Mining for Children’s Data in Today’s Digital World

Damin Park

Follow this and additional works at: https://digitalcommons.pepperdine.edu/naalj

Part of the Administrative Law Commons, Internet Law Commons, Judges Commons, and the Privacy Law Commons

Recommended Citation
Available at: https://digitalcommons.pepperdine.edu/naalj/vol38/iss1/12

This Comment is brought to you for free and open access by the Caruso School of Law at Pepperdine Digital Commons. It has been accepted for inclusion in Journal of the National Association of Administrative Law Judiciary by an authorized editor of Pepperdine Digital Commons. For more information, please contact Katrina.Gallardo@pepperdine.edu, anna.speth@pepperdine.edu, linhgavin.do@pepperdine.edu.
Mining for Children’s Data in Today’s Digital World

By Damin Park

I. INTRODUCTION..................................................................................................................321

II. BACKGROUND ....................................................................................................................323
   A. Technology’s Grip on Children ....................................................................................323
   B. Children and Smartphone Apps in the U.S. ...............................................................325
      1. In the Real of Education .........................................................................................326
   2. Behavioral Marketing .................................................................................................327
   C. Children and Mobile Gaming Apps ............................................................................328

III. DIGITAL PRIVACY ..........................................................................................................330
   A. Privacy Law in California ..........................................................................................335
      1. Marketing Geared Towards Children .....................................................................336
   B. Children’s Online Privacy Protection Act .................................................................338
      1. Amendments and Limitations ................................................................................338
   C. Data Security .............................................................................................................340

IV. CONSEQUENCES OF A LARGE DIGITAL FOOTPRINT....................................................342
   A. Balancing Rights Between the Parents and Child .....................................................343
   B. Legal Vs. Moral Argument .........................................................................................344
   C. Potential Harms .........................................................................................................345

V. POSSIBLE REMEDIES ....................................................................................................346

VI. CONCLUSION ..................................................................................................................351
I. Introduction

My nephew, a goofy one-year-old who is yet unable to talk, is like most young kids today: playful, curious, and surprisingly skilled at navigating a smartphone. Just ten years ago, seeing a toddler with a smartphone—let alone using one so naturally—would surprise most. In 2018, however, young children using smartphones is increasingly becoming a common sight to behold in this tech-pervasive world. Since the 1990s when the internet was first popularized in the United States,\textsuperscript{1} there have been massive innovations in technology that affect the way we drive, do business, advertise, entertain, and even the way we raise our children. In fact, the percentage of Americans who use the internet has jumped from just 52\% in 2000 to 88\% in 2016.\textsuperscript{2} Moreover, mobile devices and other similar technology play a significant role in children’s lives today regardless of age, gender, and family income levels.\textsuperscript{3} Today, 98\% of children age eight and under live in a home with a mobile device.\textsuperscript{4}

Notwithstanding the innovative changes that come with these technological advances, they also bring with them new problems to consider. As technology continues to entangle itself within the intimate corners of our lives, there are increasing issues with privacy,

\textsuperscript{1} Damin Park is a Juris Doctor candidate for the Class of 2019 at Pepperdine University School of Law. Damin received her Bachelor of Arts in English Literature at the University of California, Los Angeles. I would like to thank all the editors that helped fine-tune this comment, and my parents, Noah and Cindy Park, for encouraging and guiding me through all of life’s obstacles. Your love and support mean the world to me.

\textsuperscript{2} Lauren Estacio, Protecting the User: The Necessity of Governing the Privacy Settings of Social Media Websites, LAW SCHOOL STUDENT SCHOLARSHIP, 1, 2 (2013), http://scholarship.shu.edu/cgi/viewcontent.cgi?article=1156&context=student_scholarship.

\textsuperscript{3} Aaron Smith, Record shares of Americans now own smartphones, have home broadband, Pew Research Center (Jan. 12, 2017), http://www.pewresearch.org/fact-tank/2017/01/12/evolution-of-technology/.

\textsuperscript{4} Victoria Rideout, The Common Sense Census: Media Use by Kids Age Zero to Eight 3 (2017). A 2017 study surveyed media use among children from birth to age eight who come from all regions of the United States across a diverse demographic of candidates, taking into consideration race, income level, ethnicity, and gender.

\textsuperscript{4} Id.
especially those concerning children, which must be addressed.\textsuperscript{5} Indeed, 69\% of parents with children eight and under have expressed concern over advertising in relation to their child’s use of media.\textsuperscript{6}

One concerned parent brought a lawsuit against The Walt Disney Company alleging that the company violated the Children’s Online Privacy Protection Act (COPPA) in some of its children’s apps.\textsuperscript{7} The lawsuit specifically names the app Disney Princess Palace Pets as the one that tracked her child, and also lists forty-two other Disney apps that allegedly violate COPPA.\textsuperscript{8} According to the lawsuit, the allegations claim that these gaming apps by Disney, while not collecting personal data such as email addresses, collects more “obscure data” such as a smartphone’s “persistent identifier”\textsuperscript{9} which is unique to each mobile device.\textsuperscript{10} To a layperson, this may not sound as threatening or serious as it has the potential to be. In fact, this data has the capacity to be used to follow a child’s activity through multiple apps and across different devices.\textsuperscript{11} Even more problematic, this data is sold to third-parties who may use the information for themselves or sell again for further profits.\textsuperscript{12} This lawsuit, moreover, is not the first time Disney has faced this issue, and probably not its

\textsuperscript{5} Id.

\textsuperscript{6} Id. at 7.

\textsuperscript{7} Shayna Posses, Disney Slapped With Suit Over Games That Swipe Kids’ Info., Law 360, (Aug. 4, 2017), https://advance.lexis.com/document?pdmfid=1000516&crid=46e910e5-bd65-4bd9-be16-c765ed478a8&pdworkfolderid=5cbe352a-d0b3-4391-b9f9-4ce4bb71b19&ecomp=gpptk&carg=5cbe352a-d0b3-4391-b9f9-4ce4bb71b19&prid=274df851-cdf8-4b14-9e05-67f1b661369c (Amanda Rushing, on behalf of her child L.L., brought a lawsuit against The Walt Disney Co. on the basis that Disney’s apps violated privacy laws by tracking and collecting L.L.’s information without parental consent and sending that information to third parties for advertisement purposes).


\textsuperscript{9} “Persistent identifiers,” also commonly known as “cookies,” can track a user’s online activity and provide information such as geolocation, photos, videos, and audio recordings. See infra text accompanying note 81.

\textsuperscript{10} Vanian, supra note 8.

\textsuperscript{11} Id.

\textsuperscript{12} Id.
last. Ultimately, the plaintiff wishes that Disney and other similar companies would cease tracking practices and get rid of any personal data obtained through these deceptive methods.

