Journal of Business & Technology Law

Volume 15 | Issue 1 Article 3

After Over-Privileged Permissions: Using Technology and Design to Create Legal Compliance

Anjanette Raymond

Jonathan Schubauer

Dhruv Madappa

After Over-Privileged Permissions: Using Technology and Design to Create Legal Compliance

ANJANETTE RAYMOND, JONATHAN SCHUBAUER, AND DHRUV MADAPPA*©

ABSTRACT

Consumers in the mobile ecosystem can putatively protect their privacy with the use of application permissions. However, this requires the mobile device owners to understand permissions and their privacy implications. Yet, few consumers appreciate the nature of permissions within the mobile ecosystem, often failing to appreciate the privacy permissions that are altered when updating an app. Even more concerning is the lack of understanding of the wide use of third-party libraries, most which are installed with automatic permissions, that is permissions that must be granted to allow the application to function appropriately. Unsurprisingly, many of these third-party permissions violate consumers' privacy expectations and thereby, become "over-privileged" to the user. Consequently, an obscurity of privacy expectations between what is practiced by the private sector and what is deemed appropriate by the public sector is exhibited.

Despite the growing attention given to privacy in the mobile ecosystem, legal literature has largely ignored the implications of mobile permissions. This article seeks to address this omission by analyzing the impacts of mobile permissions and the privacy harms experienced by consumers of mobile applications. The authors call for the review of industry self-regulation and the overreliance upon simple notice and consent. Instead, the authors set out a plan for greater attention to be paid to socio-technical solutions, focusing on better privacy protections and technology embedded within the automatic permission-based application ecosystem.

INTRODUCTION

Most lawyers recall with a level of fondness the series of shrink-wrap cases, founded in somewhat extensional twists of the law at the time. The law landed on the determination that a customer can buy software and agree to the primary terms of use prior to its installation, and as purchasers retain the option to return software once they see the terms inside the box. The cases slowly came to a somewhat reasonable line of legal business efficiency.

Fast forward to today's world, software–at least on a disk in a box–is a thing of the past, and the ability to download a piece of software is ubiquitous. One might

assume, those tried and true cases of old still lead the reasoning, but you would likely be surprised. While downloading applications are still subject to terms of use, buried inside the download, and rarely mentioned in the fine print, are the series of third-party libraries installed with automatic permissions–that is permissions that must be granted to allow the application to function appropriately.

In addition to such libraries, applications use these third-party permissions in ways that may violate consumers' privacy expectations and thereby, become over-privileged to the user. For example, Silverpush, an advertising company, developed a mobile ad library repository that passively listened for ultrasonic audio beacons to track users TV viewing activities.[1] Similarly, Facebook was recently awarded a patent for utilizing a mobile device's camera to analyze users' emotions while they are browsing their newsfeeds.[2] In such instances, these third-party libraries are granted over-privileged permissions to collect advertising information, without any notification to inform the consumer. Of course, these are just a couple of the more nefarious examples, consider an application that provides up-to-date weather, or traffic, or locations of friends.[3] These applications are often drawing information from other databases–and are aggregating the data in a real time provision. Each of these external databases–or other providers of data–often want access to the data, both stored and generated.

While most individuals may be comfortable with sharing such data, individuals are unaware of the privacy risks they consensually agreed upon. Consumers are blindly conforming to the blanketed disclosures, while coupled with their lack of understanding of the inner workings of how their technology may be used in their daily routines. Thus, we have since returned our society to the days of the uncertainty of the law in the face of shrink-wrap clauses.

---

* Anjanette Raymond is the Director of the Program on Data Management and Information Governance, Ostrom Workshop; Associate Professor, Department of Business Law and Ethics, Indiana University, Kelley School of Business. Jonathan Schubauer *is an* Affiliate Scholar at the Data Management and Information Governance, Ostrom Workshop; Research Fellow, Center for Security and Privacy, Department of Informatics, Indiana University, School of Informatics, Computing, & Engineering. Dhruv Madappa is a Master's Student studying Cybersecurity Risk Management, Department of Informatics, Computing & Engineering at Indiana University, Kelley School of Business.

1. *See* Dan Goodin, *More Android Phones than ever are Covertly Llistening for Inaudible Sounds in ads*, ARS TECHNICA (May 5, 2017, 11:14 AM), https://arstechnica.com/information-technology/2017/05/theres-a-spike-in-android-apps-that-covertly-listen-for-inaudible-sounds-in-ads/.

2. *See* Minda Zetlin, *Facebook Is Patenting Technology to Spy on You Through Your Smartphone Camera and Microphone*, INC. (June 25, 2018), https://www.inc.com/minda-zetlin/facebook-patents-spying-smartphone-camera-microphone-privacy.html.

3. *See* W. Enck et al., *A Study of Android Application Security*, *in* PROC. OF THE 20TH USENIX SECURITY SYMPOSIUM (2011); s*ee also* Glen Urban & Fareena Sultan, *The Case for 'Benevolent' Mobile Apps*, 56 MIT SLOAN MGMT. REV. 31, 31–37 (2015) (describing how the "free Sea Tow app supports boaters' navigation needs by offering information about local tide tables, detailed marine weather forecasts, GPS coordinates and bearing, and speed.").

Consequently, it's time to revisit the approach that was developed in response to shrink-wrap issues, one that recognizes the importance of balancing law and business interests. This article will explore a governance regime for the consumer driven digital world. The paper asserts that regulation must be designed with key features in mind: legal compliance, technology as a driver, the seamless, unobtrusiveness, and transparent, processes, focused on creating balances between business interests and the need to regulate. The paper will accomplish this by demonstrating consent by design deployed in the automatic permission-based application ecosystem.

In 1994, the first smartphone was launched by IBM's Simon Model.[4] It had over 10 inbuilt applications and there was no iOS or Google app stores for consumers to download additional applications. The phone came preloaded with generic productivity apps like the Address Book, Calendar, Mail, Note Pad and Sketch Pad. Although not known as "applications," but instead "features" these developments were the first signs of what was to come in the mobile application environment.[5]

Fast-forward to 2008, the Apple AppStore went live, featuring over 500 iOS applications. There were over ten million apps downloaded within the first week highlighting the massive market potential of mobile apps, with numerous amounts of these applications offered as what many consumers considered as "free."[6] One month later, Google would announce the Android Market and would make it available for Android users within a few months of the Apple AppStore release.[7] Android Market would later become known as Google Play, which then merged all Android application markets into one store to support the mass market of users.[8]

With the AppStore and Google Play Store now serving millions of people internationally, individual app downloads reached hundreds of millions in the first month. Applications were soon categorized by their intended purpose (game, lifestyle, productivity, etc.), which was distinguished by both the description and

4. *See* Ira Sager, *Before iPhone and Android Came Simon, the First Smartphone*, BLOOMBERG (June 29, 2012, 8:50 AM), https://www.bloomberg.com/news/articles/2012-06-29/before-iphone-and-android-came-simon-the-first-smartphone.

5. *See id.*

6. *See* Caroline McCarthy, *Apple: One million iPhones sold, 10 million App Store downloads in first weekend*, CNET (July 15, 2008, 7:13 AM), https://www.cnet.com/news/apple-one-million-iphones-sold-10-million-app-store-downloads-in-first-weekend/.

7. *See* Dean Takahashi, *Google Releases Details on Android Market Launch*, VENTUREBEAT (Oct. 22, 2008, 9:25 AM), https://venturebeat.com/2008/10/22/google-releases-details-on-android-market-launch/;*see also, e.g.*, Chris Velazco, *Goodbye Android Market, Hello Google Play*, TECHCRUNCH (Mar. 6, 2012, 1:00 PM), https://techcrunch.com/2012/03/06/goodbye-android-market-hello-google-play/.

8. *See* Ron Amadeo, *Google launches the Google Store, a new Place to buy Hardware*, ARS TECHNICA (Mar. 11, 2015, 2:09 PM), https://arstechnica.com/gadgets/2015/03/google-launches-the-google-store-a-new-second-place-to-buy-hardware/.

the core functions of what the app intended to use from the smartphone device.[9] The core functionality of applications introduced a need for consumers to be notified what they were agreeing to when downloading and using a mobile app. These notification and consent needs formed what would become the mobile application permission model.[10]

The article is structured as follows. Part I offers a description of what the permission system represents for both the Android and iOS operating systems. Part II then focus on the application technology of permission systems with an emphasis on over-privileged permissions. Subsequently, an analysis of the legislative flaws and failings of regulating third-party services in modern technology is then offered in Part III. Part IV reveals third-party permission practices and violations of privacy in mobile applications. Part V overviews the current U.S. privacy legislation and industry regulations in place. Finally, Part VI concludes the article with a discussion of potential guidelines mobile developers could adopt, and the need for a sociotechnical & legal reconstructive approach to help provide consumers with the protections to promote consumer privacy.

I. HOW PERMISSION SYSTEMS ARE MODELED: A DESIGN PRIMER

While basic permission models have been around in some form since computers were distributed,[11] the mobile permission system has been flawed by design since its conception.[12] A case in point is the automatic process by which some permissions of mobile applications are allowed. In most cases, there are too many permissions included in an application that do not align with its intended purpose. Even more alarming, the consumers have very little choice in what the application can access on their smartphone. The transparency that is provided within notice and disclosure forms is also presented at an excessive length that is written broadly in legal language that the consumer may not understand. Simply put, the consumer has limited choice and control with their information in the mobile application ecosystem. A more thoughtful representation of transparency is needed if we want to provide consumers with adequate means of protecting and controlling their

9. *See, e.g.*, *Play Console Help*, GOOGLE, https://support.google.com/googleplay/android-developer/answer/113475?hl=en (last visited Oct. 8, 2019) (describing the different categories and descriptions for applications in the Google Play Store).

10. *See Permissions Overview*, ANDROID, https://developer.android.com/guide/topics/permissions/overview (last visited Oct. 8, 2019) ("Android apps must request permission to access sensitive user data (such as contacts and SMS), as well as certain system features (such as camera and internet). Depending on the feature, the system might grant the permission automatically or might prompt the user to approve the request.").

11. *See* David F. Ferraiolo & D. Richard Kuhn*, Role-Based Access Control, in* 15TH NAT'L COMPUTER SECURITY CONF., Oct. 1992, at 554–63 ("The current set of security criteria, criteria interpretations, and guidelines has grown out of research and development efforts on the part of the DoD over a period of twenty plus years.").

12. *See* Franziska Roesner et al., *User-Driven Access Control: Rethinking Permission Granting in Modern Operating Systems*, *in* PROC. OF THE 2012 IEEE SYMP. ON SECURITY & PRIVACY, May 2012, at 224.

personal information. First, though, it is important to understand the way in which the permission model works and to distinguish the differences of the Android and iOS permission systems.

A. Understanding Permission Norms

To uncover the foundations of what makes a permission system, consider the general formality of asking permission for something. When we do this task, what we are really doing is providing the recipient of our conversation a degree of notice to what we are requesting and then waiting for our request to receive consensual agreement.[13] If the recipient party consensually provides permission to a request, the party who initially asked permission to do a task is permitted to conduct whatever was requested.[14] Similarly, if the party who is asked permission by a requester does not agree with what is being asked, the recipient of the request may choose to deny permission from completing a task.[15]

The mobile permission system generally tries to mimic this formal process, but with a degree of difficulty. The formal permission process of human-to-human interaction often entails a single request, followed by a mutual agreement or disagreement.[16] Conversely, the mobile permission process includes several permissions in a single request.[17] For example, if the recipient downloading an application is asked by an application permission to use a feature, the recipient is typically agreeing to more than one permission in a single request.

This can be problematic since the recipient is not informed of the additional permissions they are agreeing to. In the same example, if the recipient of the permission request does not agree to grant permission to the application, the mobile app may refuse to download and thereby, render the services impossible to be used. Hence, consumers downloading applications are met with a "take it or leave" ultimatum. Enter the mobile permission system and how applications address the formal permission process.

B. How the Mobile Permission System Works

Permission systems for mobile platforms are described as "user-centric,"[18] where the consumer using the app makes the first decision about granting permission to

13. *See generally The Basics of Getting Permission*, STAN. U. LIBR., https://fairuse.stanford.edu/overview/introduction/getting-permission/ (last visited Sept. 24, 2019) (outlining the basic steps for obtaining permission).

14. *Id.*

15. *See id.*

16. *See id.*

17. *See generally* Adrienne Porter Felt et al., *How to Ask for Permission*, *in* PROC. OF THE 7TH USENIX CONF. ON HOT TOPICS IN SECURITY, 2012, at 4 (discussing various platforms' permission systems).

