

[6] *See id.* (emphasis added) (discussing monetary gains behind data collection and its effects). This script from 60-minutes broadcast grapples with the idea of privacy and preservation of PII in comparison with the notion of merely accepting the internet as an "advertising medium" over which too much regulation would "cripple" one of the fastest-growing sectors of the United States economy today. *Id.*

[7] *See id.* (explaining collected data generally sold to other companies, marketing and advertising companies and sometimes government).

[8] *See id.* (detailing certain types of information being collected).

[9] Packet of data sent by a server to a browser to identify the user or track their access.

[10] *See* Darla Cameron, *How targeted advertising works*, WASH. POST (Aug. 22, 2013), https://www.washingtonpost.com/apps/g/page/business/how-targeted-advertising-works/412 (explaining concept of targeted advertising); *see also Online Tracking*, FED. TRADE COMM'N (June 2016), https://www.consumer.ftc.gov/articles/0042-online-tracking (answering most commonly asked questions regarding online tracking and cookie software).

[11] *See Online Tracking*, *supra* note 10 (discussing how companies can track users across multiple devices). The Federal Trade Commission ("FTC") also explains that companies use device identifiers, such as Apple iOS's Identifiers for Advertising ("IDFA") and Google Android's Advertising ID, to monitor the different applications on a particular device and collect the device's unique ID, which can later be matched to unrelated PII. *Id.*

Furthermore, companies utilize a number of layers to achieve this seamless experience.[12] For example, once the user visits a retail site, companies place a first-party cookie on the user's browser to improve her experience through methods of remembering login information or other information relating to that user's visit.[13] Next, the initial visited site shares this information with third parties.[14] Then, third-party cookies are placed by "someone other than the site you are on," typically, an independent advertising networks that deliver ads, or analytics companies that examine user's online behavior.[15] Ultimately, this combination of first and third-party cookies allows companies to monitor a user's behavior over time, develop a detailed history of that user's interests, and then deliver ads tailored to that user's interests.[16]

This Note will: 1) examine the development of modern privacy laws in the United States ("U.S.") and the use of cookies and protections, depending upon whom they are geared towards in comparison with laws established in the European Union ("E.U.");[17] 2) analyze these laws and their practicality in the vast technological era, as well as their applicability and enforceability in disputes;[18] 3) argue that U.S. privacy protections should extend past merely industry specific regulations and those aimed towards the protection of children to cover all consumers whose personal data is being utilized by companies while still allowing the market to advance;[19] and 4) ultimately conclude that as new privacy regulations are enacted in the U.S. and internationally, the Supreme Court and Congress must address the various questions and concerns stemming from circuit splits, as well as determine the uniform definitions of key terms and clarify their applicability to global companies.[20]

---

[12] *See id.* (summarizing process of collecting data and subsequent online tracking).

[13] *See id.* (characterizing first party cookies as login information, weather, zip code, and shopping carts).

[14] *See id.* (explaining how cookies are shared).

[15] *See id.* (discussing placing of third-party cookies).

[16] *See Online Tracking*, *supra* note 10 (outlining types of information obtained). Imagine if, for example, a user reads numerous articles about running and the relevant advertising company notices, the "seamless" experience is achieved when, while later visiting a completely unrelated site, the user stumbles upon a sneaker ad that sparks his or her interest in purchasing and proceeds to place an order for the sneakers. *Id.*

[17] *See infra* Part II, A-B (examining privacy laws and use of cookies).

[18] *See infra* Part III, A-B (considering applicability of privacy cookies).

[19] *See infra* Part IV (asserting need for appropriate regulations).

[20] *See infra* Part V (articulating final reasoning for necessity of privacy regulations).

II. HISTORY

A. Privacy Laws in the U.S.

The United States' concern with privacy is embodied in the Fourth Amendment.[21] While the Fourth Amendment's protections are wholly blurred when it comes to the technology era, privacy advocates have long promoted its protections to extend to PII.[22] PII was first defined by the 1997 Information Infrastructure Task Force ("IITF") under President Clinton as "an individual's claim to control the terms under which personal information . . . identifiable to the individual – is acquired, disclosed, and used."[23] However, as technology continues to progress, new challenges are created.[24] The U.S. currently has no comprehensive federal law regulating the collection and use of personal data or PII.[25] Opponents argue that the U.S. model for data privacy establishes protections not for its people, but for the government and corporations through its vague terminology and sector specificity.[26] "U.S. laws associated with data protection ideas have focused on selected sectors or types of information and not on general regulation of the use and collection of information."[27] One U.S. example that puts the consumer in control is the Children's Online Privacy Protection Act ("COPPA"), which was enacted in 1998 as a result of the longstanding

---

[21] *See Technology and the Fourth Amendment: Reconciling Law with the Digital Era*, ENVISAGE TECH (Nov. 15, 2017), https://www.envisagenow.com/technology-fourth-amendment-reconciling-law-digital-era/ (discussing how Fourth Amendment and evolving technology work together).

[22] *See id.* (explaining how Fourth Amendment does not cover technology era).

[23] *See* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1205 (1998) (favoring default rule that would allow PII use unless parties expressly agree otherwise).

[24] *See id.* (explaining new challenges caused by technology).

[25] *See* LEUAN JOLLY, DATA PROTECTION IN THE UNITED STATES: OVERVIEW, WESTLAW: PRACTICAL LAW COUNTRY Q&A 6-502-0467 (2018) (providing overview of U.S. privacy laws regulated by FTC). The most well-known example is the Health Insurance Portability and Accountability Act ("HIPAA") (42 U.S.C. §1301 et seq.), which regulates medical information. *Id.*

[26] *See* Dan Shearer, *EU-US Cloud Privacy Crash: Why, How, What's Next*, KOPANO (Oct. 25, 2017), https://kopano.com/kopano-documents/EU-US-Cloud-Privacy.pdf (summarizing U.S. and E.U.'s approach, history, future implementation, and arguments). Conversely, the E.U.'s approach requires meeting fundamental moral standards and protecting citizens' privacy rights. *Id.* The document seeks to show while the U.S. is lagging behind, the E.U. has long focused its economic future around privacy protections and establishing trust with its citizens relating to personal data and online markets. *Id.*

[27] *See* Raymond T. Nimmer & Holly K. Towle, Data Privacy, Protection, and Security Law § 2.01(3)(a) (LexisNexis, A.S. Pratt 2018) (explaining data protection covered in U.S.)

concern for the privacy of children.[28] COPPA deters companies from utilizing inadequate protections when collecting the PII of children under the age of thirteen when the company has actual knowledge they are doing so by imposing hefty fines for noncompliance.[29] In addition to forbidding the collection of names, address, screen names, telephone and social security numbers without explicit parental consent, COPPA specifically expands upon the typical definition of PII to include any personal identifiers that *could* identify a child or his parents, whether alone or by combining with another identifier.[30] This expansive definition therefore includes any online contact information including but not limited to IP addresses or video chat identifiers, photo, video, or audio files containing a child's image or voice, and geolocation sufficient to identify a street name and city or town.[31] The FTC is further authorized by COPPA to expand this definition when it deems necessary.[32]

While the definition of PII in the U.S. varies, COPPA is currently one of the only U.S. statutes explicitly stating that Internet Protocol ("IP") and Media Access Control ("MAC") address our personal information but limit the scope only in relation to children and their online activity.[33] Another example is the Video Privacy Protection Act ("VPPA") of 1988 prohibiting "video tape service provider[s]" from "knowingly" disclosing its

---

[28] *See* 15 U.S.C. § 6501 (2012) (codifying online privacy rights for children under age of 13); *see also* Children's Online Privacy Protection Rule, 16 C.F.R §312.3 (2018) (detailing regulation of unfair acts or practices in connection with collection of PII from children). To be in compliance with COPPA, servers geared towards children consumers must: (1) provide clear notice as to information on what PII is being collected and how such information is being used; (2) obtain parental consent before collecting, using, or disclosing; (3) provide a way for parents to review or delete the information; (4) not make prizes, activities or contests conditional upon consent; and (5) "establish and maintain reasonable procedures to protect" the privacy of the child's PII. 16 C.F.R §312.3.