This article will explore the history of privacy law and examine the flaws, successes, and features of past privacy policy enforcement regimes. It will also address reasons compliance has been so messy and hard to enforce, explore avenues of possible solutions, and suggest recommendations for how to best tackle the problem. Part II details the increasing presence of technology in children’s lives by examining relevant data regarding children’s use of technology as well as the impact that this increased presence has on children’s lives. Part III goes through the entities, laws, and regimes that were or currently are in place in regard to privacy law. Part IV studies the consequences and implications of having the majority of a person’s life tracked through data and what this means for the children of the future. Part V explores the possible remedies that are available to us, and Part VI concludes on the legal and practical impact these new privacy concerns have on the world today.

II. BACKGROUND

A. Technology’s Grip on Children

From the television to the internet and now to mobile devices, children today have a plethora of technology to choose from as their form of entertainment. But how has the advent of the smartphone changed children’s screen time with other media, such as the television or a gaming console? According to a 2017 study by Common Sense:

13 Brian Fung, These 42 Disney Apps are Allegedly Spying on your Kids, Washington Post (Aug. 07, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/08/07/these-42-disney-apps-are-allegedly-spying-on-your-kids/?utm_term=.45697894ac3e. In 2011, Disney’s subsidiary, Playdom, was penalized $3 million after the Federal Trade Commission discovered that it registered 1.2 million users, most of whom were children, for online games.

14 Vanian, supra note 8.

15 Rideout, supra note 3.
[S]ince 2011[,] time spent watching DVDs is down by 14 minutes a day, time spent watching a television set is down by 11 minutes a day, time spent playing video games on a console or handheld game player is down by eight minutes, and time spent using a computer is down by seven minutes—a total drop of 40 minutes a day in use of those screen devices.\(^{16}\)

Despite such a drop in each of these categories, the loss in forty minutes of screen time is made up for in the use of mobile devices: there has been an increase in mobile device usage of forty-three minutes a day—almost exactly as how much time was lost in the usage of the other devices.\(^{17}\) The fact that mobile devices have absorbed this decrease in children’s use of DVDs, various gaming devices, and computers suggests not only that mobile devices serve as a three-in-one device, but also that children prefer mobile devices to all the previously used media.\(^{18}\) Not surprisingly, children today spend vastly more time playing games on mobile devices such as tablets or smartphones rather than on previously popular console players, computers, or handheld gamers.\(^{19}\)

Specifically, among five-to-eight year-olds, 59% have a tablet, 9% have an iPod Touch or similar device, and 7% have their own smartphone.\(^{20}\) Moreover, 84% of children eight or under have used a mobile device,\(^{21}\) and 71% of parents reported to having downloaded apps for their children to use.\(^{22}\) Even toddlers are not immune: 46% of children under two have used mobile media,\(^{23}\) with a reported average of seven minutes a day spent on mobile devices.\(^{24}\)

\(^{16}\) *Id.* at 13.

\(^{17}\) *Id.*

\(^{18}\) *Id.*

\(^{19}\) *Id.* Children spend an average of 16 minutes a day gaming on mobile devices, five minutes a day on console players, three minutes on computers, and one minute on handheld gamers. *Id.* at 31.

\(^{20}\) *Id.* at 23.

\(^{21}\) *Id.* at 24.

\(^{22}\) *Id.* at 26.

\(^{23}\) *Id.* at 37.

\(^{24}\) *Id.* at 15.
All this is to say, children seem to like mobile devices just as much as or even more so than adults do, and technology does not seem to be going anywhere.\textsuperscript{25} The problem is, children often do not have the proper learning or even the mental capacities to understand the complexities of privacy and more importantly, to appreciate the significance of guarding privacy, especially in this digital age we live in today.\textsuperscript{26} In anticipation of these issues, the government, parents, app developers, and educators must begin to consider the regulation of digital privacy and the enforcement of privacy laws in terms of how they affect children’s psychosocial development.\textsuperscript{27} Privacy in the digital realm is especially important because it gives children the security to freely explore and search out their identities and interests without the possibility of being exposed or investigated.\textsuperscript{28} Moreover, the concept of privacy stands at the core of important American values such as “autonomy, self-determination, and dignity,” which positions privacy at the forefront of “civic and political engagement” among youth.\textsuperscript{29}

\textit{B. Children and Smartphone Apps in the U.S.}

In 2013, the Federal Trade Commission (FTC)\textsuperscript{30} modified its scope of protection in digital privacy by revising the definition of “personal information” that cannot be collected without verifiable parental consent to include photographs, voice recordings, and device identifiers.\textsuperscript{31} In addition, in June 2017 the FTC updated its six-step compliance plan\textsuperscript{32} for businesses bound by its COPPA rule to reflect

\textsuperscript{25} \textit{Id.}

\textsuperscript{26} Kathryn C. Montgomery, Jeff Chester, and Tijana Milosevic, \textit{Children’s Privacy in the Big Data Era: Research Opportunities}, 118, 118 (Apr. 19, 2017), http://pediatrics.aappublications.org/content/140/Supplement_2/S117.

\textsuperscript{27} \textit{Id.}

\textsuperscript{28} \textit{Id.}

\textsuperscript{29} \textit{Id.}

\textsuperscript{30} Federal Trade Commission, FTC.\textit{GOV}, https://www.ftc.gov/about-ftc/what-we-do (last visited Feb. 5, 2018). The FTC is in charge of enforcing privacy laws such as COPPA. \textit{Id.}


\textsuperscript{32} See infra note 133.
the rise of technologies and other recent developments in the marketplace.\textsuperscript{33}

With smart phones’ ever pervasive presence in Western consumers’ lives, they likely become a part of a child’s life very early on.\textsuperscript{34} In fact, a BBC survey found that more than three-quarters of ten to twelve-year-olds have social media accounts.\textsuperscript{35} In addition, the amount of time that children between eight and eleven spend online has more than doubled in a decade.\textsuperscript{36}

1. In the Realm of Education

Privacy concerns with increased smart phone app usage in education settings have recently arisen as well.\textsuperscript{37} As the undeniable benefits of technology continue to flood our lives, the school system has taken a step towards innovative education methods using technology.\textsuperscript{38} School districts often contract with third parties called “application service providers” for special technological services in the classroom.\textsuperscript{39} These apps include popular programs such as Google Apps for Education and Khan Academy.\textsuperscript{40}

Although these new education methods provide practical benefits to students using them, such practices also raise privacy concerns and create the possibility of invading the privacy of these children who


\textsuperscript{34} “In the United States, 92% of two-year-olds already have an online presence.” Stacey V. Steinberg, \textit{Sharenting: Children’s Privacy in the Age of Social Media}, 66 EMORY L.J. 839, 849 (2017).