18. *See* Mohammad Nauman et al., *Realization of a User-Centric, Privacy Preserving Permission Framework for Android*, 8 SECURITY COMM. NETWORKS 368, 369 (2014).

an application at the installation stage.[19] The core functionality of the permission system is to allow consumers to regulate access to sensitive data on mobile devices,[20] such as address book contacts, location information, and text messages. These permissions granted by the consumer are then applied to all subsequent cases of the same app accessing the device.[21]

The permission systems of Android and iOS applications were intended to provide consumers with general notice to what features an application may use when it is functioning.[22] For instance, applications cannot simply access and turn on a consumer's camera. Instead, the application must first be granted permission by the consumer during the installation process,[23] so the person using the app can distinguish if the ability to access the camera is reasonable within the applications purpose. Whether the camera should be appropriately used is determined within the reasoning of the applications functionality. Snapchat, for example, would reasonably need permission to use the camera feature.[24]

In a privacy tech utopia, consumers would be given unlimited choice and control over their data. However, the platform on the mobile device must make implicit assumptions for the consumer so that the core elements of the applications may run properly.[25] For instance, if a consumer had to accept or decline every function on an application, the process may exhaust the consumer's patience and render the importance of the permissions messages useless. The permission description may not be read and the habituation of a quick acceptance out of convenience is more likely.[26]

---

19. *See* Adrienne Porter Felt et al., *Android Permissions Demystified*, *in* PROC. OF THE 18TH ACM CONF. ON COMPUTER & COMM. SECURITY, Oct. 2011, at 627 (declaring up front the required permissions, apps allow notify users about the received permissions).

20. *See* Adrienne Porter Felt et al., *Android Permissions: User Attention, Comprehension, and Behavior*, *in* PROC. OF THE EIGHTH SYMP. ON USABLE PRIVACY & SECURITY, July 2012 ("In order to protect Android users, applications' access to phone resources is restricted with *permissions*.").

21. *See id.*

22. *See id.*

23. *See id.*

24. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE, CHAPTER 8 BREAKING RULES FOR GOOD (2009) (discussing information sharing is the primary threat to privacy in today's technological society); *see generally Android Permissions*, SNAPCHAT (last visited Oct. 14, 2019), https://support.snapchat.com/en-US/a/android-permissions (explaining that Snapchat must be given permission from user to access camera).

25. *See generally* Rebecca Balebako, et al., *The Impact of Timing on the Salience of Smartphone App Privacy Notices*, *in* PROC. OF THE 5TH ANN. ACM CCS WORKSHOP ON SECURITY & PRIVACY IN SMARTPHONES & MOBILE DEVICES, Oct. 2015, at 63, at 63–74 (2015) (discussing the effects of privacy notices on participants in a study).

26. *See generally* Soyun Kim & Michael S. Wogalter, *Habituation, Dishabituation, and Recovery Effects in Visual Warnings*, *in* 53 PROC. OF THE HUMAN FACTORS & ERGONOMICS SOCIETY ANN. MEETING 1612, 1612–16 (2009) (finding that participants in a study became less alert to the presence of privacy warnings the more exposed they were to such warnings).

On the other hand, the consumer may not be sufficiently knowledgeable to understand which permission must be used in order to allow the application to function correctly.[27] To avoid these issues, the permission system provisions to automatic approval of different types of permissions at both the installation and runtime.[28] While both Android and iOS use mobile permission models similarly, each has a distinctively different permission system.[29] It is worth highlighting the core differences in the two major mobile ecosystems. Firstly, the use of intents–a mechanism in Android which allows applications to internally exchange information–facilitates a large part of app development in the android permission environment.[30] This mechanism does not exist in iOS, since URL Schemes dictate iOS inter-app communication. To put it simply, these two mobile operating systems communicate to their applications differently. Secondly, the developer environments are inherently distinctive. Android development is encapsulated in an open-source environment, while iOS is produced in a closed source system. Moreover, these distinctions create special security issues that could result in privacy risks.

Since the development process is very different, tackling the privacy issues ensued by their similar permission models becomes complicated. Within the Android system, permissions are requested by the application developer, incorporated into the application package,[31] and then approved by the user when the application has been installed.[32] While this may seem simple, it is not. In fact, the Android Application Platform Interface ("API") currently contains more than 130 varying permissions the developers can implement.[33]

---

27. *See* Haoyu Wang, et al., 2017. *Understanding the Purpose of Permission Use in Mobile Apps.* 35 ACM TRANSACTIONS ON INFO. SYSTEMS, July 2017, at 2–6, 31 ("Understanding the purpose of why sensitive data [on our phones] is accessed could help improve privacy as well as enable new kinds of access control.").

28. *See id.* at 4 (explaining certain permissions must be accepted at install time).

29. *See* Zinaida Benenson, et al., *Android and iOS Users' Differences Concerning Security and Privacy, in* CHI'13 EXTENDED ABSTRACTS ON HUMAN FACTORS IN COMPUTING SYSTEMS 817, 819 ("compar[ing] Android and iOS users according to their demographic differences, security and privacy awareness, and reported behavior when installing apps.").

30. *See generally Intents and Intent Filters*, ANDROID, https://developer.android.com/guide/components/intents-filters (last visited Sept. 18, 2019) (providing information on the various types of intents and intent filters).

31. *See generally Android API's*, GOOGLE, https://developers.google.com/fit/android/ (last visited Sept. 18, 2019) (explaining the Recording API provides automated storage of fitness data using subscriptions).

32. *See generally Requesting App Permissions*, ANDROID, https://developer.android.com/guide/topics/permissions/requesting.html (last visited Sept. 18, 2019) (detailing the Android permission model).

33. *See generally Permissions overview*, ANDROID, https://developer.android.com/guide/topics/permissions/overview (last visited Oct. 14, 2019) (explaining how Android application permissions work, "including: how permissions are presented to the user, the difference between install-time and runtime permission requests, how permissions are enforced, and the types of permissions and their groups."). *See also* Michelle Atkinson, *Apps Permissions in the Google Play Store*, PEW RES. CTR. (last visited Sept. 18, 2019), https://www.pewinternet.org/2015/11/10/apps-permissions-in-the-google-

Similar to Android, iOS permissions accessing sensitive data are listed by the app developer in the app bundle. Apps that are linked to recent releases in iOS software (iOS 10 and later), are now required to include the types of data in a plug-in to store configuration metadata in order to run.[34] Users are notified of the data that is used by the app prior to its installation and are then prompted to grant or deny access to that data once the app is installed. Until the user grants access, any API calls to that data are blocked. However, the user is only notified the first time the app requests access with all subsequent API calls using existing permissions to access the data.[35]

One drastic difference between iOS and Android is the classification of permissions. Android classifies the most important type of permissions as Normal and Dangerous.[36] Normal Permissions cover areas that protect access to API calls that can notify users.[37] However, Normal Permissions are not granted access to anything that could potentially harm the consumer.[38] In contrast, Dangerous Permissions cover areas that control access to potentially harmful API calls.[39] In general, these types of permissions are considered potentially harmful because certain routine permissions granted could access private information on a user's device.[40] Therefore, the user's approval is required to be requested before the permission is granted[41] and the permission can be revoked by the user at any time.[42]

---

play-store/ ("Analysis of over 1 million apps in Google's Android operating system in 2014 shows apps can seek 235 different kinds of permissions from smartphone users. The average app asks for five permissions.").

34. *See generally Documentation: Contacts*, APPLE, https://developer.apple.com/documentation/contacts (last visited Sept. 18, 2019) (detailing the Contacts framework for all Apple platforms).

35. *See generally Device Compatibility*, APPLE, https://developer.apple.com/library/archive/documentation/DeviceInformation/Reference/iOSDeviceCompatibility/DeviceCompatibilityMatrix/DeviceCompatibilityMatrix.html (last visited Oct. 14, 2019) (providing information on device capability requirements).

36. *See* Developers Guide, *Requesting App Permissions*, *supra* note 32.

37. *See* Android, *Permissions overview*, *supra* note 33.

38. *See generally* William Enck et al., *A study of Android application security*, *in* PROC. OF THE 20TH USENIX CONF. ON SECURITY, Aug. 2011, at 21, (finding insufficient protection of privacy sensitive information and widespread misuse).

39. *See* Jon Howell & Stuart Schechter, *What you see is what they get: Protecting Users from Unwanted Use of Microphones, Cameras, and Other Sensors*, *in* WEB 2.0 SECURITY & PRIVACY, May 2010, at 5 (explaining once an application is granted access, it can abuse that access and gain access to personal information in a user's phone).

40. *See* Adrienne Porter Felt et al., *Permission Re-Delegation: Attacks and Defenses*, *in* PROC. OF THE 20TH USENIX CONF. ON SECURITY, Aug. 2011, at 22 (explaining permission de-regulation occurs when an application performs a privileged task for an application without permissions).

41. *See* Adrienne Porter Felt et al., *The Effectiveness of Application Permissions, in* PROC. OF THE 2ND USENIX CONF. ON WEB APPLICATION DEV., June 2011, at 7 ("Application permissions offer several advantages over traditional user-based permissions, but these benefits rely on the assumption that applications generally require less than full privileges.").

42. *See id.*

In contrast, iOS Apps are expected to encrypt all data in an iOS device. As such, accessibility to data is based upon the classification of data into four categories: Complete Protection; Protected Unless Open; and No Protection.[43]

Files that are assigned to a Complete Protection class offer the most security to their data, requiring the user's passcode and unique device identification to decrypt the data. Moreover, the data in this class are inaccessible once the user locks the device, making all data protected until the user unlocks the device again. The Protected Unless Open class–a slightly less protected class–is used for files that continue to run even while the device is locked. This function is used by apps that run in the background to perform certain operations, such as maintenance and data analytics. The No Protection Class offers the least security to the data assigned to it since any key required to decrypt a file in this class is stored in device memory.[44]

While these automatic permission are sometimes necessary,[45] these permission are also interconnected with third-party services embedded in the application.[46] These third-party services contain Software Development Kits that developers include in their application.[47] The majority of the time, these additional software packages are necessary to maintain and operate the application.[48] However, in other instances, third-party services are collecting advertising and behavioral analytics.[49] The consumer is not notified of whom or what these third-parties will be collecting, since the permission is granted automatically at the installation

43. *See iOS Security: iOS 12.3*, APPLE 19–20 https://www.apple.com/business/site/docs/iOS_Security_Guide.pdf (last visited Sept. 18, 2019) ("When a new file is created on an iOS device, it's assigned a class by the app that creates it. Each class uses different policies to determine when the data is accessible.").

44. *See id.*

45. *See generally* Patrick Gage Kelley et al., *A Conundrum of Permissions: Installing Applications on an Android Smartphone*, *in* PROC. OF THE 16TH INT'L CONF. ON FIN. CRYPTOGRAPHY & DATA SECURITY, 2012, at 68 (finding that users are generally not well informed to decide privacy and security questions when installing applications).

46. *See*, Android Developer Website, *sdkmanager*, ANDROID, https://developer.android.com/studio/command-line/sdkmanager (last visited Sept. 18, 2019) (explaining how to use the skdmanager command tool). *See also* Ilias Leontiadis et al., *Don't kill my ads!: Balancing Privacy in an ad-supported Mobile Application Market*, *in* PROC. OF THE TWELFTH WORKSHOP ON MOBILE COMPUTING SYSTEMS & APPLICATIONS, Feb. 2012 ("Allowing third-party applications to operate within a device holding private information about their owner can lead to unanticipated privacy and security risks . . .").

47. *See generally* Google, *Release notes*, GOOGLE ADMOB, https://developers.google.com/admob/ios/rel-notes (last visited Sep. 18, 2019) (detailing updates for Google AdMob since its General Availability release).

48. Ryan Stevens et al., *Investigating user Privacy in Android ad Libraries*, UNIV. OF CAL., DAVIS 1, 2 https://pdfs.semanticscholar.org/fa2c/7383769184aae4e301f0361758ae2ddb1daf.pdf (last visited Oct. 15, 2019) (2012).