[29] *See Children's Online Privacy Protection Act (COPPA)*, EPIC.ORG, https://epic.org/privacy/kids/ (last visited Apr. 10, 2019) (discussing enforcement actions and fines). To impose this stringent law, COPPA violations are equated to violating the FTC Act's prohibitions on deceptive or unfair trade practices and may result in a maximum $11,000 violation per day, and per incident. *Id.* COPPA further authorizes state attorney generals to bring enforcement actions in federal district courts. *Id.* In February 2019, the FTC obtained $5.7 million in fines from Chinese video app company, TikTok, for violating COPPA by collecting personal information from kids without parental consent. *Id.* This is the largest COPPA penalty to date. *Id.*

[30] *See Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FTC.GOV, https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance (last visited Apr. 2, 2019) (providing tips for COPPA compliance).

[31] *See id.* (highlighting far reaching nature of COPPA).

[32] *See id.* (emphasizing how FTC can change definition where and when it sees fit).

[33] *See* Children's Online Privacy Protection Rule, 16 C.F.R. § 312.3 (2012) (establishing regulations controlling collection of PII with regard to children).

"subscribers' viewing habits" to any person or second or third party.[34] However, courts have not yet agreed upon the meaning of these definitions.[35] Some U.S. circuit courts have been reluctant to define PII or to establish limitations due to possible binding consequences.[36] Although technology continues to evolve, this does not ease future cases as this dated statute and its controversial definitions must be further clarified, especially considering social media's vast online application.[37] Courts must determine exactly how a person becomes a "subscriber" and provide precedent for future cases.[38] The VPPA's creation established a federal cause of action, as it allows plaintiffs to recover actual or liquidated damages of at least $2,500, punitive damages, attorney's fees, equitable relief, and other costs.[39] "The potential

---

[34] *See* 18 U.S.C. § 2710 (2012) (explaining when liability arises).

[35] *See* 18 U.S.C. § 2710 (2012) (defining injury claim relating to privacy of renting, purchasing, or delivering of audio/video material); *see also* RICHARD RAYSMAN ET AL., INTELLECTUAL PROP. LICENSING: FORMS AND ANALYSIS § 7.04A (Law Journal Press 2018) (analyzing VPPA's nuances). While PII is broadly defined to incorporate "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider," the other terms of the statute often cause controversy. *Id.*; Yershov v. Gannett Satellite Info. Network, Inc., 820 F.3d 482, 484 (1st Cir. 2016) (reversing district court's dismissal, concluding there was PII disclosed and consumer relationship under VPPA); *but see* Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1257 (11th Cir. 2015) (analyzing term "subscriber"). The *Ellis* court decided to follow the *Yershov* district court decision instead and found that there needs to be an established relationship or commitment to be a subscriber. *See Ellis*, 803 F.3d at 1257. Furthermore, the *Ellis* court reasoned that subscriptions "involve some or most of the following factors: payment, registration, commitment, delivery, expressed association, and/or access to restricted content." *Id.* (brackets omitted) (quoting Yershov v. Gannett Satellite Info. Network, Inc., 104 F. Supp. 3d 135, 147 (2015)).

[36] *See* D. Reed Freeman and Joseph Jerome, *The VPPA and PII:Is Geolocation Another Anonymous Identifier?*, BLOOMBERG.COM (July 25, 2016), https://www.bna.com/vppa-piiis-geolocation-n73014445217/ (exploring VPPA's PII definition and impact of geolocation information).

[37] *See id.* (contemplating how other courts will define PII in light of current circuit split). This article analyzes whether PII definition will be interpreted by future courts to include such "anonymous identifiers, geolocational information and elements of data that are sometimes passed through a streaming service to third parties, such as analytics providers." *Id.*

[38] *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 267 (3rd Cir. 2016) (describing information that cannot be disclosed). Prohibition on the disclosure of PII applies only to the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior. *Id.* The Third Circuit reasoned that creating a general framework makes more sense as plaintiffs stray further from the "1988 paradigm" due to continual technological development, which leaves courts scrambling. *Id.* at 290. The Court stated, "we recognize that our interpretation of the phrase 'personally identifiable information' has not resulted in a single sentence holding capable of mechanistically deciding future cases." *Id.* "We have not endeavored to craft such a rule, nor do we think, given the rapid pace of technological change in our digital era, such a rule would even be advisable." *Id.*

[39] *See* Allison Grande, *Google, Viacom Ruling Limits Scope of Video Privacy Actions*, LAW 360 (July 14, 2014, 10:16 PM), https://www.law360.com/articles/557319/google-viacom-ruling-limits-scope-of-video-privacy-actions (discussing recent decision's ability to hinder future class actions by narrowing scope of VPPA).

for uncapped damages rewards, coupled with the difficulty of applying vague language drafted in the 1980s to unforeseen technological developments such as the widespread prevalence of video-streaming services, has resulted in numerous VPPA class actions over the dissemination of consumer video-viewing habits . . . ."[40] VPPA also extends its limitations to social media sites that share subscribers' viewing habits by capturing PII. [41]

In addition to COPPA and the VPPA, other heavily regulated sectors include the healthcare and financial industries, however, privacy advocates in the U.S. have long argued that basic privacy protections are needed at every level when handling personally identifiable information, especially technology companies handling immense amounts of PII.[42] Most recently, California passed a digital privacy law granting consumers more control and insight into the ways companies use their personal information online, creating one of the most significant regulations overseeing data-collection practices of technology companies that the U.S. has seen to date.[43] On September 23, 2018, the governor of California signed into law the amended version of the California Consumer Privacy Act of 2018 ("CCPA"), which was originally enacted in June 2018.[44] The CCPA, which will officially go into effect in January 2020, grants consumers: 1) the right to ask companies

---

[40] *See id.* (summarizing scope of VPPA). Article discusses two important VPPA determinations due to the ruling: (1) rejecting stretch . . . of video tape service provider to cover any party that is in possession of [PII]; and (2) clarifying that VPPA applies to online videos and not online advertising practices. *Id.*

[41] *See* JAMES B. ASTRACHAN ET AL., 3 LAW OF ADVERTISING § 56.05 (Matthew Bender & Co., Inc., ed. 2018) (explaining laws surrounding advertising and development of social media law). "[W]herever someone's personal information is used to sell them something, there will always be issues with privacy." *Id.* While none of the 2011 cases analyzed reached a trial on the merits, a case against Facebook resulted in a settlement requiring Facebook to: (1) "[stop] misrepresenting the privacy of information on its website; (2). . . give users a clear and prominent notice and to obtain a user's express consent before sharing their information with third parties). . . ; (3). . . establish and maintain a comprehensive privacy program; and (4) subject itself to regular privacy audits for the next 20 years." *Id.*

[42] *See Personally Identifiable Information: What Companies Need to Know*, REGERLAW.COM (March 29, 2017), https://www.regerlaw.com/personally-identifiable-information-what-companies-need-to-know.html (listing examples of Congressional enacted statutes related to data privacy).

[43] *See* Daisuke Wakabayashi, *California Passes Sweeping Law to Protect Online Privacy*, N.Y. TIMES (June 28, 2018), https://www.nytimes.com/2018/06/28/technology/california-online-privacy-law.html (explaining effects and nuances of new California data privacy law).