\textsuperscript{36} Citron, \textit{supra} note 31.

\textsuperscript{37} Alex M. Peddy, \textit{Dangerous Classroom “App”-itude: Protecting Student Privacy from Third-Party Educational Service Providers}, 17 BYU EDUC. & L. J. 125, 127.

\textsuperscript{38} Id.

\textsuperscript{39} Id.

\textsuperscript{40} Id.
use these operators’ products. Specifically, three substantial risks include: “[(1)] illegal data collection, [(2)] susceptibility to criminal activity, and [(3)] identity theft caused by hacking.” Students are at risk of illegal data collection by hackers, which include both advertisers and criminals. These methods are dangerous because data tracking methods often track personal information such as a student’s name, address, or location. Next, the student’s information may also be at risk of criminal activity such as “identity fraud, harassment, and stalking.” The third major concern is that entire school databases may be vulnerable to hackers, which can lead to identity theft by stealing students’ names, birthdays, and social security numbers. These serious risks provide even more urgency for the need for better enforcement and regulation of privacy laws in a digital landscape.

2. Behavioral Marketing

Behavioral marketing is a method of business that “targets consumers based on their behavior on websites rather than purely by the content of pages they visit.” The types of technology used in these behavioral marketing algorithms raise privacy concerns because they track the private interests of the consumers in a non-obvious way. To be more specific, these algorithms run in the background of a personal search; thus, “the technologies and the information that they capture are generally invisible to most consumers.” These potentially damaging effects of commercial practices and the collection of personally identifiable data are

41 Id. at 128.
42 Id.
43 Id.
44 Id.
45 Id.
48 Id.
additional problems we must pay close attention to in the protection of children through more stringent and comprehensive privacy laws.\(^49\)

In addition, the popularity of popular social networking sites raises new legal issues regarding consensual marketing, which spurs debate on the limits of personal data collection.\(^50\) This is a growing problem in a world where it is common for children as young as ten to have social media accounts.\(^51\)

\section*{C. Children and Mobile Gaming Apps}

Many privacy issues relating to children arise in the area of gaming apps—evidently among the more popular of app categories.\(^52\) But just how well do these apps protect privacy? Serge Egelman, “a research director of the Usable Security & Privacy Group at the International Computer Science Institute,” conducted an experiment to test just that.\(^53\) By creating an “automated test bed that allow[ed] them to download and install apps to a series of mobile devices, simulate the behavior of users . . . and then monitor the traffic flowing in and out of the devices,”\(^54\) Egelman and others involved in the study were able to determine whether certain apps participated in tracking behavior, and if so, whether they shared the information with third parties.\(^55\)

\(^{49}\) Id.

\(^{50}\) Id.

\(^{51}\) See Doward, supra note 35.

\(^{52}\) Most popular Google Play app store categories from 1st quarter to 3rd quarter 2016 and 2017, by number of downloads (in millions), STATISTA, (last visited Feb. 05, 2018), https://www.statista.com/statistics/256772/most-popular-app-categories-in-the-google-play-store/. According to a study of the Google Play app store by Statista, gaming apps were ranked the most popular category with 6.9 million app downloads. Id.


\(^{54}\) Id. The test bed was “limited to Android apps for the sole reason that the Android platform is open source.” Id.

\(^{55}\) Id.
Of the more than 5,000 apps examined, over 50% of the Google Play apps meant for children under thirteen seemed to fail at protecting data. According to the study, the apps often sent “potentially sensitive information—including device serial numbers, which are often paired with location data, email addresses, and other personally identifiable information—to third-party advertisers.” More troublingly, more than 90% of those apps were those “transmitting identifiers,” which are akin to “hardware serial numbers” that allow for long-term tracking and cannot be changed or deleted.

Although reusing “ready-to-use code” from different third parties allows app developers to save time and decreases the potential for error, these same time-saving, error-reducing shortcuts may be a contributing factor to why so many of the tested apps failed to adequately protect privacy. This is because regardless of who wrote the code used for the app, the app developer remains liable for whatever code is included in their apps. However, the problems with compliance are not the end of the issue; enforcement of these regulations is a pressing problem as well. With more and more potential COPPA violations being revealed with lawsuits such as the one brought by Ms. Rushing, app stores like Google Play and Apple’s iTunes Store as well as regulatory agencies such as the FTC are not wholly without fault.

In fact, the FTC has influential power over certain actions. The FTC has the ability to publish guidelines and press releases concerning certain issues. When it does this, the FTC in effect creates a “soft law” by intentionally not specifying the portions of the

---

56 Id.
57 Id.
58 Id.
59 Id.
60 Id.
61 Id.
62 See Posses, supra note 7.
63 See Federal Trade Commission, supra note 30.
64 Rebecca Lipman, Online Privacy and the Invisible Market for Our Data, 120 Penn St. L. Rev. 777, 790 (2016).
65 Id.
guidelines or recommendations that would be mandatory by law and what portions are merely encouraged as “best practices.”

Larger companies show a tendency to follow even these “soft laws” as a cautionary measure to prevent unwanted enforcement actions.

III. DIGITAL PRIVACY

What protections do we have over our privacy in this digital world? A good starting point is the Fourth Amendment to the United States Constitution, which states, “The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . .” The Fourth Amendment is the source of our constitutional right to be protected against unreasonable searches and seizures. As the world developed, the law quickly caught up to extend this protection in searches of digital data as well.

However, while technology and advertising continue to flourish at a rapid pace, education and scholarship on privacy concerns related to children is moving at a much slower speed. The staggering amount of innovation that has taken place in “computer technology, artificial intelligence, digital communication networks, and sophisticated data processing and analysis have vastly improved how data can be gathered and processed.” Although these improvements are good for business and marketing in that newer digital marketing practices can now be utilized for selling products, they can also create complications for the realm of digital privacy. These complications arise as third-party data collectors encroach more and more onto people’s lives, analyzing our interests against personal information about ourselves such as age, gender, and race.