49. *See generally* Michael Grace et al., *Unsafe Exposure Analysis of Mobile in-app Advertisements*, PROC. OF THE FIFTH ACM CONF. ON SECURITY & PRIVACY IN WIRELESS & MOBILE NETWORKS, Apr. 2012, at 101 (providing a study on the Android platform discovered that most existing ad libraries collect private information from phones that cannot be justified).

process.[50] For example, Android applications exchange information from app to app through a process called "inter-Process Communication ("IPC"),"[51] which in practical terms means that multiple applications can collect data and share resources, so long as they operating under the same service agreement on the same device.[52] As this process became more widespread, application designers introduced a more seamless process called a "signature permission," which enables automatic access to the same resources for applications which are signed with the same certificate.[53] In practical terms, this means signature permissions are installed without notification to the user.[54] Of course, this notice work around was done out of necessity, as these elevated privileges are primarily for maintenance and updates.[55]

In contrast, iOS applications also cross-communicate with other applications in the background. Apple applications use URL schemes to communicate from application to application through custom protocols developers define.[56] Similar to the signature permission in Android, the iOS developer creates a custom URL scheme which may access other app systems. Once the URL scheme from another application accepts the handler that is passed through, the app system protocol permission is granted to access and communicate with libraries of another iOS

50. *See* Solon Barocas & Helen Nissenbaum, *On Notice: The Trouble with Notice and Consent*, *in* PROC. OF THE ENGAGING DATA F.: THE FIRST INT'L F. ON THE APPLICATION & MGMT. OF PERS. ELECTRONIC INFO, Oct. 2009 (explaining it is practically impossible to opt-out of tracking under the current mechanism put in place by some certain ad networks).

51. Erika Chin et al., *Analyzing Inter-Application Communication in Android, in* PROC OF THE 9TH ACM CONF. ON MOBILE SYSTEMS, APPLICATIONS AND SERVICES, June-July 2011.

52. *See id. See also* Theodore Book & Dan S. Wallach, *A Case of Collusion: A Study of the Interface Between Ad Libraries and Their Apps*, PROC. OF THE THIRD ACM WORKSHOP ON SECURITY AND PRIVACY IN SMARTPHONES & MOBILE DEVICES, Nov. 2013, at 79.

53. *See generally Define A Custom App Permission*, ANDROID, https://developer.android.com/guide/topics/permissions/defining (last visited Sept. 12, 2019) (explaining how app developers can define their own permissions, which allows the app's resources and capabilities to be shared with other apps); *see also <permission>*, ANDROID, https://developer.android.com/guide/topics/manifest/permission-element (last visited Sept. 13, 2019) (describing the component of a security permission and how a security permission may be used for more than one application).

54. *See, e.g.*, Yuan Zhang et al., *Vetting Undesirable Behaviors in Android Apps with Permission Use Analysis*, 9 IEEE TRANSACTIONS ON INFO. FORENSICS AND SECURITY 1828, 1828 (2014) (explaining that after app in Android grants a set of permissions upon explicit request during installment, there is no way to inspect how those permissions are used by the app to utilize sensitive resources).

55. *See id.* (explaining that the Android framework manages most system resources).

56. *See Allowing Apps and Websites to Link to Your Content*, APPLE, https://developer.apple.com/docudocumenta/uikit/inter-process_communication/allowing_apps_and_websites_to_link_to_yoyo_content (last visited Sept. 13, 2019) (explaining how universal links allow one app to send small amounts of data direct to another app, absent a third-party server).

application.[57] Furthermore, the consumer is not presented with any degree of notice while the data is being collected among multiple applications.

II. OVER-PRIVILEGED PERMISSIONS

As previously mentioned, the iOS and Android permissions are intended to provide consumers with the ability to control their privacy and reduce potential vulnerabilities in applications. However, a permission system is ineffective at providing proper privacy protections if developers routinely request more permissions than an application requires.[58] It was quickly observed that the majority of applications on app stores requested a number of permissions that exceeded the scope of purpose intended to provide basic app functionality.[59] Developers embedded additional permissions used for collecting information–like geolocation data and address book contacts–for tracking and behavioral marketing purposes. In such instances, these permissions were over-privileged to the applications intended function and exceeded the consumer's privacy expectations.

Defining an over-privileged permission would depend on the context of the application itself and the scope of which the permission fails to align with its intended functionality of the mobile app.[60] For example, a flashlight app may reasonably require access to the consumer's camera on their mobile device to operate the necessary light component.[61] If that flashlight app conjointly installs the read and write contact permissions, that application would potentially be violating consumer's privacy expectations. The intentional purpose of the application is to provide a source of light, not collect contact information. Moreover, the consumer may be unaware that the permissions granted are accessing such data. A reasonable implementation of an application like a flashlight app would only need a single permission with two API calls—one to turn on and another to turn off the camera flash.[62]

In the modern application market both the Google and Apple app stores are populated with an excess of "free" applications that routinely install over-privileged

57. *See id.*

58. *See* Alessandra Gorla et al., *Checking App Behavior Against App Descriptions*, *in* PROC. OF THE 36TH INT'L CONF. ON SOFTWARE ENGINEERING, May 2014, at 1025–26 (exemplifying how certain apps' governing permission allows for additional access outside the scope of the permission).

59. *See id.*

60. *See* Primal Wijesekera et al*., The Feasibility of Dynamically Granted Permissions: Aligning Mobile Privacy with User Preferences*, *in* PROC. OF THE 2017 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (2017) (explaining some ask-on-the-first-use permissions fail to account and provide notification for uses of the permission that are different from the initial granted use).

61. *See id.*

62. *See id.* ("[P]rivacy violations occur when sensitive resources are used in ways that defy users' expectations."); *see also* Efthimios Alepis & Constantinos Patsakis, *Hey Doc, Is This Normal?: Exploring Android Permissions in the Post Marshmallow Era, in* INT'L CONF. ON SECURITY, PRIVACY, AND APPLIED CRYPTOGORAPHY ENGINEERING (2017).

permissions.[63] Asking the consumer to provide permission was initially well-intentioned by the market controllers. However, both Android's and Apple's permission systems were crafted with imminent design failures from the very beginning.[64] The original Android permission system required the approval of every permission at the beginning of the installation stage. The consumer was presented with a list of permissions the app would require and was only left with the option of clicking "next" to continue the installation process.[65] Denying any of the requested permissions was not provisioned by the developers as an option for the consumer. If the consumer were to "cancel" the permission list,[66] the application would stop the downloading process,[67] rendering the application unusable without the full approval of every listed permission.

Conversely, Apple's first release of its iOS 1 mobile operating system occurred prior to the release of their official App Store.[68] Any prior third-party applications downloaded by users were not authorized by Apple.[69] As a result, Safari, Mail, and Bluetooth were incredibly vulnerable.[70] Attackers easily enticed users to malicious web pages that allowed cross-site scripting and dialing phone numbers without user confirmation.[71] Apple's permission model would resemble similar components to the Android model,[72] however, an earlier adoption to *ask-on-install* (*"*AOI")[73] would be implemented for users. The release of iOS 2 opened location services to third-party applications, but prompted consumer permission first.[74] While the consumer was granted the option of approving certain permissions, there was limited control

63. *See id.* (explaining how some apps request for permission the first time accessing certain data and enforce users' approval for subsequent permissions).

64. *See* Jialiu Lin et al., *Modeling Users' Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings*, *in* TENTH SYMP. ON USABLE PRIVACY AND SECURITY, July 2014, at 199 ("early studies in this area have shown that privacy interfaces, whether for iOS or for Android, did not provide users with adequate information or control.").

65. Xuetao Wei et al., *Permission Evolution in the Android Ecosystem*, *in* PROC. OF THE 28TH ANN. COMPUTER SECURITY APPLICATIONS CONF., Dec. 2012, at 31, 33

66. *See generally* Paolo Calciati et al., *How Do Apps Evolve in Their Permission Requests? A Preliminary Study*, *in* PROC. OF THE INT'L CONF. ON MINING SOFTWARE REPOSITORIES, May 2017, at 37 (finding that apps have required more permissions overtime).

67. *See id.*

68. Joshua Long, *The Evolution of iOS Security and Privacy Features*, INTEGO (Feb. 29, 2016), https://www.intego.com/mac-security-blog/the-evolution-of-ios-security-and-privacy-features/.

69. *Id.*

70. Jim Dalrymple, *Apple Released iPhone Update 1.1.1.*, MACWORLD (Sept. 26, 2007, 11:00 AM), https://www.macworld.com/article/1060250/iphoneupdate.html.

71. *Id.*

72. Ashni Sharma, *Android v. iOS: Which One Fares Well in App Permission System*, OPEN SOURCE FOR YOU (July 19, 2016), https://opensourceforu.com/2016/00/android-vs-ios-one-fares-well-app-permission-system/.

73. Wijesekera et al., *supra* note 60.

74. Lang, *supra* note 67.

over Location Services.[75] If Location Services were granted permission, all other apps theoretically could access the same information.[76] In response to permission protection failures, Google and Apple developed newer developer guidelines with each release of their newer operating systems,[77] which required developers to produce apps with a different permission model.[78]

A. Android Developer Guidelines Evolution

To address the shortcomings of the previous install-time permissions approach, Android 6.0 Marshmallow was released as the 13th version of a newer mobile operating system.[79] The release of Marshmallow was significant, since the operating system would require developers to reveal dangerous permissions to the consumer using an AOI[80] model.[81] The consumer would be provided the choice of granting approvals of dangerous permissions upon the first installation stage, instead of the application automatically receiving approval of every listed permission without consent at install-time.[82]

For the dangerous permissions, the new operating system would now prompt consumers at runtime when the application would attempt to access sensitive data for the first time.[83] So, for example, if the flashlight app were to attempt to access contacts on a phone, the consumer would first be notified about the functionality and then be provided with the option to grant or deny dangerous permissions. The decision the consumer makes at that moment is processed for all future permission decisions for that specific command (i.e. the app would always deny the access to

75. *See* Press Release, FED. TRADE COMM'N, Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations Without Permission (June 22, 2016) (on file with author) (explaining InMobi was found to be tracking consumers' locations "whether or not the apps using InMobi's software asked for consumers' permission to do so.").

76. *See generally* Hazim Almuhimedi et al., *Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging*, *in* PROC. OF THE 33RD ANNUAL ACM CONF. ON HUM. FACTORS IN COMPUTING SYS., Apr. 2015, at 78 (discussing an experiment which includes participants' reactions after realizing certain apps were using their location).

77. *See* Yury Zhauniarovich & Olga Gadyatskaya*, Small Changes, Big Changes: An Updated View on the Android Permission System*, *in* PROC. OF INT'L SYMP. ON RES. IN ATTACKS, INTRUSIONS AND DEFENSES, Sept. 2016, at 346, 349-50.

78. *See id*.

79. *See* Ron Amadeo, *Android 6.0 Marshmallow Thoroughly Reviewed*, ARS TECHNICA (Oct. 5, 2015, 12:06 PM), https://arstechnica.com/gadgets/2015/10/android-6-0-marshmallow-thoroughly-reviewed/5/.

80. Wijesekra, *supra* note 60.

81. *See* Guides, *Request App Permissions*, ANDROID, https://developer.android.com/studio/command-line/sdkmanager (last visited Dec. 13, 2019).

82. *See* Jamal Eason, *Develop a Sweet Spot for Marshmallow: Official Android 6.0 SDK & Final M Preview*, ANDROID DEVELOPERS BLOG (Aug. 17, 2015), https://android-developers.googleblog.com/2015/08/m-developer-preview-3-final-sdk.html.

83. *See* Panagiotis Andriotis et al., *Permissions Snapshots: Assessing Users' Adaptation to the Android Runtime Permissions Model*, *in* PROC. OF THE 8TH IEEE INT'S WORKSHOP ON INFOR. FORENSICS & SECURITY, 3 (2016).

read or write contacts. No further permission would be asked explicitly). While Marshmallow did allow the option for consumers to change their permission decision, the initial denial of a permission was buried within multiple levels of system settings. The consumer's decision at the start of the installation process would dictate whether the app could access resources at all future times.[84]

The modern permission model of Android applications utilizes an *ask on first use* ("AOFU") approach.[85] The consumer is prompted at each first instance the application attempts to access the data. The AOFU improved the previous AOI permission model because it gave consumers the chance to deny permissions, while still allowing use of the application.[86] For instance, a chat application wanting to access the microphone at install-time may seem unreasonable to a consumer, but if prompted to access the microphone when a voice message is to be sent to a friend, the intention of the permission is communicated more clearly. The consumer understands that the permission is necessary to properly implement the function the app is attempting to use, while maintaining a reasonable degree of context to the functionally of the applications purpose. The consumer is provided a better understanding of the features that the permission enables and has more contextual information to be informed when making a decision.

B. iOS Developer Guideline Evolution

Prior to iOS 4, users had no per-app control over the Location Services function. If the user had the Location Services function turned on, all other apps could access that information as well. Besides not prompting user permission first, it did not indicate if another app was tracking user location.[87]

Fast-forward to iOS 10, when the third-party apps downloaded by users did not ask the user for permissions, even if the app was accessing user data.[88] The release of iOS 10 saw some major changes to app permissions, increasing the responsibility of app developers by adding a requirement that developers would need to provide a description for any requested permissions of user data.[89] When downloaded, accessing its API will launch a permission prompt to the user (or crash if no description is given). This includes the use of Bluetooth sharing, camera, location, contacts, and others.[90]

---

84. *See* Ahmed Alaa Al-Hamami & Mohammad Nassar, *Future Challenges in Android*, 5 INT'L J. OF ADVANCED STUD. IN COMPUTER SCI. AND ENGINEERING, 95, 97 (2016).