[44] *See id.* (explaining creation of proposed ballot). Under California law, citizens can propose new laws and constitutional amendments and may secure a statewide vote on their initiatives if they get enough signatures on a petition advocating that the proposed law appear on a future ballot. *Id.* Due to this right, three unlikely privacy advocates proposed the ballot that would eventually be enacted into law to provide consumers with protections from the nation's toughest privacy laws. *Id.*

what information they are collecting about them, including why and with whom they are sharing it; 2) the right to request companies to delete their information; 3) the right to demand that companies not share or sell their data for business purposes; and 4) the right to sue or fine companies that violate these rights.[45] Further, the law makes it increasingly more difficult for companies to share or sell data of younger children by requiring that children under the age of sixteen to affirmatively opt in and that the parents of children under the age of thirteen must opt in on the child's behalf before businesses can sell their personal data.[46] In the wake of the E.U.'s General Data Protection Regulation ("GDPR"), the CCPA is considered the first regulation in the U.S. to attempt to match the GDPR's broad definitional scope of what type of information is covered under PII while also granting consumers extensive rights to control that information.[47] "The nation's most populous state, considered a political trendsetter, is responding to consumers' growing unease with the massive and largely unchecked collection and sharing of vast amounts of their private information that has produced a string of privacy mishaps."[48] The new law will likely carry a tremendous impact on technology companies as most are headquartered in California.[49]

B. Privacy Laws in the E.U.

The European Union's attitude towards personally identifiable information differs substantially from that of the United States, with its longstanding commitment to regulate and standardize data protection across member states.[50] Accordingly, the most notable effort to regulate the

---

[45] *See* Wakabayashi, *supra* note 43 (summarizing key rights of CCPA). Businesses must adhere to these and other new regulations while still providing the same quality of service even for consumers who opt out. *Id.*

[46] *See id.* (discussing data protections for children); *see also* Nancy L. Perkins et al., *California's New Privacy Statute: Is It a US GDPR*, ARNOLD & PORTER (Oct. 3, 2018), https://www.arnoldporter.com/en/perspectives/publications/2018/10/californias-new-privacy-statute?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original (summarizing opt-in requirements for protection of children's PII).

[47] *See* Perkins, *supra* note 46 (noting CPPA has significant similarities to GDPR).

[48] Jessica Guynn, *California passes nation's toughest online privacy law*, USA TODAY (June 28, 2018), https://www.usatoday.com/story/tech/2018/06/28/california-lawmakers-pass-tough-new-online-privacy-rules-could-model-other-states/743397002/ (crediting bill's passage to recent data breaches and consumer outrage).

[49] *See id.* (explaining why California companies will need to comply with CCPA).

[50] *See* Phil Lee, *The differences between US and EU data protection*, YOUTUBE (Jan. 13, 2017), https://www.youtube.com/watch?v=-_zLeGKHOpc (explaining key differences such as EU providing "constitution" like fundamental right protections to privacy). The E.U. characterizes the right to privacy as so fundamental as to have it codified within the E.U. Charter of Fundamental

technology industry came from Europe through the enactment of the General Data Protection Regulation ("GDPR"), which was fully implemented on May 25, 2018.[51] Prior to its enactment, however, the E.U. similarly faced a lack of uniformity in protecting and controlling the privacy and data of its citizens.[52] The "1995 Directive"[53] required its member states to implement mandatory standards for the processing of personal data at a stricter standard than that of the U.S.[54] While the 1995 Directive's fundamental goal was the "harmonization of data protection laws and the transfer of personal data to third countries," it was only somewhat successful in supervising these goals as, ultimately, it was unable to control individual member states' level of protection or quality of implementation.[55] While the 1995 Directive successfully created a more unified standard across Europe and furthered the concept that privacy is a fundamental right, its power reached only as far as a suggestion because each individual member state interpreted and administered the law differently.[56] Thus, the E.U. proposed an updated regulation, the GDPR, to bridge the gap between the 1995 Directive and the

---

Rights of 2000, which is an enactment resembling the U.S. Constitution. *Id.* This instrument sets out two specific rights of protection stating, first, in Article 7, "everyone has the right to respect for his or her private and family life, home and communications," and second, in article 8, "everyone has the right to the protection of the personal data concerning him or her." *Id.*

[51] *See* Wakabayashi, *supra* note 43 (explaining GDPR as stringent privacy regulation). The GDPR restricts how technology companies "collect, store and use personal data" of E.U. citizens. *Id.*

[52] *See How did we get here? An overview of important regulatory events leading up to the GDPR*, EU GEN. DATA PROTECTION REG, https://www.eugdpr.org/how-did-we-get-here-.html (last visited Feb. 23, 2019) (noting E.U. struggled to control data privacy of its 28 member-states).

[53] European Data Protection Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data ("1995 Directive").

[54] *See* DAVID H. BERNSTEIN ET AL., THE LAW OF ADVERTISING, MARKETING AND PROMOTIONS §6.06 (Law Journal Press ed. 2019) (setting out regulations directing to all member states to pass legislation implementing such requirements).

> For example, the European Directive requires that: (1) personal data may be processed only with the informed consent of the individual; (2) entities collecting data must disclose the purpose for which the data will be used; and (3) individuals have the right to access their personal data, make changes to the data they have provided and object to the use of the data.

Id.; *see also* DAVID H. BERNSTEIN ET AL., THE LAW OF ADVERTISING, MARKETING, AND PROMOTIONS §§ 10, 12, 14 (Law Journal Press ed. 2019) (describing procedural aspects of false advertising challenges, supervisory skills and remedies).

[55] *See How did we get here?, supra* note 52 (explaining major changes from 1995 Directive to current). Through means of "establish[ing] independent public authorities called Data Protection Authorities (DPAs) in each member state," the directive was able to supervise the application. . . of said regulation and serve as a regulatory body. *Id.* However, the transference of personal data to third countries was conditioned on that country's own level of protection, which is more difficult to supervise. *Id.*

[56] *See id.* (describing challenge in making 1995 Directive enforceable law).

modern data-driven world in the hopes of protecting individuals' fundamental privacy rights regardless of evolving technological innovations.[57]

The GDPR remains true to its predecessor, but imposes heightened protections and major changes, and was correctly predicted to have a tremendous impact on companies conducting any business with E.U. citizens.[58] The GDPR fully replaces the 1995 Directive framework by imposing a host of new obligations on parties handling personal information of European citizens, while also enforcing substantial penalties when companies, including U.S. companies, fail to comply.[59] The GDPR creates and strengthens specific rights of individuals, including: 1) the right to obtain details about how their data is being processed; 2) the right to obtain copies of any personal data that companies have on them; 3) the right to have companies fix incorrect or incomplete data; 4) the right to have their data erased if company has no legitimate reason for retaining the data; 5) the right to obtain their data from one company and transfer it to another; 6) the right to object to the processing of their data in certain circumstances; and 7) the right to not be subject to automated profiling.[60]

Upon its implementation, the GDPR superseded the 1995 Directive and any other existing regulations across all European countries, and applied its own definitions with the goal of providing clarity and uniformity.[61] For example, the GDPR uniformly defined IP addresses as PII.[62] This is exemplified in two recent rulings by the Court of Justice of the European Union ("CJEU"), which stated that "one stop shop" must apply to the E.U. member states, and also invalidated the "Safe Harbor Statutes" between E.U.-U.S. for data transfers, thus requiring U.S. companies to comply or suffer substantial penalties.[63] The CJEU clarified its position of requiring uniformity by ruling that IP addresses must be considered PII because they

---

[57] *See id.* (comparing GDPR and 1995 directive's fundamental difference: GDPR is enforceable law).

[58] *See GDPR Key Changes*, EU GEN. DATA PROTECTION REG., https://www.eugdpr.org/key-changes.html (last visited Jan. 29, 2018) (summarizing changes from 1995 Directive to GDPR).

[59] *See* Caroline Krass et al., *A GDPR Primer for U.S.-Based Cos Handling EU Data,* LAW360 (Dec. 12, 2017, 12:16 PM), https://www.gibsondunn.com/publications/Documents/Krass-Baladi-Kleinwaks-Bartoli-A-GDPR-Primer-For-US-Based-Cos-Handling-EU-Data-Part-2-Law360-12-13-2017.pdf (laying out scope of GDPR).