---

66 Id.
67 Id.
68 U.S. CONST. amend. IV.
69 Id.
70 Lipman, supra note 64, at 787.
71 Montgomery, supra note 26, at 118.
72 Id.
73 Id.
74 Id. at 118–19.
For instance, these new data gathering and marketing strategies are being used “to identify children and youth of color . . . and [to] create targeting marketing messages based on their ethnicities and cultures.”\textsuperscript{75} In addition, “[a] data broker-created category containing high numbers of low-income minorities might be targeted with high-interest payday loans.”\textsuperscript{76} To illustrate how these “profiling” practices work, we may consider the fact that the FTC conjectures that a category called “Biker Enthusiasts” might be used by advertisers who want to sell motorcycles, but also by a company that is looking for “signs of risky behavior.”\textsuperscript{77} Moreover, the fact that many of these methods are “invisible” also makes raising the importance about guarding data and personal information more difficult and practically harder to enforce.\textsuperscript{78} These practices are a sobering reminder that privacy issues that arise from marketing tactics may lead to exploitation of certain vulnerable individuals in society, namely children, who are unable to comprehend the gravity of privacy violations, or even that it is happening at all.\textsuperscript{79}

So how does the tracking work? Smartphone apps generally count on third-party services to improve user experience by reporting any bugs that the app may have and tracking the app for user information and ad integration.\textsuperscript{80} The most common practice today is for mobile platforms to give users the option of either enabling or disabling permissions for each app.\textsuperscript{81} However, the issue with this model is that there is a lack of general knowledge and transparency regarding the information harvested by these third-party services.\textsuperscript{82} Specifically, some users may be wholly unaware of the implications of giving an app permission to access their data.\textsuperscript{83} Users are also

\textsuperscript{75} Id.
\textsuperscript{76} Lipman, supra note 64, at 781.
\textsuperscript{77} Id.
\textsuperscript{78} Id. at 783.
\textsuperscript{79} Montgomery, supra note 26, at 118.
\textsuperscript{81} Id.
\textsuperscript{82} Id.
\textsuperscript{83} Id.
often uninformed about which apps use the same third-party services, which would make these users extra vulnerable to a third party’s massive data mining operations. In other words, there is an “intuition gap” here which demonstrates that people do not completely understand how public their data actually is because it still “feels” private when they use their apps on their phones. Although users may have knowledge that they have enabled others to access their personal information, there is still no “physical trigger” which warns users about what information to disclose or to be cautious about behavior patterns when using apps. In fact, a 2010 report by the FTC to Congress claimed that “The Notice and Choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand.” Bridging this “intuition gap” might encourage more smartphone users, especially concerned parents, to guard and protect themselves and their children from data exploitation and invasion of privacy.

Although Congress has made efforts to increase protections for regulating privacy in specialized areas, namely through passing statutes such as the Family Educational Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPPA), increasing privacy concerns suggest that these

---

84 Id.
85 Lipman, supra note 64, at 785.
86 Id.
88 Id. at 786.
90 HIPAA (Health Insurance Portability and Accountability Act), (last updated July 2017), “provides data privacy and security provisions for safeguarding medical information.” http://searchhealthit.techtarget.com/definition/HIPAA.
statutes are not enough. This is because these particularized statutes only cover limited types of information in factually narrow situations.

Moreover, the FTC has shown “significant interest in privacy through reports on facial recognition technology, privacy disclosures in apps, and privacy issues in apps aimed at children.” Specifically, section 5 of the Federal Trade Commission Act prohibits “unfair or deceptive acts or practice.” This broad language allows the FTC to review and penalize companies that try to deceive or scam people, including children. Unfortunately, this, too, has problems in its application. The problem with section 5 is that the language necessitates an actual lie, which creates problems with companies exploiting this bright line with gray areas. The language of the statute created a loophole where companies could intentionally be vague about its privacy policies or read privacy policy in an overbroad manner so that section 5 of the Federal Trade Commission Act would not apply.

When the internet first started to take hold in American society, Congress passed legislation to tackle this problem directly. The Electronic Communications Privacy Act of 1994 (ECPA), “one of the broadest statutes that applies to today’s electronic environment,” protected data at a time when older technologies such as floppy disks and cassette tapes were more common and used to store digital data such as letters, messages, and transcripts of letters. The ECPA also covers communications relating to voice, data, and electronically-stored communications and “prohibits the interception of, access to, and disclosure of such communications.” However, even with amendments, laws such as this are outdated and are unable to resolve

---

91 Lipman, supra note 64, at 787.
92 Id. at 788.
93 Id. at 789.
94 Id.
95 Id.
96 Id. at 790.
97 Id.
98 Estacio, supra note 1, at 18.
99 Studwell, supra note 47, at 234.
100 Estacio, supra note 1, at 2.
web-based or social media abuse problems.\textsuperscript{101} This is due to the fact that the language of the statute seeks to control the way a communication is stored or intercepted to reflect the needs of the time in which the legislation arose.\textsuperscript{102} Today, there is a need for emphasis on law that directly protects individual privacy. Unfortunately, at this time there is no inclusive legislative privacy scheme that governs data privacy and social media abuse in the United States,\textsuperscript{103} nor is there any law that clearly defines an individual’s right to privacy from the eyes of other individuals with respect to information on the internet.\textsuperscript{104}

There have been actions by other administrative agencies to further address these limiting issues. For instance, the FCC has taken steps to regulate data security.\textsuperscript{105} The Fair Credit Reporting Act (FRCA) was passed to give the FTC enforcement authority over companies that provide consumer reports.\textsuperscript{106} The FRCA “regulates the ability of financial institutions to share customer’s credit-related data with its affiliates” by obliging them to provide customers with “disclosure, notice, and an opt-out option before such information is shared.”\textsuperscript{107} This allowed the FTC to bring charges under the FRCA when companies exploiting the loophole “fail[ed] to properly verify their information, fail[ed] to ensure that their information will only be used for legally permissible purposes, or fail[ed] to notify consumers about the information they are selling about them.”\textsuperscript{108} Furthermore, the FTC also has the power to bring charges under the COPPA\textsuperscript{109} when companies gather private information from children without parental consent.\textsuperscript{110} Despite the above-mentioned methods of

\textsuperscript{101} Id.
\textsuperscript{102} Id.
\textsuperscript{104} Estacio, \textit{supra} note 1, at 18.
\textsuperscript{105} Lipman, \textit{supra} note 64, at 792.
\textsuperscript{106} Id.
\textsuperscript{107} Estacio, \textit{supra} note 1, at 19.
\textsuperscript{108} Lipman, \textit{supra} note 64, at 792.
\textsuperscript{109} See \textit{infra} Part III, Section D.
\textsuperscript{110} Lipman, \textit{supra} note 64, at 792.
enforcement, the FTC is still very limited in its ability to deal with digital privacy concerns more completely.\textsuperscript{111}

\textit{A. Privacy Law in California}

States such as California have passed their own laws to further protect citizens’ private data.\textsuperscript{112} Section 22575 of California’s Business and Professions Code requires that “any website collecting personally identifiable information must ‘conspicuously post’ a privacy policy on its website.”\textsuperscript{113} In addition, the “Shine the Light” law, section 1798.83 of California’s Civil Code, requires disclosure by companies if the companies sold a consumer’s personal information for purposes of direct marketing, or they must alternatively allow the consumer to opt out of the information sharing.\textsuperscript{114} Furthermore, if the company chooses to disclose this information, it must disclose both the “companies with which it shared the individual’s information and what information was shared.”\textsuperscript{115}