85. Wijesekera, *supra* note 60.

86. *See id.*

87. *See* Almuhimedi *supra* note 76, at 787 (discussing an experiment which includes participants' reactions after realizing certain apps were using their location).

88. *See Contacts*, APPLE, https://developer.apple.com/documentation/contacts (last visited Dec. 13, 2019).

89. *See iOS Security*, APPLE (May 2019), https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf.

90. *See id.*

Similar to Android, permissions to access data are listed by the app developer in the app bundle.[91] Apps that are linked to recent releases in iOS software (iOS 10 and later), are now required to include the types of data it requires in the Info.plist file in order to run. Users are notified of the data that is used by the app prior to its installation and are then prompted to grant or deny access to that data once the app is installed.[92] Until the user grants access, any API calls to that data are blocked. However, the user is only notified the first time the app requests access, and any subsequent API calls use existing permissions to continue to access the data.[93]

With regard to permissions, the OS uses a permission structure that was designed to prevent apps from performing unauthorized operations. In order to protect system integrity, all third-party apps are run as non-privileged users that is partitioned by the OS as "read-only," which prevents apps from modifying system files or making unauthorized system calls.[94] Third-party apps are also restricted by iOS APIs from expanding their privileges or accessing files that belong to other apps.[95] So if a third-party app attempted to access a user's contacts, for example, the user would first be prompted to provide or deny permission to the app. User information can only be accessed through the use of declared 'Entitlements' that are digitally signed, which are used by some of the system apps to perform specific privileged operations. iOS also prevents apps from accessing data from other files by assigning apps to a random unique home directory when they are installed.[96]

Apple has also taken security measures regarding its own applications and programs. Apple's virtual assistant, Siri, uses an iOS extension mechanism to verify a third-party app's permissions before providing it with access to iOS protected user data.[97] In order to prevent any exposure of user data to Apple from information communicated between a user's home IoT devices and an iOS device, Apple introduced 'HomeKit,' which is a software framework infrastructure that utilizes iOS security to protect private data.[98]

Unfortunately, the newer AOFU permission models do not solve issues with managing consumer privacy in mobile environments. Blanketed approval to access consumer data is still processed without consensual agreement. Additionally,

91. *See* ANDRES KURTZ ET AL., DYNAMIC PRIVACY ANALYSIS OF iOS APPLICATIONS (Friedrich-Alexander-Universität Erlangen-Nürnberg Technical Rep. 2014).

92. *See Device Compatibility*, APPLE (Oct. 30, 2017), https://developer.apple.com/library/archive/documentation/DeviceInformation/Reference/iOSDeviceCompatibility/DeviceCompatibilityMatrix/DeviceCompatibilityMatrix.html.

93. *See App Store Review Guidelines*, APPLE (June 3, 2019), https://developer.apple.com/app-store/review/guidelines/.

94. *See iOS Security*: *iOS 12.3*, APPLE (May 2019), https://www.apple.com/business/docs/site/iOS_Security_Guide.pdf.

95. *See id.*

96. *See id.*

97. *See id.*

98. *See id.*

multiple third-party libraries are embedded within the majority of modern applications. The purpose of these libraries varies: they ease application development and enable features such as crash analytics, social network integration, and app monetization from advertisements.[99] While these third-party services are benevolently intended to aid mobile systems, the functionality of such services are also largely invisible to consumers. In some instances, libraries present negative consequences for consumer privacy as third-party services can track behavior without consent, even across multiple applications on the same device.[100]

Applications also continue to bury means of reasonable notice and choice with their third-party services.[101] Information overload and use of complex legal language in privacy policies also continues to reinforce forced consent on the consumer. What is even more alarming is that once consumers agree to a forced disclosure agreement, U.S. law provides very few protections against third-party involvement.[102] Moreover, as consumers are unaware that third-party recipients collect their personal information and the uses to which it is put, there is virtually no opportunity for individuals to mitigate against privacy harm. To understand what privacies exist, we offer a brief description of previously defined privacy harms experienced by the consumer.

C. Defining Privacy Harms

According to Professor Calo, privacy harms can be categorized into two types of harm: subjective and objective privacy harm.[103] Subjective harm results from perception of unwanted observation or surveillance, or from a feeling of helplessness from lack of control over the flow of personal information.[104] An example of subjective privacy harm could be a consumer gaining knowledge of companies profiling information from a database that contained personal

99. *See* Narseo Vallina-Rodriguez et al, *Tracking the Trackers: Towards Understanding the Mobile Advertising and Tracking Ecosystem*, *in* PROC. OF THE WORKSHOP ON DATA & ALGORITHMIC TRANSPARENCY (2016).

100. *See id.*

101. *See* James P. Nehf, *The FTC's Proposed Framework for Privacy Prot. Online: A Move Toward Substantive Controls or Just More Notice and Choice?*, 31 WM. MITCHELL L. REV. 1727, 1744 (2011) ("insurmountable problems regarding the transparency of privacy and data aggregation practices, the inability to hold firms accountable for harms caused by maintaining suboptimal privacy practices, and the practical realities and behavioral tendencies of individuals making decisions about privacy matters in an online environment all render even an enhanced notice and choice approach to privacy wholly ineffectual.").

102. *See generally* DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 120 (2019) (presenting an overview of such standards).

103. *See* Ryan Calo, *The Boundary of Privacy Harm,* 86 IND. L.J. 1131, 1133 (2011).

104. *See id.*

information.[105] Subjective privacy harm can be exhibited from the increased anxiety experienced by the consumer from data collection activities.[106]

Objective privacy harm persists when personal information that has been collected and used against a consumer in an unexpected, forced manner.[107] For example, identity theft wrongful disclosure of information, blackmail, or a widespread data security breach, constitute objective privacy harm.[108] It is important to note, under Professor Calo's definition unwanted spam, junk mail, and other undesired contacts are also forms of objective privacy harms, due to the significant amounts of time and monetary value placed on protecting against these types of activities.[109] As consumers become aware of reports produced by media and online sources about the massive amounts of personal information industries collect and share with others multiparty members, objective privacy harm becomes more likely to occur because of the helplessness consumer's face in stopping information exchange.[110]

In contrast, subjective privacy harm occurs when a consumer's state of anxiety is heightened which in turn, may alter a consumer's routine behavior.[111] As Professor Calo asserts, despite consumers growing awareness of third-parties actively having access to their personal information, the chance of objective privacy harm also increases.[112] The more third-parties have access to multiple forms of consumer information, the more likely that a consumer who has been profiled, will receive unwanted contacts, or be conditioned to external action that could be potentially harmful.

Third parties have no obligation, aside from certain legal restrictions, to issue choice as an option to inform consumers as to how they will use and disclose collected information. What's even more concerning from a consumer perspective is that such third parties may also not be implementing sufficient data security with the consumer's information. Some of the information collected could be sensitive to the consumer and if there is a security breach, the harm is out of the consumer's control. Thus, once a consumer's personal information has been collected within an exhaustive policy notice system, there is little evidence the consumer has read or appreciates the breadth of the places where their data may end up.[113] In some scenarios it's possible that one of these destinations may be in the hands of third-

105. *See id.*

106. *See id.* at 1131; Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA L. REV. 477, 489–91 (2006) (developing a taxonomy for privacy harms, including those associated with intrusion and/or surveillance).

107. *See* Calo, *supra* note 103, at 1148.

108. *See id.* at1147–52; Solove, *supra* note 106, at 532–48.

109. *See* Calo, *supra* note 103 at 1147–52.

110. *See id.*

111. *See id.*

112. *See id.*

113. *See* Nissenbaum, *supra* note 24, at 7.

party recipients that use it against a consumer in an objectively harmful manner. Or worse, with third parties who face a security breach with personally sensitive data.[114]

III. MULTIPARTY INVOLVEMENT: CONSUMER PRIVACY CONCERNS

There is a disconnect between what is consensually agreed upon by consumers and what data is collected by third-party members. These obscurities put consumer's data at risk. Third-party security regulation varies across different industries and in the event of a data breach, consumers may incur damages from sensitive data leaks, with little to no options for recourse. In the mobile app environment, third-party services also track users without consent across multiple applications and the extent of third-party involvement remains largely invisible to the consumer. This section seeks to first identify the use cases of third-party libraries found in mobile applications. We then introduce media permissions that third parties inherit and identify instances where consumers lack control of their information. To that end, we identify data collection practices conducted by third parties that are invasive to the consumer's rights and over-exceed the user's privacy expectations.

A. Third-Party Libraries

Many mobile app developers rely on third-party services for a variety of purposes, including maintenance, analytics, social network integration, security, and, most notably, advertising.[115] However, third-party libraries inherit the set of permissions requested by the host app, allowing them access to a wealth of valuable consumer data, often beyond what is needed to provide the expected service to the app developer.[116] For instance, an application allowing location sharing may in turn allow the same set of location permissions to be automatically granted to the third-party service embedded in its application code.[117] If the same library is used by multiple applications, the third-party service can collect multiple streams of consumer data simultaneously from different apps while a mobile device is active.[118]

114. *See* SYMANTEC, INTERNET SECURITY THREAT REPORT (2019).

115. Ziang Ma et al., *LibRadar: Fast and Accurate Detection of Third-Party Libraries in Android Apps*, *in* PROC. OF THE INT'L CONF. ON SOFTWARE ENGINEERING (2016).

116. FED. TRADE. COMM'N, *supra* note 75, at 19.

117. *See* Theodore Book & Dan S. Wallach, *A Case of Collusion: A Study of the Interface Between Ad Libraries and Their Apps*, *in* PROC. OF THE ACM WORKSHOP ON SECURITY & PRIVACY IN SMARTPHONE & MOBILE DEVICES (2013); *see also* Michalis Diamantaris et al., *REAPER: Real-time App Analysis for Augmenting the Android Permission System, in* CODASPY '19 (2019).

118. Vallina-Rodriguez, *supra* note 99, at 17.

These active libraries present negative consequences for consumer privacy.[119] Most third-party services operate in the background of a mobile device and do not provide any form of visual cue inside the app to notify the consumer that information is being collected.[120] The general lack of transparency in mobile systems leaves the consumer with virtually zero means to identify the third-party services used by their active application, let alone to know what extent those service are able to collect, correlate, and aggregate with their personal information.[121] As a result, consumers have no insight into how these services operate or how they handle sensitive data. Moreover, once the data leaves the device, a consumer is not provided any sufficient information explaining whether or not that third-party service sells the data to other third-parties.[122] Despite past efforts by academics and regulators, there is still a clear deficiency of consumer protection rights provisioned in the mobile environment.[123] A collective understanding of how companies coordinate their relationships and partnerships with third-parties, where they operate, and what their privacy data sharing policies are will need to be more clearly disclosed if the consumer has any hope of being provided sufficient means to protect their personal privacy.

B. Third-Party Media Permissions

The ubiquitous internet connectivity that mobile devices now offer has resulted in a drastic increase in mobile applications that rely on multimedia features.[124] These features rely on high fidelity sensors found in many mobile devices. For example, a mobile device's camera and microphone enable a user to capture pictures, video, and recorded audio files. Apps also utilize other services such as personal voice assistants, facial recognition, and fingerprint authentication.[125]

These multimedia features are dictated by the permissions of the consumer to approve or deny functionality. While these media featured applications offer beneficial use cases to the consumer, apps using such features often violate consumer privacy expectations.[126] When a consumer grants a multimedia

119. *See* Vincent Toubiana et al., *Adnostic: Privacy-Preserving Targeted Advertising*, *in* PROC. NETWORK & DISTRIBUTED SYS. SYMP. (2010).

120. Michael Kassner, *Take Secret Photos by Exploiting Android's Camera app*, TECHREPUBLIC (June 16, 2014, 7:53 AM), https://www.techrepublic.com/article/take-secret-photos-by-exploiting-androids-camera-app/.

121. *See* Ashwin Rao et al., *Meddle: Enabling Transparency and Control for Mobile Traffic*, TECHNOLOGY SCIENCE (Oct. 30, 2015), https://techscience.org/a/2015103003/.

122. *See* Shuai Hao, Bin Liu, Suman Nath, William G.J. Halfond & Ramesh Govindan, *PUMA: Programmable UI-Automation for Large-Scale Dynamic Analysis of Mobile Apps*, *in* PROC. OF THE INT'L CONF. ON MOBILE SYSTEMS (2014).