[60] *See GDPR Compliance, The Most Important Changes Under the GDPR*, HUBSPOT.COM, https://www.hubspot.com/data-privacy/gdpr (last visited Mar. 9, 2018) (setting out new and updated rights of individuals under GDPR).

[61] *See* Eric Lambert, *Are IP and Mac Addresses Personal Information?*, LINKEDIN (June 16, 2016), https://www.linkedin.com/pulse/ip-mac-addresses-personal-information-eric-lambert/ (noting that differentiating definitions between various countries led to need for GDPR).

[62] *See id.* (establishing IP address as part of PII definition).

[63] *See id.* (summarizing important E.U. court decisions).

can be combined with other PII to precisely identify an individual.[64] Even American companies engaging in business in Europe must be aware of the penalties when they fail to meet the standards under the 1995 Directive, which prohibited the transfer of personal data outside the E.U. except where a third-party country "ensure[s] an adequate level of protection" acceptable under the protections of "Safe Harbor Statutes."[65] In October 2015, the CJEU invalidated the Safe Harbor Statutes and replaced them with the EU-US Privacy Shield.[66] However, in reality, the U.S.'s "decentralized privacy regime" would certainly be found inadequate even under this lower standard.[67] The tougher scope of the GDPR shifts on an "absolutely data-centric" approach and applies to all personal data processed by organizations both *inside* the E.U. and personal data of E.U. citizens by organizations *outside* the E.U., even where such data is outside its borders.[68] "Repeated non-compliance with the GDPR can invite fines for up to 20 million EUR or 4% of the total worldwide annual turnover of the preceding financial year,

---

[64] *See id.* (holding IP addresses to be PII). Both the 1995 Directive and the GDPR define personal data as "any information relating to an identified or identifiable person." *Id.* However, member states have differed on whether an IP address should qualify as personally identifiable personal data. *Id.* The CJEU reasoned that IP addresses must be considered PII under the GDPR because such online identifiers derived from devices, applications, cookie identifiers, internet addresses, etc. "may leave traces which, in particular when combined with unique identifiers and other information received by servers, may be used to create profiles of the natural person and identify them." *Id.*

[65] *See id.* (defining safe harbor statutes). Safe Harbor Statutes were principles developed between U.S. and EU to prevent businesses from losing or accidentally disclosing consumer PII. *Id.*

[66] *See* Lambert, *supra* note 61 (explaining why safe harbor statutes were replaced); *see also Schrems v. Data Protection Commissioner* (CJEU- "Safe Harbor"), EPIC.ORG, https://epic.org/privacy/intl/schrems/ (last visited Mar. 10, 2018) (explaining important CJEU case). In *Schrems v. Data Protection Comm'n*, the Court invalidated the Safe Harbor Statutes where Facebook user data was not adequately protected when it was transferred to the U.S. from Facebook's European headquarters. *Id.* The CJEU found that U.S. data privacy laws cannot provide security that EU citizens "expect[] and require[]." *Id.* The new EU-US privacy shield was intended to make data transfers easier while also protecting citizens further, however, it received much criticism. *Id.*

[67] *See* JAMES B. ASTRACHAN, ET AL., 3 THE LAW OF ADVERTISING § 56.05 (2017) (explaining safe harbor statutes). The U.S. was able to escape some of the 1995 Directive's provisions through these "safe harbor statutes" by only having to comply with seven principles including providing notice, opt-out or opt-in provisions and assuring data collected is relevant for its intended use. *Id.*

[68] *See Complying with the General Data Protection Regulation of the EU*, SECLORE, https://www.seclore.com/solutions-compliance-gdpr/ (last visited Feb. 18, 2019), (summarizing security company's compliance with GDPR through implementation of data-centric technology). Enterprise Digital Rights Management ("EDRM") technology is capable of protecting data-centric information wherever it goes, while traditional perimeter-centric security tools fail to secure when data-centric information as it travels from one platform to another. *Id.* EDRM technology has assisted numerous E.U. organizations in preparing for the GDPR. *Id.*

whichever is higher."[69] The GDPR embraces a risk-based approach to data protection, where organizations that control the processing of personal data or "controllers" are encouraged to implement protective measures corresponding to the risk level of their data processing activities.[70]

III. FACTS

A. Interpretation of Privacy Laws in the U.S.

One of the essential and fundamental cases that explores the limitations of VPPA, while also attempting to redefine some of its terminology, is *In re Nickelodeon Customer Privacy Litigation.*[71] In *Nickelodeon,* the plaintiffs consist of children younger than thirteen years of age who allege that the defendants, Viacom and Google, unlawfully collected PII about them and their internet viewing habits, and sold and distributed this information for the purpose of targeted advertising based on each user's web browsing.[72] Plaintiffs further argue that targeting ads toward

---

[69] *See id.* (noting that noncompliance exposes even U.S. based companies to significant fines); *see also* Gabriel Maldoff, *The Risk-Based Approach in the GDPR: Interpretation and Implications*, INTERNATIONAL ASSOCIATION OF PRIVACY PROFESSIONALS, https://iapp.org/media/pdf/resource_center/GDPR_Study_Maldoff.pdf (last visited August 30, 2018) (explaining three categories of risk analysis for companies with relevant GDPR articles). Accordingly, the strictest penalties of up to 20 million EUR or 4% of the global annual turnover arise for violations such as processing, obtaining consent, data subject rights, and cross-border data transfers. *Id.*

[70] Maldoff, *supra* note 69 (explaining risk-based approach). The GDPR grants local regulators or "Supervisory Authorities" extensive powers and responsibilities including investigative and enforcement powers. *Id.* Supervisory Authorities are empowered to impose significant administrative fines on both data controllers and data processors that violate the GDPR. *Id.* In order to avoid the grave fines, companies that own internal compliance will need to determine what personal data they process about EU citizens, such as personal data about employees, evaluate current state of compliance, and formulate a roadmap to lay the groundwork for a GDRP compliance program. *Id.*

[71] *See In re* Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 267 (3d Cir. 2016) (raising two first impression questions in Third Circuit). Viacom owns the children's television station Nickelodeon and operates Nick.com, a website geared towards children that offers streaming videos and interactive games. *Id.* at 268. To register for Nick.com, one must sign up for an account creating a username and password by providing information such as birthday and gender. *Id.* Subsequently, Viacom assigns the person a unique code based on the information. *Id.* at 269.

[72] *See id.* (explaining plaintiffs' claims). Plaintiffs alleged that Viacom expressly stated that they did not collect any information about children, but then unlawfully used cookies to track children's web browsing and video-watching habits on Viacom's websites in four ways: (1) placing a first-party cookie on that user's computer during their first visit to the site; (2) allowing Google to contract with Viacom to place ads on Viacom's website by means of placing third-party cookies; (3) providing Google with access to children's profiles and other PII available only in the first-party cookies; and (4) Viacom, allowing Google to place their cookies on children's computer,

children is much more profitable than targeting ads toward adults because children are by nature more susceptive and unable to differentiate between content and ads.[73] Contrary to the defendants' assertion that plaintiffs lacked standing, the court found standing to be satisfied because in some cases, invasion of certain statutes are enough to constitute an injury-in-fact.[74] The Supreme Court has held that intangible harms can qualify as concrete for Article III standing purposes.[75] Accordingly, the Third Circuit concluded that the facts alleged in this case are sufficient to establish Article III standing because the "purported injury is clearly particularized, as each plaintiff complains about the disclosure of information relating to his or her online behavior[,]" and while it may be "intangible[,]" it has traditionally been enough for redressability under the law.[76] The more seminal question is whom, under VPPA, the plaintiffs have the right to sue: the video tape service provider who disclosed PII, the person who received that information, or both.[77] Next, the court determined that the information in question did not even qualify as PII, although the Act "is not entirely clear" as to what triggers liability.[78] The court notes that the fundamental disagreement turns on the idea of a "spectrum," one end of which is a person's actual name, on the other end is "pieces of information such as

---

thereby permitted Google to track that person across any website on which Google displays ads and combine that information with information it collected from people using its own websites. *Id.*

[73] *See id.* at 270 (presenting another fundamental argument for plaintiffs). The court, however, found that most of these allegations have been rendered moot due to a preceding case. *Id.*; *see also In re* Google Inc., 806 F.3d 125, 153 (3d Cir. 2015) (dismissing all claims except for invasion of privacy and intrusion upon seclusion). The court determined that a reasonable fact finder could determine that defendants used deceitful methods to override plaintiffs' cookie blockers, constituting an invasion of privacy under California law. *See Google*, 806 F.3d at 153.