There has also been legislation geared toward protecting children, such as Section 22581 of California’s Business and Professions Code, which “requires that websites and apps allow minors to take down content they previously posted.”\textsuperscript{116} Although this is progress, the issue still remains that even if a website such as Facebook allows a minor to remove a photo that he or she had put up earlier, the photo may have been disseminated to third-party websites already by the time the user removes it.\textsuperscript{117} California also passed the Student Online Personal Information Protection Act in 2014 which works to “regulat[e] educational apps that track students’ development.”\textsuperscript{118} The Act makes illegal “targeted advertising, using students’ data to build a profile about them for non-educational purposes, and selling

\textsuperscript{111} Id.
\textsuperscript{112} Id. at 793.
\textsuperscript{113} Id.
\textsuperscript{114} Id.
\textsuperscript{115} Id. at 794.
\textsuperscript{116} Id.
\textsuperscript{117} Id.
\textsuperscript{118} Id.
or disclosing students’ information.” 119 Although bills similar to California’s Student Online Personal Information Protection Act have been mentioned, Congress has yet to follow California’s lead. 120

While these laws seem like positive steps toward increasing protection of digital data, there are still many limitations. 121 For instance, the statute’s use of the phrase “direct marketing purposes” only covers solicitations made to consumers via phone, mail, or e-mail, 122 and fails to cover ads on websites and phones or collection by data brokers. 123 With these issues, marketing towards children produces its own problems as well.

1. Marketing Geared Towards Children

Because children are often quick to embrace new technologies, they are commonly pursued as the focal point of a flourishing and ever-growing e-commerce marketplace. 124 The one-to-one marketing tactics used by businesses require constant data gathering and monitoring of children’s behavior patterns online. 125 Because of this, complex marketing schemes used by these businesses often create issues related to privacy. 126

One new frontier of smart devices that have arisen in the category of children’s toys is a new generation of “interactive digital toys,” such as Mattel’s “Hello Barbie.” 127 This new smart toy “records a child’s voice, sends the recording to the Cloud, uses voice-recognition software to decode the content, and learns the child’s name, conversational styles, habits, and interests.” 128 In a recent test carried out by Which? and a German consumer group called Stiftung

---

119 Id. at 794–95.
120 Id. at 795.
121 Id. at 794.
122 Id.
123 Id.
124 Montgomery, supra note 26, at 118.
125 Id.
126 Id.
127 Id. at 119.
128 Id.
Warnest, the study group discovered that strangers could potentially talk to a child through his or her smart toy due to flaws in the toy’s Bluetooth and Wifi capabilities.\textsuperscript{129} Specifically, the investigation discovered that four out of seven toys that were tested had the potential to be used to communicate with the children who owned the toy.\textsuperscript{130} The security failures were found in the Furby Connect, i-Que Intelligent Robot, Toy-Fi Teddy and Cloud Pets.\textsuperscript{131} The specific issue in all these toys was that the Bluetooth connection had not been secured, "meaning the researcher did not need a password, pin or any other authentication to gain access."\textsuperscript{132} Not only that, but not much technical know-how was needed to hack into the toys to start conversations with the child.\textsuperscript{133} With the numerous vulnerabilities that already exist for children using the worldwide internet, we must take care to protect our children in every way possible, especially from vulnerabilities that are easily preventable such as the one with these products.\textsuperscript{134} With this new trend of smart toys, the aggregation of data collected from children born in this digital age will be massive. This raises the urgency for a comprehensive and effective enforcement mechanism that protects children from data mining and deceptive advertisement.\textsuperscript{135}

However, there are laws in California specifically catered towards protecting children’s privacy in the digital world.\textsuperscript{136} For instance, Section 22581 of California Business and Professions Code requires websites and apps to allow minors to take down content they previously posted.\textsuperscript{137} In addition, the Student Online Personal Information Protection Act of 2014 prohibits advertising that is targeted towards students, the use of students’ data to build a profile

\textsuperscript{129} Rebecca Smithers, Strangers can talk to your child through ‘connected’ toys, investigation finds, THE GUARDIAN (Nov. 2017), https://www.theguardian.com/technology/2017/nov/14/retailers-urged-to-withdraw-toys-that-allow-hackers-to-talk-to-children.

\textsuperscript{130} \textit{Id.}

\textsuperscript{131} \textit{Id.}

\textsuperscript{132} \textit{Id.}

\textsuperscript{133} \textit{Id.}

\textsuperscript{134} \textit{Id.}

\textsuperscript{135} \textit{Id.}

\textsuperscript{136} Lipman, supra note 64, at 794.

\textsuperscript{137} \textit{Id.}
about them for non-educational purposes, and the selling or disclosing of the students’ information to any other sources.\textsuperscript{138}

B. Children’s Online Privacy Protection Act

COPPA was enacted in 1998 and became effective in April of 2000 with the goal of protecting and promoting privacy for children who are under the age of thirteen.\textsuperscript{139} The act requires commercial websites and online services directed at children to obtain a parent’s permission for the collection or use of any personal information about a young child.\textsuperscript{140} It also gives companies obligations to fulfill these rules.\textsuperscript{141} For COPPA to apply, the operators of commercial websites and online services must have actual knowledge that their operations are “collecting personal information directly from users of another website or online services directed to children.”\textsuperscript{142}

Specifically, the law requires operators to clearly and comprehensively describe their “information practices” for the personal information gathered from children, obtain parental consent before gathering personal information from children, and allow parental access to children’s information to review or delete, among others.\textsuperscript{143}

1. Amendments and Limitations

COPPA was amended on July 1, 2013 to expand the definition of what it means to collect data from children.\textsuperscript{144} This revision

\textsuperscript{138} Id.


\textsuperscript{140} Montgomery, supra note 26, at 119.

\textsuperscript{141} Id.

\textsuperscript{142} Complying with COPPA: Frequently Asked Questions, supra note 139.