123. *See id.*

124. *See* Vasilios Mavroudis et al., *On the Privacy and Security of the Ultrasound Ecosystem*, *in* PROC. OF THE PRIVACY ENHANCING TECH. SYMP. (2017).

125. *See* Vallina-Rodriguez, s*upra* note 99, at 16.

126. *Id.*

permission to an app, the designated permission also is applied to any third-party library Software Development Kit ("SDK") package included in the app. Thus, consumers are unaware of the extent of privacy risks generated from the approved permissions they grant access to.[127]

In addition, on both iOS and Android there is no permission required for third-party code in an app to continuously record what is displayed on a consumer's device.[128] As such, consumers unwittingly use apps that are granting over-privileged permissions. For instance, an applications third-party library may collect video recordings containing sensitive information similar to session-replay scripts or browser tracking mechanisms on websites.[129] Moreover, these libraries can accomplish this functionality without requiring any permission from the consumer.[130] When applications are used, sensitive information is often displayed by default. In turn, undisclosed monitoring by third parties stealthily captures personal information of consumers while in session. Several apps also share image and video data if the permissions that granted functionality to a camera or device storage is allowed. For instance, several photo editing applications process photo images online in the background without explicit mentioning of such behavior in the privacy policy or to the consumer.[131]

Consequently, large amounts of applications request multimedia permissions that are never used and include code that uses multimedia sensors without explicitly requesting such permissions to the consumer.[132] This inconsistency violates consumer expectation, while increasing potential privacy risks. Even worse, previously unused permissions can be exploited by third-party libraries that a developer includes in an app.[133] Third-party code that does not provide permissions to use multimedia in a version of an application may start exploiting any

---

127. *Id.*

128. *See* Xing Gao, Dachuan Liu, Haining Wang & Kun Sun, *PmDroid: Permission Supervision for Android Advertising*, *in* SYMP. ON RELIABLE DISTRIBUTED SYSTEMS (2019); *see also* Michael C Grace, et al., *Unsafe exposure analysis of mobile in-app advertisements*, *in* ACM CONF. ON SECURITY AND PRIVACY IN WIRELESS AND MOBILE NETWORKS (2012).

129. Steven Englehardt, *No Boundaries: Exfiltration of personal data by session-replay scripts*, FREEDOM TO TINKER (Nov. 15, 2017), https://freedom-to-tinker.com/2017/11/15/no-boundaries-exfiltration-of-personal-data-by-session-replay-scripts/.

130. *See* Christophe Leung et al., *Should You Use the App for That?: Comparing the Privacy Implications of App- and Web-based Online Services*, *in* PROC. OF THE INTERNET MEASUREMENT CONF. (2016).

131. *See* Elleen Pan et al., *Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications*, *in* PROC. ON PRIVACY ENHANCING TECHNOLOGIES 1-18 (2018); *see also* Szymon Sidor, *Exploring Limits of Covert Data Collection on Android: Apps can Take Photos with your Phone without you Knowing*, EZ.AI (May 22, 2014), http://www.ez.ai/2014/05/exploring-limits-of-covert-data.html.

132. *See id; see also* Abbas Razaghpanah et al., *Apps, Trackers, Privacy, and Regulators: A Global Study of the Mobile Tracking Ecosystem*, *in* PROC. OF THE NETWORK & DISTRIBUTED SYS. SECURITY SYMPOSIUM (2018).

133. *See* W. Enck, P. Gilbert et al., *Taintdroid: an information-flow tracking system for realtime Privacy Monitoring on Smartphones, in* PROC. OF THE 9TH USENIX SYMP. ON OPERATING SYSTEMS DESIGN AND IMPLEMENTATION (2010).

permissions granted to a future version of the app for an unrelated purpose. Such practices could impose additional privacy risks, since third-party libraries can potentially load additional code once a permission is granted without developers or consumers knowing.[134]

Furthermore, there is an inconsistency between permissions and API calls found in an application's intention of use.[135] These problems lead to over-privileged permissions provisioned in large quantities of mobile apps. Therefore, there is a need for developers to more carefully consider how they request certain media functionality. For example, an application may have required permission in a previous version, however, the developer may have failed to update the requested permissions in the newer version of the app.[136] Additionally, the mapping between the applications permissions and the APIs referenced may be poorly documented, leading to confusion among the development teams.[137] Also, third-party software development kits provide copy-and-paste instruction for integration that includes all potentially needed permissions, even if the app does not use the embedded library to function.[138]

C. Privacy Notices

Privacy notices are intended to provide the consumer the opportunity to control their information and protect their privacy,[139] but often times the consumer does not take the time to read the notices provided.[140] The utility benefit of reading policy notices as opposed to the immediate gratification of skipping such statements and gaining access to services far exceeds how consumers make their choice. While privacy notices are produced to provide consumers the opportunity to control and protect their information, such notices are defective because consumers receive very little relevant information about the involvement of third-party services.[141] Adequate information that determines who your personal data is

134. *See id.*

135. Szymon Sidor, *Exploring Limits of Covert Data Collection on Android: Apps can Take Photos with your Phone without you Knowing*, EZ.AI (May 22, 2014), http://www.ez.ai/2014/05/exploring-limits-of-covert-data.html.

136. *See* Pan, *supra* note 131, at 9.

137. *See id.*

138. *See id.*

139. *See* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, iii (2010), http://www.ftc.gov/os/2010/12/101201privacyreport.pdf (stating "the Commission's goal in the privacy arena has remained constant: to protect consumers' personal information and ensure that they have the confidence to take advantage of the many benefits of the ever-changing marketplace.").

140. *See id.* (stating "the notice-and-choice model, as implemented, has led to long, incomprehensible privacy policies that consumers typically do not read, let alone understand.").

141. *See id*. at 24 ("Complaint, Request for Investigation, Injunction, and Other Relief of Center for Digital Democracy, U.S.PIRG, and World Privacy Forum, In the Matter of Real-time Targeting and Auctioning, Data

shared with and what purpose it is used for are basic levels of trustworthy disclosure company privacy notices should be willing to reveal.[142] Technologist have created many types of different applications consumers can use as options to make sense of privacy notices and the flow of information, however, consumers are reluctant in effectively utilizing these technologies, and the most relevant devices are still underdeveloped.[143]

Privacy notices can't be improved until the U.S. privacy regime actively employs effective policy enforcement which requires companies to produce notices that reasonably allow the consumer to have controlled notice and choice to their personal information. Additionally, the public will need to take their privacy rights seriously. Fast acting design options implemented through sociotechnical enhancements can help simplify privacy notice information in a manner presented in a more easily understandable and less burdensome format for the consumer to read. Developers and technologist creating such technologies can help create incentives that allow consumers to more actively inform themselves about company notices and take their privacy rights seriously. The public will continue to suffer from the ambiguity we find in privacy notices until both legislative enforcement and sociocultural elements surrounding information privacy are improved.

In order to implement effective notice and choice to the consumer, policy technologists and legislators must be willing to implement policies that address the exhaustive amount of criticisms surrounding notices consumers receive. On top of the notice issues consumers already experience, personal information is constantly being transferred from one international jurisdiction to another, with drastically different privacy laws at play. If there is any hope to improve third-party disclosure issues and consumer control, these criticisms must be addressed. Accordingly, if these criticisms are not realized, third-party members will continue to actively use and spread consumer information with very little concern to the consumer's privacy.

D. Notice Deficiency

While many sources have noted that consumers do not read the entirety of notices, it is no secret that the majority of privacy notices are unreasonably long.[144]

Profiling Optimization, and Economic Loss to Consumers and Privacy (2010), available at http://www.uspirg.org/uploads/eb/6c/eb6c038a1fb114be75ecabab05b4b90b/FTCfiling_Apr7_10.pdf.").

142. *See id.* at 26–27 (stating "privacy policies have become long and incomprehensible, placing too high a burden on consumers to read, understand, and then exercise meaningful choices based on them.").

143. *See id.*

144. *See* PATRICK GAGE KELLEY ET AL., STANDARDIZING PRIVACY NOTICES: AN ONLINE STUDY OF THE NUTRITION LABEL APPROACH 1 (2010), http://www.cylab.cmu.edu/_files/pdfs/tech_reports/CMUCyLab09014.pdf (determining that "standardized privacy policy presentations can have significant positive effects on accuracy and speed of information finding and on reader enjoyment of privacy policies.").

Researchers from Carnegie Mellon, Lorrie Cranor and Aleecia McDonald, collected privacy policies from the top 75 websites and calculated the median length of policies, with the results showing the median length to be 2,514 words.[145] A standard reading rate in academic literature was assessed as being 250 words a minute, so assuming that the majority of consumers have standard reading levels of academics (which they don't), then a privacy policy would cost the average person about 10 minutes to read.[146] Professor Cranor then calculated the amount of time for the average person to read every privacy policy from every website out of the 75 sites analyzed.[147] To accomplish this feat, it would take the average person a total of 25 days. If reading these policies were to be quantified from a 9:00 AM – 5:00 PM job scenario, it would take the average person 76 workdays to complete the task.[148] Nationally, the total amount of time implemented by all consumers was calculated at 53.8 billion hours (6,141,552 years) of time required.[149]

The opportunity cost lost was even more staggering. Professor Cranor constructed a hypothetical opportunity cost nationally for reading internet privacy policies.[150] The researchers first split up web surfing between home and work visits, valued the time spent reading privacy policies at two times a worker's wage, and multiplied the time spent reading at home by one-quarter of average wages for home visitors.[151] Professor Cranor calculated the hypothetical national net opportunity cost of reading privacy policies at $781 billion.[152] For comparison, Google's market cap value was $780 billion in July of 2019.[153] Professor Cranor's study was conducted in 2008, so there is little doubt that the number has only increased.[154] These statistics alone show how fundamentally broken information privacy is. This data continues to add to the notion that the collective weight of policy length does not reasonably allow consumers to maintain responsible ownership of personal data. Third-party recipients will always be blanketed in dubious protections if the lengths of privacy notices given to the consumer are unreasonably long.

145. Aleecia M. McDonald & Lorrie Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A J. L. & POL'Y FOR THE INFO. SOC'Y 543, 553–54 (2008).

146. *See id* at 554–55.

147. *See id*. at 562–63.

148. *See id*. at 563.

149. *See id.*

150. *See id.* at 561–62.

151. Aleecia M. McDonald & Lorrie Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: A J. OF L. & POL'Y FOR THE INFO. SOC'Y 543, 558–59, 561–62 (2008).

152. *See id.* at 544.

153. *See Alphabet Market Cap*, YAHOO, (Aug. 13, 2019, 12:07 AM), https://ycharts.com/companies/GOOG/market_cap.

154. *See id.*

IV. LEGAL MANEUVERS PROTECTING PRIVACY

The United States lacks a single, comprehensive federal privacy law that regulates the collection and use of personal information. Instead, the U.S. privacy regime relies on regulating data protection with only certain sectoral laws at the federal and state level. A misplaced reliance on privacy torts has also created overlapping problems that further complicate the privacy law discussion. The United States approach to privacy laws fails to address consumer protection, and the related proposals leave these issues gaping. This section will briefly explore the U.S. Privacy Protections from the Federal and State level and will then explore several of the more promising areas of emerging regulation.

A. Overview of U.S. Privacy Protections

There are several adopted sectoral and state laws practiced within the U.S. that provide specific industry guidelines with different types of personal information. For example, sectoral laws include: The Fair Credit and Reporting Act ("FCRA"); The Gramm-Leah-Bliley Act; The Children's Online Privacy Protection Act ("COPPA"); and The Video Privacy Protection Act ("VPPA"). However, if the company doesn't fall within an often-narrow scope of sectoral coverage, the law is inapplicable to their activities. Hence, the limited coverage leaves gaps in regulation and often leaves individuals unprotected.

1. At the Federal Level

While there are several federal sectoral based privacy laws within the U.S., many of the protections afforded to consumers-under these laws are less than stellar. In fact, it is often the case that the limited scope of the law provides little-to-no protection for the consumer. For example, while individuals may assume the Health Insurance Portability and Accountability Act ("HIPAA") may cover the information contained on your IoT enabled Garmin or Fitbit device, in fact, only "covered entities" such as health plans, health care providers, and health care clearinghouses, fall within the regulation.[155] Similarly, the FCRA only protects as private the information contained within the files of consumer reporting agencies. The Gramm-Leach-Bliley Act, also known as the Financial Modernization Act, requires financial institutions to explain company information-sharing practices to their consumers.[156] As one can see, the majority of privacy-based protections are incredibly limited in scope–thereby leaving a large swath of individuals who fall outside these situations and environments unprotected.