[74] *See Nickelodeon*, 827 F.3d at 272-73 (explaining plaintiffs must demonstrate invasion of concrete, particularized harm accompanied by actual and individual effect).

[75] *See* Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549-50 (2016) (remanding because Ninth Circuit only addressed "particularized" requirement ignoring whether it was sufficiently concrete).

[76] *See Nickelodeon*, 827 F.3d at 274 (finding plaintiffs have standing). *But see* Bernardino v. Barnes & Noble Booksellers, Inc., No. 17-CV-04570 (LAK) (KHP), 2017 U.S. Dist. LEXIS 129038, at *PINCITE (S.D.N.Y. Aug. 11, 2017) (concluding plaintiff did not meet standing requirement). The case did not discuss the merits where plaintiff could not make a clear and substantial showing of likelihood of such success, even if she could show irreparable harm. *Id.*

[77] *See Nickelodeon*, 827 F.3d at 279-80 (deciding against plaintiffs that only video tape providers who disclose PII are liable under VPPA). In doing so, the court dismissed the plaintiffs' direct claims against Google as the third-party who received the PII and found Google could not be liable for merely receiving this information from another party. *Id.*

[78] *See id.* at 281 (evaluating merits of claim Viacom disclosed PII). Plaintiffs argue that Viacom disclosed the children's IP addresses, "browser fingerprint," and the device's unique identifier, permitting Google to track that computer across time and space. *Id.* While defendants contend that the information is not PII because it does not, by itself, identify a particular person. *Id.* at 282. Even more remote are social security numbers, which can be linked to a specific person, but not absent assistance of another entity. *Id.* "The kind of information at issue here – static digital identifiers – falls even further down the spectrum." *Id.*

telephone number or physical address, which may not by themselves identify a particular person but from which it would be possible to identify the person by consulting publicly available sources."[79] However, the court found Viacom's narrower understanding more persuasive, relying upon both statutory interpretation and legislative history, and simultaneously cautioned that when Congress passed the VPPA, it did not intend to cover far removed circumstances.[80] In sum, the court reasoned the information disclosed by Viacom falls on the side of "too unforeseeable" and thus, does not constitute a violation.[81]

Conversely, the First Circuit has become an "outlier" as it has been more liberal across the board with its definition of what qualifies as PII and what qualifies someone as a "subscriber" under the statute.[82] Creating an

---

[79] *See Nickelodeon*, 827 F.3d at 282-83 (finding static digital identifiers even further down this spectrum). Most courts follow the rule that digital identifiers cannot hypothetically be combined with other information to link to a person are not by themselves PII. *Id.*; *see also In re* Hulu Privacy Litig., No. C 11-03764 LB, 2014 U.S. Dist. LEXIS 59479, at 36 (N.D. Cal. Apr. 28, 2014) (finding unique ID alone not PII but context could render identification of specific person); *see, e.g.*, Robinson v. Disney Online, 152 F. Supp. 3d 176, 178 (S.D.N.Y. 2015) (recognizing there must be some limitation on what information qualifies as PII). While the court found that disclosures to third-party data analytics companies of the encrypted serial number of the digital device and viewing history would generally constitute a VPPA claim, here, the information itself did not rise to the level of PII required, i.e. identifying a "particular person" as having accessed "specific video materials." *Robinson*, 152 F. Supp. 3d at 183. *See* Ellis v. Cartoon Network, Inc., 803 F.3d 1251, 1257 (11th Cir. 2015) (deciding merely downloading free mobile app does not deem consumer a "subscriber"); Eichenberger v. ESPN, Inc., No. C14-463 TSZ, 2015 U.S. Dist. LEXIS 157106, at *PINCITE (W.D. Wash. May 7, 2015) (dismissing plaintiff's complaint with prejudice where plaintiff failed to allege defendant disclosed PII); *but see Yershov*, 820 F.3d at 489 (applying VPPA where static identifiers could "theoretically" permit company to identify viewer).

[80] *See Nickelodeon*, 827 F.3d at 284-90 (interpreting intent of PII under VPPA). The court focused heavily on Congress's decision to retain the 1988 definition of PII under VPPA when it recently revisited the law, leaving it almost untouched nearly thirty years later, signifying its direct intent to keep the law intact. *Id.* at 288. Additionally, the court justified its fundamental disagreement with *Yershov* on the basis that the First Circuit merely believed that "GPS coordinates contain more power to identify a specific person than, in our view, an IP address, a device identifier, or a browser fingerprint." *Id.* at 289. Further, the court highlighted this quote from *Yershov*: "there is certainly a point at which the linkage of information to identity becomes too uncertain, or too dependent on too much yet-to-be-done, or unforeseeable detective work" to trigger liability under this statute. *Id.*

[81] *See id.* (highlighting reasoning of court).

[82] *See* Perry v. CNN, Inc., 854 F.3d 1336, 1339 (11th Cir. 2017) (finding plaintiff was not subscriber by merely obtaining the channel on TV even though he had standing); *see also* Brian Amaral, *CNN Viewer Isn't CNN Subscriber, Network Tells 11th Circ.*, LAW360 (Sept. 2, 2016), https://www.law360.com/articles/836214 (identifying *Yershov* as "outlier lacking any meaningful limiting principle" in permitting random device identifiers to qualify as PII); Erin Mendillo, *Massachusetts Supreme Court Rules ZIP Codes Are Definitely "Personal Identification Information,"* PRIVACY LAW BLOG (Apr. 1, 2013), https://privacylaw.proskauer.com/2013/04/articles/data-privacy-laws/massachusetts-supreme-court-rules-zip-codes-are-definitely-personal-identification-information/ (interpreting PII under state law to include ZIP code, giving consumer right to sue). In *Tyler v. Michael's Store Inc.*, the

exception to the general rule, *Yershov v. Gannett Satellite Info. Network, Inc.* recently analyzed VPPA.[83] In *Yershov*, Gannett, an international media company that produces news and entertainment programming, offered its content via a free mobile app without obtaining the user's consent to disclose any information to third parties.[84] Each time a user viewed a video clip, Gannett sent Adobe (an unrelated third party) the title of the video, the GPS coordinates of the device at the time of the viewing, and certain identifiers associated with the user's device, such as its unique phone ID.[85] As the third party, Adobe compiled this behavioral information by creating user profiles containing "user's name, address, age, income, household structure and online navigation and transactional history" and sold it to its clients through data analytics and online marketing services.[86] Such profiles provided Adobe and its paying clients with "intimate" information that "may reveal, or help create inferences about a user's traits and preferences to accurately target advertisements to them."[87] In reaching its decision that the disclosed information qualified as PII under VPPA, the First Circuit highlighted Congress' intention in enacting the statute in the first place: to "preserve personal privacy" and in turn, went as far as to create a civil remedy for precisely these disclosures.[88] Next, the court answered the consumer question by determining that plaintiff was a "subscriber" because the court reasoned that Congress intended to limit the term "subscriber" by narrowing the definition to require some form of payment, and it would not have made a distinction between "purchasers" and "renters" in preserving the 1998 definition, which clearly showed the same level of protection as it originally

---

SJC reasoned regardless of whether ZIP code was explicitly defined in the statute as PII, it could be used to obtain such information, thus giving rise to a violation of Mass. Gen. Laws, ch. 93, § 105(a). *Id.*; *see also* Tyler v. Michaels Stores, Inc., 492, 984 N.E.2d 737, 746 (2013) (finding injuries where merchant uses PII by sending unwanted marketing materials or selling for profit). *But see* Kashmir Hill, *A Ridiculous California Court Ruling: Zip Codes are Private*, FORBES (Feb. 11, 2011, 12:52 PM), https://www.forbes.com/sites/kashmirhill/2011/02/11/a-ridiculous-california-court-ruling-zip-codes-are-private/ (highlighting how easy it is for online retailers to target customers through cookies).