\textsuperscript{143} Id.

broadened the definition of children’s personal information\textsuperscript{145} to include what are called “persistent identifiers,” colloquially called “cookies,” which can track a user’s online activity, as well as include information such as geolocation, photos, videos, and audio recordings.\textsuperscript{146} These changes recognized the frequency with which young children access the internet through mobile devices such as smart phones and tablets, and also placed more stringent controls on identifying information such as geolocation information, photos, videos, and audio recordings.\textsuperscript{147}

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.\textsuperscript{148} For instance, although 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.\textsuperscript{149} In addition, children may simply lie about their age online, which research has shown is a common practice among children.\textsuperscript{150}

Texas has even gone farther from the amendments to further protect children in cases against app providers that collect location data without parental consent.\textsuperscript{151} Specifically, these agreements include injunctive relief forbidding app providers from collecting location data from children under thirteen with or without parental consent.\textsuperscript{152} However, even these efforts have limitations on the way consumers’ interests in the internet and digital privacy are protected, because COPPA provides no limitation on the type of data that can

\textsuperscript{145} Personal information includes information such as: “First and last name; A home or other physical address including street name and name of a city or town; Online contact information; A telephone number; A social security number . . . .” Complying with COPPA: Frequently Asked Questions, supra note 139.

\textsuperscript{146} Revised Children’s Online Privacy Protection Rule Goes Into Effect Today, supra note 144.

\textsuperscript{147} Studwell, supra note 47, at 236.

\textsuperscript{148} Montgomery, supra note 26, at 119.

\textsuperscript{149} Id.

\textsuperscript{150} Id.

\textsuperscript{151} Id.

\textsuperscript{152} Id.
be collected from children.\textsuperscript{153} That means everything from personal information, entertainment preferences, and audio recordings may be collected.\textsuperscript{154} Issues surrounding information privacy, database relationships, big data compilation of consumer information, and social media protections remain largely unanswered in any legislative scheme presented separately as a whole in the enactments presented above.\textsuperscript{155}

\textit{C. Data Security}

Companies in the tech industry are becoming more and more aware of the compliance issues that their apps have been facing, and some have implemented their own policies in hopes of lessening privacy law violations in this complex area of the law.\textsuperscript{156} For instance, Google has set in place a set of “COPPA-compliance checklists”\textsuperscript{157} that are presented to app developers who create apps in the “Family” category of the Google Play Store.\textsuperscript{158} Newly implemented programs such as Google’s “Designed for Families”

\begin{itemize}
\item Step 1: Determine if Your Company is a Website or Online Service that Collects Personal Information from Kids Under 13.
\item Step 2: Post a Privacy Policy that Complies with COPPA.
\item Step 3: Notify Parents Directly Before Collecting Personal Information from Their Kids.
\item Step 4: Get Parents’ Verifiable Consent Before Collecting Personal Information from Their Kids.
\item Step 5: Honor Parents’ Ongoing Rights with Respect to Personal Information Collected from Their Kids.
\item Step 6: Implement Reasonable Procedures to Protect the Security of Kids’ Personal Information.
\end{itemize}

\textsuperscript{153} Id.
\textsuperscript{154} Id.
\textsuperscript{155} Id.
\textsuperscript{156} Egelman, supra note 53.
\textsuperscript{157} \textit{Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business}, Federal Trade Commission, FTC.GOV, \url{https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance} (last visited Feb. 28, 2018). The FTC has provided the following checklist for businesses that must abide by COPPA to encourage and help businesses to be more compliant:

\textsuperscript{158} Id.
program aims to fix the various issues regarding compliance. However, there seems to be no verification system in place to make sure that the app developers did in fact comply with the “COPPA-compliance checklists” that they were provided with.\textsuperscript{159}

On the other hand, Apple, another tech industry giant, has also implemented an app review process.\textsuperscript{160} According to Egelman’s study\textsuperscript{161}, however, the system is “opaque,” and similar to Google’s Play Store, there is no sure way to know that these new policies are being consistently enforced.\textsuperscript{162} Upon further testing, in fact, Egelman noted that out of the several iOS games he tested, “all of them had behavioral advertising enabled, a practice prohibited by COPPA, and were not caught by Apple’s review process.”\textsuperscript{163}

These problems 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.\textsuperscript{164} Even the time spent to investigate, however, is a “slow and laborious” practice involving manual testing methods.\textsuperscript{165} Because of this, it is difficult to know whether most mobile apps are meeting the compliance standards set out by the FTC in regards to apps geared towards children.\textsuperscript{166} In turn, this lack of concrete knowledge makes enforcement of the FTC’s privacy laws challenging if not highly improbable.\textsuperscript{167}

Another contributing factor to the lack of enforcement of these privacy law violations is that parents often have no knowledge over whether the apps their children use are gathering data from their children.\textsuperscript{168} This lack of transparency, however, seems to be a preventable issue. Consumers may bridge the gap between parent and

\textsuperscript{159} Id.

\textsuperscript{160} Id.

\textsuperscript{161} Egelman, supra note 53.

\textsuperscript{162} Id.

\textsuperscript{163} Id.

\textsuperscript{164} Id.

\textsuperscript{165} Id.

\textsuperscript{166} Id.

\textsuperscript{167} Id.

\textsuperscript{168} Id.
app by “demanding more transparent disclosures” from those that do the data tracking and transmission, namely the app developers and third-party-advertisers. As a final encouragement to comply, the last step would be for the FTC to delete apps that do not comply.

IV. CONSEQUENCES OF A LARGE DIGITAL FOOTPRINT

There are significant privacy risks that come with sharing personal information online. These disclosures are often connected to certain individuals and third parties who have the ability to access that same information later on. A possible scenario that could arise from sharing personally identifiable information online is that any corporation may buy and sell your personal information, or use the information to profile you or discriminate against you through it.

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 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. Indeed, the research dedicated to learning more about children’s understanding of privacy “in the context of commercial data collection” found that these young children do not fully understand the complicated ways businesses or advertising functions,

---

169 Id.
170 Id.
171 Lipman, supra note 64, at 801
172 Id.
173 Id.
174 See Steinberg, supra note 34.
175 Lipman, supra note 64, at 801.
176 Id.
nor do they understand the extent of their exposure to potential risks in the future.\textsuperscript{177}

The problem lies in the targeted advertising strategies so often used on children who continue to expand their consumption of media and advertisements through digital devices such as a smartphone or a similar device.\textsuperscript{178} Some of the advertising tactics include targeting the consumer, in this case a child, with “personalized content and marketing messages based on individual profiles.”\textsuperscript{179} These marketing trends could be a huge problem if these “digital dossiers” of gathered data follow these young children into adulthood, which would in turn affect their “access to education, employment, health care, and financial services.”\textsuperscript{180}

In the United States, policies regarding children’s privacy and marketing are based mostly on studies conducted in the 1970s.\textsuperscript{181} These studies examined “children’s cognitive developmental vulnerabilities to the persuasive techniques of advertising”; however, because these studies were conducted at a time when television was the most common mode of advertising towards children, these dated policies must be updated to meet the technological and marketing demands of today’s world.\textsuperscript{182} In order for these policies to be updated, further studies must occur about the impact that current advertising techniques have on children today.