Moreover, even in the events that information is covered within one of these sectoral laws, the laws fail to protect information within the current data gathering

155. *See* U.S. DEP'T OF HEALTH & HUM. SERVICES, UNDERSTANDING HIPPA PRIVACY: FOR COVERED ENTITIES (2017).

156. *See* Federal Trade Comm'n, Fair Credit Reporting Act, 15 U.S.C. § 1681 (2012).

environment. For example, all of these industry-specific laws require "covered entities" to produce forms of notice and choice to consumers before providing collected consumer information to third-parties, with the notice and choice coming in the form of a blanketed opt-in/opt-out approach[157] that is deficient (as described above).[158] In situations such as this, the consumer is unaware and is in fact, often unable to discern entities that will receive their information and has no real means of discovering how the entity will use the data. This ambiguity, therefore, still leaves the consumer with little control over their personal information, despite being offered thoroughly produced privacy notices that followed strictly practiced, industry-specific guidelines.[159]

Supplementary to federal sectoral laws, the Federal Trade Commission ("FTC") has privacy related enforcement powers arising when companies engage in defined and proximate "unfair" or "deceptive" trade practices.[160] Under this law, entities are prohibited from commercial conduct that: (1) causes (or is likely to cause) substantial injury to consumers; (2) that consumers cannot reasonably avoid themselves; and (3) without offsetting benefits to consumers or competition.[161] As information technology continues to advance in business operations and advertising, what constitutes deceptive or unfair trade practices continues to evolve. For example, the failure to implement sufficient security measures or failure to adequately disclose information-handling practices have already given rise to enforcement action against companies.[162]

Unfortunately, even federal enforcement authority fails to address the consumer's lack of control or understanding of information provided in privacy notices.[163] For example, the majority of enforcement activity is squished so long as the entity can demonstrate the existence of an opt-in/opt-out information sharing agreement. As previously discussed, these approaches often fail to provide adequate information to the consumer and provide no meaningful way to receive services once an opt-out is selected. As such, these agreements are widely used within industries and thereby leave little protections to consumers.

157. GRAMM-LEACH-BLILEY ACT OF 1999, 15 U.S.C. § 6808 (2012).

158. *See supra* discussion accompanying notes 155–57.

159. *See* Barocas & Nissenbaum, *supra* note 50.

160. *See* PETER SWIRE & SOL BERMANN, INFORMATION PRIVACY 70 (2007).

161. Federal Trade Comm'n Act, 15 U.S.C. § 45 (2012).

162. Press Release, Fed. Trade Comm'n, Sears Settles FTC Charges Regarding Tracking Software (Jun. 4, 2009), http://www.ftc.gov/opa/2009/06/sears.shtm (agreeing that Sears "failed to disclose adequately the scope of consumers' personal information it collected via a downloadable software application.").

163. *See, e.g.*, FED. TRADE COMM'N, GATEWAY LEARNING SETTLES FTC PRIVACY CHARGES (2004), https://www.ftc.gov/news-events/press-releases/2004/07/gateway-learning-settles-ftc-privacy-charges (agreeing that Gateway "violated federal law when it rented consumers' personal information to target marketers").

2. At the State Level

From an information privacy perspective, state statutory law also provides very little assistance to the consumer. With the exception of California's "Shine the Light Law," and the California Consumer Privacy Act ("CCPA")[164] no other state requires companies to provide consumers disclosure of information with their information-sharing practices or a list of companies they share consumers information with for advertising purposes.[165] So long as companies provide consumers with an opt-in or opt-out mechanism and the consumer is not a California resident, companies are not required by law to disclose the third-parties with which a company shares information with or provide access rights to the consumers they collect from.[166]

Consequently, the majority of states in the United States do not even require companies to develop privacy policies or any kind of useful notice and choice the consumers may read.[167] As previously mentioned, the most promising form of state statutory law can be exemplified with California's "Shine the Light Law" and CCPA.[168] California's information privacy laws require companies to disclose their information-sharing practices to consumers and, if requested by the consumer,[169] companies are required to disclose consumers with a list of third-party members they have shared the consumer's information with.[170] Other notable state laws include Utah's statutory adoptions,[171] which require certain companies to disclose to consumers what type of information they may disclose to third-parties.[172] Connecticut has also required privacy policies to be posted in the event that entities collect social security numbers.[173]

While these state laws are a step in the right direction for consumers' information privacy, most of these state statues do not require notice and choice about the specific third-parties to be included in their privacy policies.[174] Even if California's "Shine the Light" statute does not mandate active third-party listing and

164. *Examining Safeguards for Consumer Data Privacy Before the S. Comm. on Commerce, Science & Transp.*, 115th Cong. (2018).

165. Clark D. Asay, *Consumer Information Privacy and the Problem(s) of Third-Party Disclosures*, 11 NW. J. TECH. & INTELL. PROP. 321, 330 (2013).

166. *See* CAL. CIV. CODE § 1798 (2006).

167. *See* Asay, *supra* note 165, at 341.

168. *See* Leslie Flint, *California's "Shine the Light" Marketing and Junk Mail Law*, PRIVACY RIGHTS CLEARINGHOUSE (June 2005), https://www.privacyrights.org/consumer-guides/shine-light-marketers-find-out-how-they-know-your-name.

169. *See id.*

170. *See California S.B. 27, "Shine the Light" Law* EPIC, https://epic.org/privacy/profiling/sb27.html (last visited Dec. 13, 2019).

171. *See* National Conference of State Legislatures, *Selected State Laws Related to Internet Privacy*, NAT'L CONF. OF STATE LEGISLATURES (May 13, 2019), http://www.ncsl.org/default.aspx?tabid=13463#isp.

172. *See id.*

173. *See id.*

174. *See id.* (explaining that NCSL notes only three such states: California, Nevada, and Vermont).

companies are exempt from this law if consumers are offered opt-in/opt-out options.[175] Therefore, state privacy statutes barely scratch the surface in adequately protecting consumer's privacy. The consumer is left virtually unprotected in the majority of U.S. jurisdictions.[176]

Instead of comprehensive protection, the majority of states recognize privacy torts such as: (1) intrusion upon seclusion or solitude, or into private affairs; (2) public disclosure of embarrassing private facts; (3) publicity which places a person in a false light in the public eye; and (4) appropriation of one's name or likeness.[177] Some commentaries go so far as to claim that additional regulations would be unduly burdensome, with little-to-no real privacy benefits provided to the consumers.[178] In contrast, some commentators and organizations argue that since almost every state recognizes privacy torts these tortious based rights are therefore the best hope for protecting consumer information privacy.[179] They support this argument by highlighting the limitations of implementation at the socioeconomic or technical levels.[180]

Unfortunately, as emphasized above, the advancement in technology and the insistence upon third-party permissions and misguided developer practices, imposes upon the consumer sharing expectations and reduces the options which a consumer can assert in opposition. In environments such as this, consumers are essentially left with no recourse at all.[181] This is because, the standards currently established are outdated[182] and are not able take into account the increasing advancements of technologies and how they affect information privacy.[183] For example, Professor Asay emphasizes that "courts have been reluctant to recognize privacy torts in cases where the information collected was publicly available or

175. *See id.*

176. *Consumer Privacy*, PUBLIC KNOWLEDGE https://www.publicknowledge.org/issues/consumer-privacy/(last visited Dec. 13, 2019).

177. *See* William Prosser, *Privacy*, 48 CAL. L. REV. 383, 422 (1960) ("It is evident from the foregoing that, by the use of a single word sup-plied by Warren and Brandeis, the courts have created an independent basis of liability, which is a complex of four distinct and only loosely related torts; and that this has been expanded by slow degrees to invade, overlap, and encroach upon a number of other fields".).

178. *See* Robert E. Litan, *Balancing Costs and Benefits of New Privacy Mandates, in* AEI-BROOKINGS JOINT CTR. FOR REGULATORY STUDIES, (1999) ("[P]olicy makers here should consider new privacy-related proposals. . . that *balances* privacy interests on a case-by-case basis against the importance of ensuring the free flow of information."), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=179074.

179. *See* Andrew J. McClurg, *A Thousand Words Are Worth a Picture: A Privacy Tort Response to Consumer Data Profiling*, 98 NW. U. L. REV. 63, 142 (2003).

180. *Id.* at 91–101.

181. *Id.* At 89–91.

182. Helen Nissenbaum, Deregulating Collection: Must Privacy Give Way to Use Regulation? 1 (May 1, 2017) (unpublished manuscript) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3092282.com/sol3/papers.cfm?abstract_id=3092282.

183. *Id.*

where a reasonable person would not be offended by the collection."[184] In these types of instances, however, the courts are neglecting the fact that database technology can store thousands of confidential pieces of information about a person in a profile, making it very easy for companies to share sensitive information with third-parties.[185]

In some instances, courts have also adopted a view of consumer privacy differentiated as public or private,[186] where some information is voluntarily public[187] and other forms of information are viewed as private.[188] The ambiguity between what is voluntarily private and public, however, is distorted as context matters in most of these instances. Moreover, as Professor Asay interjects, privacy torts rely on the concept of physical space to define expectations and harm.[189] Because of this viewpoint, "courts in applying privacy torts to the digitized world have largely neglected privacy harm that does not fit neatly into the old paradigm."[190] As a result, consumers are left to fend for themselves and even when they discover a potential avenue to protect their privacy the outcomes often fail to offer any true protection.

B. Promising Legal Regulations

Over the last decade privacy regulation has changed markedly. Policymakers have been forced to design privacy and data protection laws that are flexible to the unforeseen advancements of technology. Most notably, the General Data Protection Regulation ("GDPR") and CCPA are two globally impactful laws that are creating sweeping changes toward consumers privacy rights. The GDPR, which began enforcement last year, enhances data protection and privacy rights for individuals within the European Union ("EU") and European Economic Area ("EEA"). Like the GDPR, the CCPA is an American law aimed at providing control of personal data to California residents and will go into effect by January 1, 2020. Both regulations provide the consumer with better means of control over their personal data. The cascading impacts of both the GDPR and CCPA continue to change the U.S. privacy law regime on a global scale, leading to numerous laws being passed and multinational organizations elevating privacy to a board level issue. Privacy is all over the media and it is hard to dispute the role that the GDPR and CCPA have played in sustaining the privacy law conversation. Among tech companies, it has become common knowledge that to ignore privacy is to risk reputation and leave the organization in the competitive dark ages. Moreover, the regulations introduce

184. Asay, *supra* note 165.

185. *Id.*

186. *Id.*

187. *Id.* at 330 n.60 (arguing that context is an essential consideration).

188. *Id*.

189. *Id.*

190. *Id.* at 330.

serious fines that companies must now consider with their data collection practices. Furthermore, both laws present promising outcomes for the future of consumer privacy rights.

1. GDPR

The GDPR is a new data protection directive that builds upon the European Data Protection Directive[191] and implements new models of privacy and data protection law. While the Data Protection Act previously sought out how personal information was used by companies, government entities, and other organizations,[192] the GDPR now changes how personal information can be used. Individuals, organizations, and companies who are defined as either "controllers"[193] or "processors"[194] of personal information are held accountable for their information collection practices, including the requirement of the completion of a data protection impact assessments and accurate explanations of how data is collected and processed.[195] Moreover, the GDPR requires concise and clear information to be provided about consent, thereby requiring a "positive opt-in"[196] option for the consumers. Garnering the most attention are the provisions relating to the consumers ability to request all information that a company holds about them[197] and the "Right to Be

191. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281), 31–50.

192. Data Protection Act, 1998, c. 29, § 1, (U.K.), http://www.legislation.gov.uk/ukpga/1998/29/section/1/enacted.

193. *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679/EC, art. 3–4, 7–8 Recitals 2, 7, 8, 14, 22-–5 (explaining that the GDPR only protects natural persons (individuals) and does not cover legal persons. A data controller is a natural or legal person, public authority, agency or other body that determines the purposes and means of the processing of personal data, alone or jointly with others. A controller is defined by the fact that it establishes the means and purposes of the processing).

194. *Id.* at art. 4, 17, 28, 30, 32, 33, 35, 37, 38 Recitals 90, 93 (explaining that the data processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Data processor activities must be governed by a binding contract or other legal act with regard to the controller. The contract should set out the subject matter, duration, nature and purpose of the processing, the types of personal data processed, the security measures, and the obligations and rights of the controller. Processors can only process personal data on instructions from the controller. Upon termination of the agreement with the controller, processors must return or destroy personal data at the choice of the controller. In addition, if the processor wants to engage another processor (sub-processor) it has to have the written authorization of the data controller).