[83] *See Yershov*, 820 F.3d at 489 (providing background on plaintiffs' allegations).

[84] *See id.* (highlighting how company failed to obtain consent).

[85] *See id.* (explaining type of information provided to Adobe).

[86] *See id.* at 485 (explaining how Adobe used device ID). Having the unique phone ID allowed Adobe to "identify and track specific users across multiple electronic devices, applications and services that a consumer may use." *Id.*

[87] *See id.* (highlighting way in which Adobe analyzed data). Additionally, the court hypothesized that the link between the GPS address and device identifier, as alleged in the complaint, were enough to connect to a certain person by name, address, or phone number. *Id.* Using the example of Gannett disclosing 146 videos viewed from two sets of specified GPS coordinates, the court ruled that it led to the reasonable and foreseeable inference that the two addresses were a home and work address of the person. *Id.* at 486.

[88] *See id.* at 485-86 (reasoning that Congress intended language to be broad and not exclusive).

intended to grant.[89] The vast contrast between the two recent cases provides certainty on one aspect: the future remains unclear.[90] While PII is at the center of today's privacy law debates, it has no uniform definition in the U.S.[91] Although there are arguments that significant regulation is necessary to create clearer boundaries of the law, it has not been addressed by the Supreme Court nor Congress through an all-encompassing federal law.[92]

B. Interpretation of Privacy Laws in the E.U.

According to a 2015 CJEU ruling, under the new general requirements of the GDPR, each member state will be equipped with its own DPA, enforcing a consistent "one-stop-shop" law for greater conformity with the GDPR.[93] Immediately following the *Weltimmo* holding, the CJEU invalidated the Safe Harbor provisions between the U.S. and E.U., which served as a simpler, legal way for roughly 4,500 businesses to conduct data transfers.[94] It is unknown whether the GDPR will replace the Safe Harbor provisions entirely or evolve with them, which creates uncertainty with how this will affect the U.S.'s contradicting legal framework.[95]

U.S. based ad tech companies are reasonably fearful that their businesses are at risk of being frozen out of the European market and replaced by E.U. competitors.[96] This fear is due to requirements to obtain

---

[89] *See Yershov*, 820 F.3d at 487-88 ("Congress itself, in 2012, considered the impact of the VPPA on the electronic distribution of videos and chose only to make consent easier obtain, rather than limiting the reach of the act in absence of consent.").

[90] *See* Paul Schwartz & Daniel Solove, *The PII Problem: Privacy and a New Concept of PII*, 86 N.Y.U.L. REV. 1814, 1815 (2011) (developing new PII model protecting information based on different legal interests associated with each category). This article attempts to offer a more flexible approach to please both sides of the controversy by distinguishing between PII that relates to an "identified or identifiable person," treating the former with a substantial risk, and the latter with caution to avoid using tactically. *Id.*

[91] *See* Kat Sieniuc, *Justices Wont Hear Google Online Child-Tracking Case*, LAW360 (Jan. 9, 2017, 1:09 PM), https://www.law360.com/articles/878725/justices-won-t-hear-google-online-child-tracking-case (noting no uniform definition of PII in U.S.).

[92] *See id.* (discussing Supreme Court's denial of certiorari in *Nickelodeon* in calling for judicial clarity).

[93] *See Schrems v. Data Protection Commissioner*, *supra* note 66 (finding companies must comply with local data laws if they have "establishments" in E.U state). Each state will have its own DPA, tasked with enforcing the uniform law and decisions of the GDPR along with consulting with other DPA's across Europe and ensuring data subject' rights are secured by their availability of legal redress. *Id.*

[94] *See id.* (discussing effect of *Weltimmo* on State Harbor provisions).

[95] *See id.* (referring to uncertainty of GDPR effect on Safe Harbor provisions).

[96] *See* Seb Joseph, *GDPR is coming, and many U.S. ad tech firms aren't ready*, DIGDAY (Sept. 12, 2017), https://digiday.com/marketing/gdpr-coming-many-u-s-ad-tech-firms-arent-ready/ (explaining challenges ad companies face when obtaining specific consent to use individuals' data). "[A]dvertisers won't be able to market to individuals without obtaining specific consent to use their

direct consensual relationships with individuals or not interact with them at all, which U.S. companies were previously not required to comply with, while reaping the monetary benefits.[97] "[T]he GDPR applies directly to any entity that processes personal data about E.U. residents in connection with (i) the offer of goods or services in the E.U.; or (2) [sic] the monitoring of behavior in the E.U."[98] Thus, the GDPR's framework of personally identifiable information will apply, expanding personal data to include unique online identifiers, such as IP addresses, mobile device identifiers, and individual's geo-location data, while extending its jurisdictional reach to include a digital presence and reference to E.U. individuals, currencies accepted, and languages used.[99] The GDPR requires companies to fundamentally change *how* they collect, manage, and store consumer data of E.U. citizens.[100] In practice, U.S. companies will have to store E.U. individuals' information on servers located in the E.U. and if they desire to access servers located in the U.S., the companies are required to comply with stricter standards, including notifying customers within 72 hours of a breach, fulfilling customer requests to delete their records entirely, and obtaining initial customer consent.[101] Actually enforcing the GDPR on U.S. based companies will be accomplished through authority, jurisprudence, assistance from international law, unilateral trade agreements, local due process, and geographical location of the companies.[102] For U.S. companies with "establishments" or physical presences in the E.U., the GDPR can directly

---

data. It won't matter whether a company's servers are held in Israel, India or the U.S. — if it is storing the data of an EU citizen, it must abide by the General Data Protection Regulation or face fines." *Id.*

[97] *See id.*; *see also* Yasmeen Abutaleb and Julia Fioretti, *Smaller U.S. businesses fear freeze from EU privacy ruling*, REUTERS (Oct. 7, 2015, 9:43 PM), https://www.reuters.com/article/us-eu-dataprotection/smaller-u-s-businesses-fear-freeze-from-eu-privacy-ruling-idUSKCN0S12TL20151008 (discussing U.S. concerns with court ruling).

[98] *See* Jonathan Millard and Tyler Newby, *EU's General Data Protection Regulation: Sweeping Changes Coming to European and U.S. Companies*, AMERICAN BAR ASSOCIATION (May 23, 2016), http://apps.americanbar.org/litigation/committees/technology/articles/spring2016-0516-eu-general-data-protection-regulation.html (measuring scope of EU's reach by digital, not physical, jurisdiction). As a result, the EU will now be able to hold companies accountable for not complying even if they were previously outside the jurisdictional scope. *Id.*

[99] *See id.* (explaining how companies will need to change due to GDPR).

[100] *See id.* (showing how GDPR forces companies to change data collection methods).

[101] *See id.* (providing examples of changes companies will be required to make).