\textit{A. Balancing Rights Between the Parent and Child}

One solution to protect children is an obvious one: get the parents involved.\textsuperscript{183} To a large extent, many of the administrative agencies seeking to regulate data privacy and data mining in children’s apps and websites already do this with the plethora of parental consent

\textsuperscript{177} Montgomery, \textit{supra} note 26, at 119.

\textsuperscript{178} Id.

\textsuperscript{179} Id. at 117.

\textsuperscript{180} Id.

\textsuperscript{181} Id. at 119.

\textsuperscript{182} Id. at 117.

\textsuperscript{183} Steinberg, \textit{supra} note 34, at 849.
language that is present in many of the already existing laws in this regard.\textsuperscript{184}

However, we must take a step back and explore the rights all parents have to protect their data privacy. All individuals, including children, have an interest in privacy.\textsuperscript{185} However, parents also have a right to protect their children’s interests. Sometimes, this means that parents may overstep on their children’s privacy rights in order to protect them.\textsuperscript{186} In an increasingly digital world, this duty is more important than it ever has been before.

Parents can further protect their children by getting well acquainted with the privacy policies of the apps or websites that their children use or visit,\textsuperscript{187} or by implementing a notification system that alerts the parents when their child’s name appears in a Google search result.\textsuperscript{188} Finally, parents must be mindful of how their actions might influence their children.\textsuperscript{189} Because children have a tendency to imitate what they see adults do, children who see their parents share personal information online might send a message to the children that that type of online behavior is not only normal, but appropriate.\textsuperscript{190}

\textit{B. The Legal vs. Moral Argument}

Next, the legal argument for protecting children’s privacy is both a constitutional right and a statutory right.\textsuperscript{191} As discussed earlier, the reading of the Fourth Amendment has been expanded to modern times to include data privacy as a protectable search under the Constitution.\textsuperscript{192} In addition, laws such as COPPA have been passed to give the most vulnerable members of our society, children, increased protections for their safety and future privacy interests.\textsuperscript{193}

\textsuperscript{184} Id.
\textsuperscript{185} Id.
\textsuperscript{186} Id.
\textsuperscript{187} Id. at 879.
\textsuperscript{188} Id.
\textsuperscript{189} Id. at 882.
\textsuperscript{190} Id.
\textsuperscript{191} Id.
\textsuperscript{192} See Lipman, supra note 64.
\textsuperscript{193} Id.
On the other hand, the moral argument for privacy is less explicit but in some ways, more obvious.\textsuperscript{194} There is something inherently valuable and precious about privacy that we attribute it as a basic standard for what it means to be human.\textsuperscript{195} Everyone, no matter his or her race, creed, or color, deserves privacy as an unalienable right.\textsuperscript{196} In this sense, the moral argument for privacy is an easy and obvious one to make. \textsuperscript{197} There need not be a constitutional or a man-made law acting as the authority or source for its necessity. \textsuperscript{198}

\textit{C. Potential Harms}

There is much potential for harm in failing to guard children’s privacy. When a user’s online behavior is tracked by a third-party such as a data broker, that information is personally linked with the user and will be saved for an unknown period of time,\textsuperscript{199} which creates potential for delayed reputational harm.

Active Badge illustrated the fact that social, informational, and reputational practices all must be comprehended, discussed, and addressed as new technologies are released. These concerns must become an ingrained part of the testing phase of new technologies so that they can be managed instead of handled through litigation or legislation after a privacy breach occurs.\textsuperscript{200}

Unanticipated reputational harms may arise many years into the future.\textsuperscript{201} These potential harms should, at the very least, be considered and evaluated in the discussion of protecting children’s online privacy.\textsuperscript{202}

Second, most people do not know when their data privacy has been breached until it is too late.\textsuperscript{203} In these cases, the current

\textsuperscript{194} Steinberg, \textit{supra note 34}, at 849.
\textsuperscript{195} Id.
\textsuperscript{196} Id.
\textsuperscript{197} Id.
\textsuperscript{198} Id.
\textsuperscript{199} Lipman, \textit{supra note 64}, at 785.
\textsuperscript{200} Studwell, \textit{supra note 47}, at 241.
\textsuperscript{201} Id.
\textsuperscript{202} Id.
\textsuperscript{203} Id.
regulatory scheme at work does no good for the victims of data privacy breach. This is especially true for children, whose consequences may not even matter until many years into the future. There must be a more comprehensive regulatory scheme or amendments to current laws to protect these future interests for children. Ideally, these laws should flow with the fast-paced time of technology advancements in this modern age.

V. POSSIBLE REMEDIES

In light of the serious consequences and the lack of an effective and comprehensive regulatory scheme to protect children’s need for privacy in this growing world of technology, there have been many ideas of possible solutions for these problems. Among these are to implement new models of notice and choice regimes, integrate interdisciplinary collaborations, mimic what other developed nations have done, and explore the potential for common law protections as well as protections built in to the software itself.

The notice and choice regime is a well-accepted standard in the United States regarding the protection of privacy. The FTC implemented the notice and choice model in 1997 in order to “encourage[e] firms to adopt privacy policies outlining their information practices, obtain[] consent from consumers for uses of information extending beyond the original collection purpose, and embrac[e] fair information practices through self-regulation.” One

\[204\] Id.
\[205\] Id.
\[206\] Id.
\[207\] Id.


such attempt at a notice and choice model was called “P3P, the Platform for Privacy Preferences.”

The P3P standard was based on the idea that having a standardized set of policies in regulating privacy would facilitate an understanding of the policies and unify numerous different websites’ privacy policies into a single standard. This standardization was desired because it would allow a user to simply fix their privacy preferences to his or her liking and the browser would do the work by cross-checking those preferences to the policies of each website the user visits. If the user came across a blocked site, he or she would be notified and then make the choice between avoiding the website or visiting anyway. However, this attempt at a new notice and choice regime faced many issues in application and execution.

The biggest problem came from the fact that companies were not required to create machine-readable P3P policies. Because of this, companies lacked an enforcement mechanism that kept them accountable for following their own P3P policies, which led to an ineffective system. Ultimately, P3P was criticized for being “overly complex” as well as “a false attempt at self-regulation.”

Another attempt at providing increased privacy protections for online users is by looking at the issue from a combination of different perspectives. Examining the complexity of how children respond to this “new, commercial media culture” would be best served by a collaborative effort of researchers from a wide variety of fields, including “psychology, anthropology, communication, marketing, and human-computer interaction.” This collaboration will allow a two-sided research effort: one enabling the study of “developmental issues related to different age groups,” and another enabling the study

---

210 Lipman, supra note 64, at 796.
211 Id.
212 Id. at 797.
213 Id.
214 Id.
215 Id.
216 Id.
217 Id.
218 Montgomery, supra note 26, at 120.
of “the design and functionality of digital media platforms and the strategies used to influence young people.”