195. *See id.*

196. *Id.* at art. 5–10, Recitals 39–48, 69, 70 (explaining that the GDPR provides data subjects with a right to withdraw consent at any time as well as a right to object if their personal data is processed on the basis of legitimate interest or performing of a task in the public interest); s*ee* GDPR Art. 21 Recitals 69, 70.

197. *Id.* at art. 12, 15, 20, 21 Recitals 59, 63, 64 (explaining that the GDPR states that, when responding to an access request, a data controller must indicate the purposes of the processing; the categories of personal data concerned; the recipients or categories of recipients to whom personal data have been disclosed to; and

Forgotten" provision which requires a company to delete all information about an individual upon request.[198]

Unlike other reviewed legislative enactments, the GDPR implements harsher fines that empower regulators to enforce compliance.[199] For example, the Commission Nationale De l'informatique ("CNIL"), France's data protection regulator, issued a $56.8 million fine against Google for violating user's "genuine consent" standards.[200] As can be seen, the penalties can run into the millions of dollars and can include a penalty based upon worldwide revenue.[201]

2. California Consumer Privacy Act

The CCPA enhances privacy rights and consumer protection for California residents as it applies to any business organization with annual gross revenues greater than $25 million that does business in California.[202] Under the CCPA, consumers have the following rights: (1) the right to know what personal data is being collected about them; (2) the right to know if their personal data is sold or disclosed; (3) the right to know if their personal data is being sold, to whom it is being sold to; (4) the right to deny permission of sale of their personal data; (5) the right to access their personal data; (6) the right to access to equal service and price, regardless of whether they exercise their privacy rights or not.[203]

According to the CCPA, personal data is any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked,

any sources from which data was collected. The GDPR specifies that individuals also have the right to receive a copy of the personal data processed about them).

198. *Id.* at art. 12, 17 Recitals 59, 65–66 (explaining that the scope of this right is not limited to the data controller, but also impacts third parties, such as recipients, data processors and sub-processors that may have to comply with erasure requests. This right can be exercised free of charge. There may be some instances where a fee may be requested, notably when the requests are unfounded, excessive or have a repetitive character. The GDPR specifies that data controllers must have in place mechanisms to ensure that the request is made by the data subject whose personal data is to be deleted).

199. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 83, 84, Recitals 148-152, OJ 2016 L 119/1 (depending on the violation occurred the penalty may be up to either 2% of global annual turnover or €10 million, whichever is higher; or 4% of global annual turnover or €20 million, whichever is higher. The amount of the penalty may also vary depending on "the nature, gravity and duration of the infringement," the nature of the processing, the number of data subject affected, and the damages suffered, the negligent or intentional character of the infringement, etc., with a complete list in Article 83(2) of the GDPR).

200. Emily Price, *France Fines Google $57 Million For GDPR Violations*, FORTUNE (Jan. 21, 2019), http://fortune.com/2019/01/21/france-fines-google-57-million-for-gdpr-violations/.

201. Regulation (EU) 2016/679 at art. 83, 84, Recitals 148–152, OJ 2016 L 119/1.

202. CAL. CIV. CODE § 1798.100-198.

203. Theodore Augustinos & Laura Ferguson, *CCPA Guide: Are You Covered by the CCPA*, JD SUPRA, (Jan. 15, 2019), https://www.jdsupra.com/legalnews/ccpa-guide-are-you-covered-by-the-ccpa-38771/.

directly or indirectly, with a particular consumer or household."[204] The CCPA differs from the GDPR in that the GDPR classifies consumer information as personal only. In contrast the CCPA extends its definition to households.[205] The GDPR also extends to all EU citizens while the CCPA only extends to California residents.[206]

Under the CCPA, consumers also have legal grounds to sue any businesses that violate the bill.[207] Businesses that violate the CCPA are fined up to $7,500 for each intentional violation[208] and $2,500 for each unintentional violation under Section 1798.155 of the Civil Code.[209] Like the GDPR, the CCPA will have significant global impact, given that California boast the world's fifth-largest economy. Together, the two regulations aim to guarantee individuals greater control over their personal data, while providing the consumer with rights to have access to their information.

V. LEGAL-TECHNICAL SOLUTIONS

Consumers have become increasingly cautious about providing information to companies, due to the prospect of companies misusing or mishandling their sensitive information.[210] With privacy rights becoming prioritized due to recent regulation, companies have responded with joining privacy "seal" programs such as "as TrustE,[211] and privacy alliances such as the Online Privacy Alliance.[212] These best practices typically require companies to produce notices to consumers informing them how the company collects information, how the company will use it, and what type of third-parties will have access to consumer information. While these industry practices seem reasonable and considerate to the consumer's privacy, Professor Asay states that there are two drawbacks to self-regulated industry practices: adequacy and enforcement.[213] Companies possess a self-interest in retaining flexibility with consumer information.[214] Therefore, a company's self-regulatory approach often varies with effectiveness in providing consumers with adequate

204. BigID. *CCPA Redefines Personal Information: Does Your Organization Know Its PI From PII?* MEDIUM, (Apr. 14, 2019), https://medium.com/bigid-on-id-privacy/ccpa-redefines-personal-information-does-your-organization-know-its-pi-from-pii-f5ccc38db2a9 (citing CAL. CIV. CODE § 1798.140).

205. Sarah Hospelhorn, *California Consumer Privacy Act (CCPA) vs. GDPR*, VARONIS, (last updated Nov. 5, 2018), https://www.varonis.com/blog/ccpa-vs-gdpr/.

206. Jon Fielding, *Four differences between the GDPR and the CCPA*, HELPNET SECURITY, (Feb. 4, 2019), https://www.helpnetsecurity.com/2019/02/04/gdpr-ccpa-differences/.

207. CAL. CIV. CODE § 1798.155.

208. § 1798.155(b).

209. *Id.*

210. FED. TRADE COMM'N, *supra* note 75.

211. *TrustArc Acquires Nymity to Reimagine Privacy*, TRUSTARC (Nov. 19, 2019), https://www.trustarc.com/press/trustarc-acquires-nymity-to-reimagine-privacy/.

212. *See generally Privacy Alliance,* PRIVACYALLIANCE, http://www.privacyalliance.org/(last visited Dec. 13, 2019).

213. Asay, *supra* note 165, at 331.

214. *Id.* at 331.

protection and control of their information. Self-regulation also relies on companies regulating their own behavior,[215] and not all self-regulating practices are created equal.

Even companies who attempt to implement best practices with privacy information struggle with providing consumers with adequate information control. Self-Regulating practices are still plagued with ambiguous, blanketed legal language and unidentified third-parties who can still utilize consumer information.[216] From a consumer's point of view, consumers receiving notice and choice should adequately be supplied with who is receiving their information and how the company plans to use it. Instead, consumers are presented with the general notice that unidentified third-parties will legally receive and use personal information in manners unknown.[217] While self-regulation helps provide incentives for companies to practice safe handling of privacy information, it still offers little control to consumers in receiving appropriate knowledge of where their information is going and how third-parties will use it.

In instances where self-regulation continues to leave consumers unprotected it is likely time that more consideration is given to regulating portions of the data and digital marketplaces. While widespread announcements of warnings, such as with the newest issues surrounding FaceApp,[218] can be effective the release highlights a potential solution that is often unexplored. The marketplace in which the app was approved and released is in no way insisting upon any privacy or protections from developers or third parties. One wonders how long the absence of a commitment to self-regulation will continue to be ignored as a gap in governance–thereby demanding regulation. Free or not, app environments are a marketplace, and thus can be regulated as such. Individuals have demonstrated again and again that they are unable, or unwilling, to gauge real harms. Nonetheless, regulation has long been argued as an appropriate response to the harms. Of course, this regulation is only the tip of the iceberg in terms of resolving harms suffered, yet this area is both ripe for regulation and a good first step in addressing harms to both individuals and other harms suffered by society in a digital eco-system.

Regulation in this area will likely be larger than the area addressed in this paper, as the issues of notice, consent, and design are much wider issues. Without a doubt, we should consider regulation which holds those in control of the marketplace to a standard of safe product, in which the product is certified (and truly is) attentive to privacy, consent, and notice. In addition, any attempt to regulate must be managed via a polycentric approach, in which multiple agencies and individuals have the

215. Asay, *supra* note 165, at 331–32.

216. *Id*. at 332.

217. *Id.* at 333.

218. *See* Donie O'Sullivan, *DNC Warns 2020 Campaigns Not to Use Faceapp 'Developed by Russians'*, CNN (last updated July 17, 2019, 4:18 PM), https://www.cnn.com/2019/07/17/politics/dnc-warning-faceapp/index.html.

ability to enforce regulation and seek redress. Finally, there is mounting evidence that individual designers wish to be given protections for revealing design and deployments that violate the basic expectations of the users and society as a whole. Accordingly, it is time that we support such disclosures through well designed whistleblower protections.

A. Sociotechnical Solutions

In the absence of regulation imposing requirements, technology developers are attempting to create technology driven solutions to address the harms suffered in a digital marketplace. Notice Deficiency limitation has influenced technologists to create devices that offer consumers easier methods of employing choice to privacy notices. Professor Haddadi's Databox proposed a piece of technology mitigating the lack of choice prevalent from vague third-party disclosures found in policy notices.[219]

The Databox offers the consumer a trusted platform that facilitates data management, controlled access against other parties wishing to use consumer data, and support incentive to both consumers and information collectors.[220] The Databox platform enables consumers to coordinate the collection of personal data, while selectively controlling and monitoring their data for their own specific purposes.[221] It also employs three provisions that assist the consumer with these controls: (1) legibility to inspect and reflect what data is being collected and how it is processed, (2) agency to manage data and access it whenever the consumer sees fit, and (3) negotiability to navigate the data's social aspects with the interaction of data subjects and the aligned policies.[222] All of these control mechanisms are developed and deployed through the components of MirageOS, Irmin, and Signpost methodologies.

The Databox is simply providing a consumer the means to understand, control, and negotiate access to the collection of their own data. Professor Haddadi's technology does not implement shortened privacy notices, but does empower the consumer to be able to freely monitor and access the collection of their own data.[223] This piece of developmental technology becomes relevant due to the fact that consumers are aware of where their data is going and how it may be used.[224] While the notice length hasn't changed, consumers can potentially acknowledge what

219. *See* Amir Chaudhry et. al. *Personal Data: Thinking Inside the Box*, 1 AARHUS SERIES ON HUMAN-CENTERED COMPUTING 4 (2015), https://tidsskrift.dk/ashcc/article/view/21312/19626.

220. *See id.*

221. *See id.*

222. *See id.*

223. *See id.*

224. *See id.*

information third-parties have access to and where that information may be traveling. The Databox remains in development.[225]

Further developments to privacy notice efficiency can be found in app design.[226] To mitigate the ongoing problem of privacy notice length, application designers are creating fast-acting implementations that offer consumers shortened, summarized versions of the privacy policies.[227] These summarized versions of notices give the consumer a chance to understand the agreement they are "consenting" to without spending unreasonable amounts of time reading privacy notices they may not understand. The app designers employ these design elements by addressing privacy notices with a checklist to the consumer.[228] The consumer is offered the privacy notice in the form of summarized bullet-points that display relevant content about privacy practices. The consumer is then offered a checklist to agree with each summarized privacy practice.[229]

Following the checklist, the consumer is then immediately offered the chance to enhance special privacy controls. These types of design applications not only make privacy notices easy for the consumers to understand, but also allow the consumer to have reasonable notice regarding data collection practices. Summarized policy application features address the lack of control experienced by consumers and provide the consumer with reasonable amounts of information that the consumer can understand. These design implications are relevant to third-party disclosure because they are reinforcing the willingness of the consumer to read the notices provided since the information is of adequate length. Consumers are not burdened by the feelings of helplessness, confusion, or anxiety that is typically generated by the information overload found in traditional privacy notices. Instead, the consumers receive a concise understanding of the information presented, with a realistic overview that produces a chance for the consumer to make an appropriate, educated decision with their personal data.

To mitigate the underlying lack of consumer choice in privacy notices, the traditional means of documenting communication in commerce is being superseded by multiple instances of electronic agreement,[230] rather than just one singular signature agreement required by the user. In the view of some scholars,

225. *See* Amir Chaudhry et. al. *Personal Data: Thinking Inside the Box*, 1 AARHUS SERIES ON HUMAN-CENTERED COMPUTING 4 (2015), https://tidsskrift.dk/ashcc/article/view/21312/19626.

226. *See* Vitaly Friedman, *Privacy UX: Privacy-Aware Design Framework*, SMASHING MAG. (Apr. 25, 2019), https://www.smashingmagazine.com/2019/04/privacy-ux-aware-design-framework/.