[102] *See* AJ Dellinger, *EU's GDPR: What Will American Companies Have To Do To Comply*, INTERNATIONAL BUSINESS TIMES (Aug. 1, 2017, 11:38 AM), http://www.ibtimes.com/eus-gdpr-what-will-american-companies-have-do-comply-2573002 (recommending early implementation strategies to avoid high risk of noncompliance); *see also* Aaron W., *How the EU can fine US companies for violating the GDPR*, SPICEWORKS (Jun. 21, 2017, 12:11 PM), https://community.spiceworks.com/topic/2007530-how-the-eu-can-fine-us-companies-for-violating-gdpr (explaining how E.U. has authority to enforce GDPR on U.S. companies initially).

enforce laws against them, while U.S. companies without a physical presence, will be designated a representative in the E.U. by the GDPR to investigate and fine companies that are "knowingly, and actively, conducting business in the E.U."[103]

C. Implementing the GDPR

"Any business that holds data (including IP addresses and online browsing history) on an EU citizen must be able to show where this information resides and that it was captured with the explicit consent of the individual in question."[104] Companies will be incentivized to comply due to threat of tremendous monetary fines and potential negative reputational impact on their brand name.[105] U.S. companies have acknowledged that the GDPR will be expensive, but they believe it is a "worthwhile investment."[106] In accordance with this, two-thirds plan to commit to following the GDPR's principles and further invest in the E.U, while less than one third of companies plan to reduce their E.U. presence.[107] "Companies that lead with transparency have the best chance of continuing to engage with online consumers based in Europe."[108]

An example of changes made by the GDPR is that it changes the consent standard, to requiring it "to be freely given, specific, informed and unambiguous, with controllers using 'clear and plain' legal language that is 'clearly distinguishable from other matters.'"[109] The previous standard required a company to ensure a data subject gave consent before submitting

---

[103] *See* Aaron W., *How the EU can fine US companies for violating the GDPR* (clarifying E.U. Regulators relying on international law to issue fines against noncompliant U.S. companies); *see also* Colin Truran, *GDPR Compliance Requirements and Implications for US Companies*, QUEST (Aug. 31, 2017), https://www.quest.com/community/b/en/posts/gdpr-compliance-requirements-and-implications-for-us-companies (answering how GDPR can actually in practice impose penalties on U.S. based companies).

[104] *See* Clark Boyd, *GDPR: How US businesses are preparing*, CLICKZ (Jan. 2, 2018), https://www.clickz.com/gdpr-us-businesses-preparing/203180/ (comparing U.S. and E.U. laws and tensions of new GDPR laws).

[105] *See id.* (explaining incentives to comply with GDPR).

[106] *See id.* (showing how U.S. companies' willingness to comply with GDPR).

[107] *See id.* (illustrating a reduction of U.S. business in E.U.); *see also* Mike O'Brien, *GDPR: Increased transparency and increased trust*, CLICKZ (Dec. 4, 2017), https://www.clickz.com/gdpr-increased-transparency-increased-trust/203390/ (arguing GDPR provides invaluable opportunity to rebuild consumers trust).

[108] *See* Mimi An, *The General Data Protection Regulation is Coming*, HUBSPOT (Dec. 18, 2018 11:00 a.m.), https://research.hubspot.com/general-data-protection-regulation?_ga=2.14538800.60321635.1521054985-800953669.1494012600 (summarizing survey results regarding opinions on GDPR and preparation of other companies).

[109] *See GDPR Compliance*, *supra* note 60 (discussing new consent standard).

any personal information.[110] Under the 1995 Directive, consent could be inferred, leaving open the possibility for opt-out provisions to be inferred from silence, pre-ticked boxes, and other similar tactics, while customers under the GDPR must provide explicit consent.[111]

IV. ANALYSIS

Within its Bill of Rights or other federal statutes, the U.S. does not explicitly provide that PII is protected under rights of privacy and is often criticized for its all-encompassing federal data privacy law, while continuing to rely on sector-specific rules without one controlling authority.[112] Further, in the U.S., different state legislatures and courts have implemented varying privacy rights through legislation or by recognizing privacy protections in their respective state constitutions, while some choose to not adopt any protections at all, adding to the lack of uniformity.[113] To the contrary, E.U. laws are clearer regarding implementation, while the U.S.'s system is complicated due to the incorporation of sector laws, state laws, and FTC regulations.[114] The Supreme Court's continued reluctance to clarify the

---

[110] *See id.* (discussing Hubspot's plan to comply with GDPR and to provide guidance to others). HubSpot's legal team prepared for the May 2018 date by ensuring legal documents such as Customer Terms of Service, Data Processing Agreements, and Privacy Policies, are updated to reflect mandatory GDPR changes. *Id.* Also, companies are required to make consumers aware of what they are consenting to and inform them of their right to withdraw consent in advance. *Id.*

[111] *See id.* (discussing fundamental change in consent to use PII). "Essentially, your consumer cannot be forced into consent, or be unaware that they are consenting . . . ." *Id.*

[112] *See* Lee, *supra* note 50 (summarizing key differences between E.U. and U.S.). Both the 1995 Directive and the GDPR apply to all member-states and types of sectors within Europe. *Id.* On the other hand, the 1995 Directive and the GDPR only apply to U.S.'s sector-specific laws, such as HIPPA, rules only applicable to the financial sector, or certain laws regarding specific risk groups, such as children, whom are protected under COPPA. *Id.*

[113] *See id.* (explaining differences between states). One notable example is the California Online Privacy Protection Act of 2003, which states that the right to privacy is enshrined in the state of California's constitution. *Id.* Similarly, Massachusetts has positioned itself to follow this same stringent standard; also, a large amount of U.S. companies are based out of these two states with stricter standards. *Id.*

[114] *See id.* (noting difficulty for businesses to apply U.S. privacy laws due to multiple controlling agencies). The FTC regulates and enforces trade on a federal level in the U.S and pursues businesses that engage in unfair or deceptive practices relative to private data. *Id.* The FTC will seek consent decrees to stop those businesses' conduct. *Id.* Typically, businesses will settle with the FTC and pay significant sums of money while also being subject to 20-year audits by the FTC. *Id.* On top of the federal regulations, there are sector specific rules which are regulated by specific commissions, such as privacy breaches in the communication sector. *Id.* At the state level, legislatures typically pass a set of laws regarding data breaches and collection of PII that are regulated by the Attorney General, who may bring an action against a company on behalf of state consumers. *Id.* At the consumer level, groups of consumers that are harmed by a business's wrongdoing can collectively bring an action against that business. *Id.* Thus, due to the possibility of class action lawsuits and the high probability of damages, most companies are highly

definition of PII as it pertains to online tracking activity will lead to uncertainty in the law for consumers and providers alike.[115]

A. Personal Information vs. Linkable Information

Companies must understand that linkable information is a "term to define IP addresses, MAC addresses, and other device identifiers which identify **a thing**, not a **person**, but can be linked to an individual depending on what information is obtained."[116] Linkable information becomes PII when it is, or can reasonably be, associated or linked with an identifiable individual in other business records.[117] Thus, companies using such information should ensure that their privacy policies clearly define what they constitute as personal information – opting to include IP and Mac addresses as personal information and ensure that the policy and systems are up to standards.[118] This becomes exceedingly challenging when companies collect this information from European consumers and must work closely with their attorneys and IT support groups to fully comply with the GDPR's definitions.[119]

---

incentivized to comply. *Id.* However, at the same time, these companies do not have a consistent standard to follow. *Id.*; *see also* Lambert, *supra* note 61 (suggesting companies monitor IP and Mac identifiers if collecting information from European customers).

[115] *See Nickelodeon*, 827 F.3d at 272-73 (lacking uniform federal law and expansion of scope of privacy). In denying certiorari, the Supreme Court affirmed the Third Circuit's dismissal of claims regarding federal video privacy protections under the 1988 statute, which prohibits videotape service providers from knowingly disclosing customers' personally identifiable information, finding that it is not intended to reach the conduct of Google and Viacom. *Id.* The Third Circuit found that links for viewed videos and "static digital identifiers," such as unique device identifiers or internet protocol addresses, were not considered PII under the statute. *Id.*

[116] *See* Lambert, *supra* note 61 (suggesting strategies for businesses utilizing PII).