How do other developed nations deal with these same issues? Surely, countries such as those in the European Union (EU) must also be facing similar issues with technology and privacy. The EU takes an interesting and effective approach. There, “data is protected regardless of the type of entity holding the data or the exact type of data at issue.” In addition, other administrative agencies have made efforts to tackle the problem as well.

At the most basic level, there are common law protections offered to protect children’s privacy through laws in the areas of contracts, torts, and constitutional law. However, these basic protections are often not enough when sophisticated companies use sneaky methods such as behavioral marketing to target unsuspecting children through smart phone applications.

Another option is to build protection into the technology that children use. Although it seems counterintuitive to use the very thing that is causing privacy concerns to also protect children, built-in protection can be a sensible answer when technology is so complex and multifaceted as is often the case with technologies today.

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

\[^{219}\text{Id.}\]
\[^{220}\text{Lipman, supra note 64, at 788.}\]
\[^{221}\text{Id.}\]
\[^{222}\text{Id.}\]
\[^{223}\text{Studwell, supra note 47, at 232.}\]
\[^{224}\text{Id. at 228.}\]
\[^{225}\text{Id. at 232.}\]
\[^{226}\text{Id.}\]
\[^{227}\text{Id.}\]
\[^{228}\text{Id.}\]
\[^{229}\text{Id. at 245.}\]
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. Those that have already invested substantially into the current infrastructure of the software programming industries will likely fight against this sort of government regulation.

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. Additionally, the data collection methods today are so unclear that there is no effective way to gauge how a public will react to these small, “[n]early costless actions.”

In the same line of thought as these “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. One way to do this is through an application, such as ICSI Haystack, that facilitates the understanding of the mobile ecosystem. “ICSI Haystack is an Android app, available free via Google Play, which helps mobile users understand how their mobile apps handle their private information, including the sensitive data

---

230 Id.
231 Id.
232 Id.
233 Lipman, supra note 64, at 797.
234 Id. at 798.
235 Id. “Actions like turning on the ‘Do Not Track’ signal or occasionally deleting cookies do not tell us how consumers would react to options that both actually stopped tracking and have real costs.” Id. at 802.
237 Id.
their mobile apps leak and with whom they share it.” 238 This app uses Android’s VPN permission to its advantage by studying network traffic on the device itself. 239 Doing this creates a “simplified network stack” to facilitate transmissions between the app and the network. 240 By choosing the device itself as the location of operation, the app has the capacity to “correlate disparate and rich contextual information, such as app identifiers and process IDs . . . .” 241 What Haystack essentially does is analyze the app traffic by searching for identifying information which it obtains from the smartphone subject to Android’s permissions. 242

Third-party service providers usually use the app permission method to collect information from users. 243 According to one study, popular games were connected to a high number of “advertising and tracking services (ATS).” 245 The study found that “[o]n average, 17% of app traffic is associated with ATS services.” 246

Yet another option is to introduce a whole new model for enforcing uniform privacy policy through something akin to “nutrition labels.” 247 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. 248 Each box in the grid would

238 Id. at 2.
239 Id.
240 Id.
241 Id.
242 Id.
243 Id. at 1.
244 Id. The study used data gathered by an app called the ICSI Haystack tool to identify the entity that tracks user activity. Using this classifier system, the study identified “58 domains that remained unreported by well-known tracking and advertising domain lists like AdBlock’s Easylist and hpHost’s ATS list.” The purpose of the study was to “promote mobile transparency and develop techniques to protect mobile user’s privacy . . . .” Id. at 5.
245 Id. at 1, 3.
246 Id. at 5.
247 Lipman, supra note 64, at 803.
248 Id. Specific examples of items found on the “information we collect” axis are “demographic information” and “health information.” Id. Some examples of items found on the “ways we use your information” axis include “provide service and maintain site” and “profiling.” Id.
denote a certain type of data and what use that data is put to.\textsuperscript{249} Colors can be used to mark whether or not a company collects and uses your data for a specific purpose.\textsuperscript{250} This privacy grid would be a viable method to form a uniform privacy policy, because of its simplicity and practicality.\textsuperscript{251} 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.\textsuperscript{252}

Ideally, users would not have to reference the privacy grid to begin with.\textsuperscript{253} Just by virtue of having a machine-readable policy which was previously unfeasible with the P3P program, the browser system should do the work for the user once the user inputs his or her preferences into the grid.\textsuperscript{254} The same loopholes that worked with P3P would not work under this theoretical system because the grid would act as the uniform privacy policy that every website would need to fill out.\textsuperscript{255}

One unresolved issue, however, is whether the browser should entirely block the website or offer a pop-up option that would allow users a choice on whether or not to visit the website despite it not complying with the set privacy preferences.\textsuperscript{256} Although the new “nutrition labels” solution may not be picture perfect, the ease with which this model would allow lay persons to understand complex privacy policies as well as the way it would effectively standardize a common privacy policy shows hope and promise.

VI. CONCLUSION

We are living in a technological golden age. With these new innovations, however, are significant privacy concerns that must be
addressed. As smartphones become more commonly used and widespread in the developed world, adults, parents, and educators must do their best to guard children from the manipulative and deceptive data-mining tactics of the tech world. In doing so, we must bridge the “intuition gap” between allowing certain apps to access user data and actually knowing and understanding the consequences of this seemingly innocent act of permitting access to personal information via the touch of a button.

The broader legal and practical impact of coming up with a new enforcement mechanism to keep app developers in check with privacy policies will have huge implications for the future of our children, and for privacy policies in general. As the number of devices that make up the “Internet of Things” continues to grow and latch onto daily aspects of people’s lives, it is imperative that there be a system in place to implement an effective, smooth-flowing enforcement mechanism.

Among the several possible solutions to the privacy issues discussed, the notice and choice regime model using the “nutrition label” seems to be most promising. Improving from the P3P program, the new “nutrition label” model does away with everyday smartphone users from figuring out the complicated language of the privacy policies written for each software or website. Whatever new regime or model is put in place, however, the most significant thing to remind ourselves of is that privacy in this digital world is a right that all technology-users should be entitled to, and one that carries with it great responsibility.


257 Montgomery, supra note 26, at 119.
258 Lipman, supra note 64, at 785.
259 Montgomery, supra note 26, at 119. The “Internet of Things” refers to “Internet-connected sensors that change ordinary objects such as cars, refrigerators, and toys into ‘smart’ devices.” Id.
260 Lipman, supra note 64, at 803.
261 Id.