[117] *See id.* (offering examples of when information is PII). Example of linkable information includes a driver's license and a license plate. *Id.* A driver's license is considered personal information because it has your name, photo, address, social security number, and other information that identifies you specifically. *Id.* On the other hand, a license plate identifies a piece of property, which is your car. *Id.* As a result, a license plate does not contain personal information on its own, but is linkable information. *Id.* However, once a company is able to combine a license plate with a driver's license, the license plate becomes personal information and should be treated as such. *Id.* Similarly, a phone number is a thing and therefore is linkable information; however, if that phone number is linked to a recording of one's voice, the phone number becomes personal information. *Id.* Lastly, an IP address in a company's server log alone is solely linkable information not associated with a particular person, and therefore, is not personal information. *Id.* However, once an IP address becomes part of an electronic signature record where the IP address is collected and stored alongside a person's name, time, and date of acceptance, it becomes personal information that is liked to a specific person. *Id.*

[118] *See id.* (stating failure to comply gives rise to investigation and potential litigation).

[119] *See id.* (depicting challenges and differentiating requirements in E.U. versus U.S.).

U.S. Federal Courts have conflicting views regarding what constitutes PII; the Third Circuit held that the links to videos viewed were not PII while the First Circuit held that the "USA app" violated the VPPA by recording and sending information to Adobe Systems Inc. which provided the videos watched by the plaintiff.[120] One argument supporting qualifying IP and similar identifiers is that that PII relies on the assumption that if linkable information is, or reasonably can be, associated with an identifiable individual, it triggers PII protections.[121] The difference between the FTC's view versus a company such as Google's turns on the latter's inclusion of a "reasonableness standard" compared to the former's view that privacy protections are automatically triggered when PII "can be *reasonably linked* to a particular person. . . ."[122] This simply suggests that if the identifier can be associated with an identifiable individual, it should be considered PII.[123]

B. Necessity of Compliance

The FTC and other U.S. government authorities have a strong interest in complying with the GDPR in order to protect their own ability to trade, uphold a competitive trading stance, and uphold moral obligations to U.S. citizens as other countries around the world begin to adopt similarly stringent policies.[124] Practically speaking, the U.S. will certainly continue to be pressured to adhere to the GDPR requirements if they desire to continue business relations with not only the European countries, but with E.U. citizens across the world.[125] Nonetheless, the implementation of the GDPR and its key changes will be burdensome because it requires a new operational

---

[120] *See id.* (providing two conflicting opinions by federal courts).

[121] *See* Lambert, *supra* note 61 (outlining straight forward argument providing understanding of what is identifiable information).

[122] *See id.* (highlighting varying understandings between company and federal government).

[123] *See id.* (referring to stricter standards followed by companies).

[124] *See* Truran, *supra* note 103 (stressing companies must adhere to GDPR unless they are certain no data regarding E.U. citizens utilized). The GDPR is increasingly relied upon as the standard model by countries seeking to impose fines or penalties on non-E.U. based companies through local data protection regulations and the implementation of DPAs. *Id.* However, in the U.S., where there is not a DPA, enforcement will come through the closest equivalent - the FTC. *Id.*

[125] See Shearer, *supra* note 26 (explaining how two models are in direct conflict).

> The US has, since before the year 2000, been decreasing protections of non-US citizens from the activities of US companies, and ever-increasing intrusion by the NSA and other US organisations. The EU has, over the same period, decided to base its economic future around giving its citizens reason to trust online markets, and has focused that trust on strict controls on handling personal data. These two things are totally in conflict.

Id.

practice and protocol regarding collecting, maintaining, and handling of E.U. citizens' information, which experts foresee as ultimately increasing the existing divide due to push back from U.S. companies.[126] In addition to the confusion as to whether or not the GDPR even applies to a specific company or how it will be enforced, a chaotic barrier will likely be created as companies may avoid them in full by opting to not do business with the E.U. at all rather than risk failing to comply.[127] This regulation can negatively impact the E.U.-U.S. business relationships and the growing consumer demand of seamless transactions that may not be permitted under the GDPR.[128]

C. Benefits of Compliance

However, companies can use the GDPR to rebuild any existing lost sense of trust with their consumers through transparency.[129] One study found that 56% of consumers are under the impression that brands collect their data without consent and would prefer more transparency; another study found that 75% of consumers are willing to share their data if they trust the brand and 80% are willing to do so in exchange for special offers or benefits, such as reward points or personalized recommendations.[130] Ultimately, the GDPR provides consumers with the power to control how companies and marketers use and store their data, while presenting companies with an opportunity to

---

[126] *See* Dellinger, *supra* note 102 (fearing clash of two different standards increases barrier and highlights differences rather than unifying). Various businesses in the U.S., especially smaller sized organizations, may not even be aware that they are subject to the GDPR and will not have begun the immensely complicated process of complying, inclusive of integrating new systems, separating data, and educating employees. *Id.*

[127] *See id.* (effectuating reality of GDPR).

[128] *See id.* (arguing GDPR may not be most balanced model in practice). Experts explain that consumer demand to remove "friction" in transactions resulted in "one-click" checkouts online and has increased quick functional tools that may not be in compliance with the GDPR's requirement of explicit consent, as the company would be storing individuals' information to immediately recall it for them. *Id.* In addition to the demand of a "seamless" transaction, individuals themselves are willingly sharing immense volumes of data about themselves. *Id.* The following sentence is incredibly long and complex, I began to try and edit, but I think you are better off breaking it up into a few sentences. Practical challenges of implementing the GDPR in the U.S. include training employees of all levels, high costs of implementation, lack of awareness, checkpoints, and guidance; difficulty in converting data-giants like Facebook and Google that already allow vast amounts of publicly accessible information, pushback regarding the E.U.'s actual ability to enforce the sanctions, will be actually able to enforce these sanctions, and practical problems in obtaining actual consent, especially from minors, due to the difficulty in determining whether the actual card holder was also the purchaser. *Id.* "Only time will tell if GDPR provides the correct balance of privacy and convenience or if it will create too much of a burden for companies to comply." *Id.*

[129] *See* O'Brien, *supra* note 107 (explaining majority of people believe advertisers lack integrity).

[130] *See id.* (presenting statistics and arguing in support of benefits of GDPR).

reestablish trust.[131] Proponents argue that the GDPR's data-driven foundation will redefine marketing by requiring marketers to "legally justify every bit of data they're holding," which in turn will end unpopular marketing tactics and establish trust between marketers and consumers.[132]

Companies anticipate that they will have to change security protocols and alter how they collect customer data to use as well as the length of time they can store the data.[133] Most companies are planning more social media marketing and content marketing, while shying away from retargeting ads, which also require their customers to log in for services.[134]

V. CONCLUSION

In the absence of a definitive Supreme Court ruling, the application of the VPPA, COPPA, and the definitions of personally identifiable information along with its privacy protections will continue to evolve in the lower courts, resulting in further circuit splits. Although the U.S. courts are split, the additional implications of the GDPR will require companies to implement strategies of compliance and ensure they have systems in place that enable them to adhere to the E.U.'s data holding and consent protocols, prior to being subject to fines or negative impacts on their reputations. Further, the California Act, though less comprehensive than the GDPR, will have a sweeping nature after its implementation in 2020, and will require companies to expend a great deal of efforts to achieve compliance, even reaching companies outside its state lines. Thus, businesses should be cautious when collecting IP addresses due to the current circuit splits and variation that exists between sector and targeted groups. Lastly, businesses must continue being GDPR compliant, as well as prepare to implement strong compliance programs suitable for the California Act's nuances before their reputations and profits are jeopardized.

Aleksandra Popova

---

[131] *See id.* (balancing high costs and impacts of GDPR with benefits and opportunities companies may derive).

[132] *See id.* (explaining GDPR removes opt-ins; long jargon-filled terms and conditions; and uninvited email list).

[133] *See* An, *supra* note 108 (describing access companies will have to alter).

[134] *See id.* (addressing new marketing tactics to avoid data regulations).