227. *See id.*

228. Vitaly Friedman, *Privacy UX: Common Concerns and Privacy in Web Forms*, SMASHING MAG. (Apr. 4, 2019), https://www.smashingmagazine.com/2019/04/privacy-concerns-ux-web-forms/.

229. *See id.*

230. Laurence Bull et al., *Grouping Verifiable Content for Selective disclosure*, *in* PROC. OF THE 8TH AUSTRALASIAN CONF. ON INFO. SECURITY & PRIVACY 1–12 (Rei Safavi-Naini & Jennifer Seberry eds., 2003), https://dl.acm.org/citation.cfm?id=1760481&CFID=997755448&CFTOKEN=68104605 https://link.springer.com/content/pdf/10.1007%2F3-540-45067-X.pdf.

documents are assessed to merely be containers.[231] Documents have always been semantically boxed with large collections of information. The documents themselves are not the most important properties to a consumer, but rather, the content that lies within.[232] While this observation is obvious, large collections of information contained in a document make it challenging for relevant content to be found. Instead of employing the traditional approach where the consumer signs an entire document and thereby verifies all of the policy disclosures content to a third-party recipient, Professor Bull introduces a fragment extraction policy through the use of privacy enhancing Content Extraction Signatures ("CES").[233] Professor Bull's method enables consumers to view various portions of a privacy notice, where the consumer may sign only the parts of the document he/she agrees with.

The standardization of CES empowers the consumer with reasonable choice. The document is not verified by consumers in one signature and the blanketed opt-in/opt-out methods companies hide are more challenging to insert. The CES method allows the consumers to be selective in what they are agreeing to and providing some control in what they are signing.

B. Personally Identifiable Information

Technological innovations that provide easier means of control and choice to consumer's privacy information will not be effective until federal and state laws are adequately enforced. The current U.S. privacy regime is lacking sufficient protections to consumer's privacy and third-party disclosures are too loosely regulated. Furthermore, laws requiring companies to provide sufficient notice and choice to the consumers describing the intended third-party recipients and their collection uses must be introduced. Consumers must also be uniformly entitled to privacy as a right with options of recourse to protect their privacy interests under the law.

Currently suggested proposals only apply to PII that companies collect and offer to third-party recipients.[234] Companies do not aggregate, anonymized information ("non-PII").[235] There is an unclear notion that third-party recipients could easily use non-PII to cause consumers potential objective privacy harms. These concerns extend to the possibility of re-identification.[236] For instance, a study involving a group of 10,000 anonymized twitter users were successfully re-identified using a "Supervised Learning Algorithm." This algorithm was able to re-identify the

231. *See id.*

232. *See id.*

233. *See id.*

234. *But see* Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701, 1723, 1742–43 (2010) (arguing that true anonymization is impossible).

235. Paul Schwartz & Daniel Solove, *The PII Problem: Privacy and a New Concept of Personally Identifiable Information*, 86 N.Y.U. L. REV. 1814, 1877-78 (2011).

236. *Id.*

anonymized twitter users with 97.6% accuracy.[237] Despite industry efforts to properly anonymize consumer information, computational programs were still able to re-identify these records with accuracy and could potentially aggregate and re-purpose such information.[238] As demonstrated in this study, anonymization techniques still remain in early development and don't guarantee identity perfect anonymization to consumers' data. Since the risks of objective privacy harm are more challenging to access with non-PII, the manner in which non-PII is governed should be regulated differently.[239]

Additionally, since subjective privacy harm is sometimes unavoidable, and harms vary to the levels of extreme sensitivities, legitimate issues that show subjective harm are much harder to address. As previously mentioned, Professor Asay argues that in order for subjective harm to be legitimate, objective privacy harm must also be a potential possibility.[240] As such, he asserts that arguably this "type of harm is unavoidable and results more from the extreme sensitivities of a few than a legitimate issue needing redress."[241] The elements of this discussion assess non-PII as information that cannot be reversed engineered or linked back to consumers.[242]

Following on in this argument, Professor Asay argues that one underlying issue of privacy is the clarity of what constitutes PII. The EU Directive defines "personal data" in broad terms:

> Personal data shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.[243]

This interpretation suggests that personal data may not be necessary to identify a person from related information, under the premise that information is relatable to an identifiable person. For many legislators, the definition of PII is too broad. The California Data Security Breach Act attempts to narrow PII by clarifying personal information as the name of an individual who is associated with multiple forms of sensitive information.[244] While the California law does offer a specific definition, the

237. *See* Herman T. Tavani & Frances S. Grodzinsky, *Responding to Some Challenges Posed by the Re-identification of Anonymized Personal Data*, 2019 COMPUTER ETHICS – PHIL. ENQUIRY (CEPE) PROCEEDINGS. *See also* Beatrice Perez et al., *You are your Metadata: Identification and Obfuscation of Social Media Users using Metadata Information*, 2018 ASS'N FOR THE ADVANCEMENT OF ARTIFICIAL INTELLIGENCE.

238. *Id.*

239. *See* Asay, *supra* note 165, at 341.

240. *Id.* at 341.

241. *Id.* at 341.

242. *Id.* at 341.

243. Asay, *supra* note 165, at 342 (quoting the GDPR).

244. *See id.* at 341.

interpretation only addresses certain types of objective privacy harms. A legislative proposal addressing both extremes of privacy harms that could impact consumers must be offered to effectively regulate privacy.[245] Consequently Professor Asay asserts, "the definition thus focuses the model law on the two forms of privacy harm"[246] thereby rejecting excessive detail while respecting the existing definition of PII.[247]

In further discussion of PII, there are some instances where third-party disclosures should not be applicable to legal solicitation. For example, Professor Asay argues "the law should not apply to government actors pursuing PII as part of an investigation."[248] Instead "the law should only apply if the company disclosed the PII to the third party for a secondary use of the information: a use beyond the purposes for which the individual provided the PII." [249]

Subsequently, legal scholars have proposed that the definition of the term "personally identifiable information" should also encapsulate more static digital identifiers. Additional digital identifiers could extend toward GPS coordinates, Android ID's, and unique device identifiers as being definitively included as PII and not solely interpreted as such.[250] According to Professor McAllister, a more contextual definition is needed to take into account static digital identifiers as being characterized as "personally identifying" when the "particular recipients" of the data are likely to identify a consumer.[251] This would mean that courts would be forced to more directly consider the full extent of particular disclosures.[252] The definition would focus more on the specific recipient and question the ability to identify a user issue based on the "particular" digital identifier.[253] Thus, courts would be more focused on the discovery to be assessed with the identification question. With such changes, courts would have a better understanding of when the statutory definition applies in the discovery identification process.

The suggested definitions to PII provides legislators with a clear explanation of delimiting third-party intent. In the defined instances, interpretation of PII is taking into consideration the initial flow of information taken in by companies and setting appropriate guidelines to the transfer of use by third-party recipients. The definition also addresses privacy harms in specific manners that are not too broad. By reassuring consumers that their PII is disclosed for their own consented purposes,

245. Memorandum from Clay Johnson III, Deputy Director for Management, Office of Management and Budget, to the heads of the of the Executive Departments and Agencies, at 1, n. 1 (May 22, 2007).

246. Asay, *supra* note 165, at 342.

247. *Id.*

248. *Id.*

249. *Id.*

250. *See generally* Marc Chase McAllister, *Modernizing the Video Privacy Protection Act*, 25 GEO. MASON L. REV. 102, 102–03 (2017).

251. *Id.* at 143.

252. *Id.* at 144.

253. *Id.*

and not to unrelated third-party recipients, the instance of subject privacy harm is likely reduced. Objective privacy harm would also be reduced because fewer third-party recipients would be eligible to collect PII in their systems.

C. Legislative Reconstruction

Under the condition that Personally Identifiable Information is definitively adopted in the scope of law in the manner previously suggested, policy remedies could effectively be implemented to empower the consumer with control and choice. Such policy remedies should also resemble the standards imposed in the "Shine the Light" law and the rights provisioned by the CCPA at the national level. The FTC could stipulate provisions that require companies to provide consumers with a third-party recipient list before a company shares PII with its third-party vendors. Moreover, such provisions would provide the consumer with simple means of tracing the involvement of other companies who may be collecting their personal information.[254] A third-party recipient list requirement, would also provide the consumer with a more reasonable degree of notice that is accessible and not buried in vague third-party disclosure language.

Furthermore, a provision requiring third-party recipients in short, summarized forms could also be included and be concurrent to third-party lists. The FTC could work with industries to develop these summaries to provide the most relevant description of information sharing practices and apply such practices to app transparency. By doing so, the harmonization of policy languages between information-sharing practices of the company and the consumer are mutually comprehensible.[255] These standards provide consumers with enhanced opportunity to limit the spread of their information, while limiting privacy harms that could occur from the unknown use of their personal data.

Specifically, in the app markets, companies that host apps and dictate developer requirements could also require app developers to list their ad library packages in similar fashion to the way Dangerous Permissions are already listed in the applications descriptions in the Google Play Store. Such simple means of transparency would provide the consumer with a reasonably accessible means of understanding what parties are involved in the background collection of their data when using a mobile application. Furthermore, states should collectively adopt standards similar to the "Shine the Light" California law and provisioned rights of the CCPA. App developers are not required by law to list Third-Party involvement or provide consumers with access rights in their applications and will not willing do so until regulation requires such practices.

Forty-nine out of the fifty states do not require companies to provide consumers disclosure of information with their information-sharing practices or a list of

254. *See* Asay, *supra* note 165, at 344.

255. *Id.*

companies they share consumers information with for advertising purposes.[256] As long as companies provide consumers with an opt-in or opt-out option, companies are not required by law to disclose the third-parties with which a company shares or may share consumer PII. If states uniformly adopted legislation similar to California's "Shine the Light Law," companies would be held to standards that adequately provide the consumer the chance to receive notice and at least have some sort of choice before providing their consent.

Globally, it is deemed an impossible task to reasonably track the flow of consumer information transferred from one party to another. It is unrealistic and a waste of resources, effort, and time to try and pursue such an endeavor. The way in which proper privacy control and notice can be adequately provided to the consumer is through the adoption of national privacy law as opposed to the mixture of state-by-state privacy legislation and sectoral law. The best way to empower individuals with proper control and notice to personal information is through the refinement of U.S. privacy laws that regulate technological practices at scale. Laws such as the GDPR and CCPA, force refinement of industry standards and present enough regulatory enforcement incentives–ensuring that tech firms take the requirements of the law seriously.

While the GDPR and CCPA are by no means perfect, these types of privacy regulations are the correct steps forward and they force businesses to comply if they want to conduct business in these specific jurisdictions. Similar principles to the GDPR need to be adopted nationally if we are to create a society that still respects the right to privacy.

CONCLUSION

Within the mobile ecosystem, applications are collecting personal information that violate consumer privacy expectations. In these instances, most applications operate as over-privileged to their core function(s). Many applications in both iOS and Android operate as over-privileged, by way of their third-party services embedded in their source code. While these third parties are often times benevolent, there is no notification provided to the consumer to notify who is collecting or what is being transferred. Even worse, there are severely limited

256. While California currently remains the only State that requires businesses to list their third parties upon request, other states are following several privacy right provisions similar to the CCPA California will be enforcing. Several states such as Nevada are in the process of provisioning access rights to residents. If passed, some of these state laws would allow consumers to request access to their personal information that "Operators" may process, thereby, allowing consumers to know who may collect PI, while also providing the consumer with some means of choice with their information. *See* Jeewon Serrato & Susan Ross, *Nevada, New York and Other States Follow California's CCPA*, DATA PROTECTION REPORT BLOG (June 6, 2019), www.dataprotectionreport.com/2019/06/nevada-new-york-and-other-states-follow-californias-ccpa/; *see also* Michelle Noordyke, *US State Comprehensive Privacy Law Comparison*, INT'L. ASS'N. OF PRIVACY PROF. (Aug. 15, 2019), iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/.

protections for U.S. citizens to have a choice or any control over their personal information.

Additionally, companies do not offer reasonable notice or choice in privacy disclosures that adequately inform their consumers about their information-sharing practices. This article has identified these problems in legislation, multiparty involvement, privacy harms, disclosure formatting, and policy language that is inaccessible to the reasonable understanding of the average consumer. The current U.S. approach to privacy information remains ineffective in providing the consumer with appropriate levels of protections or choice of who can collect their personal information and how it will be used. Consumers continue to lack virtually any kind of real control over their collection of their information.

As a result of this lack of control, consumers face subjective and objective privacy harms with very few options for legal recourse. Consumers willingly surrender their privacy to third parties with insufficient information regarding who receives their personal data and for what purposes it is used. Companies continue to blanket third-party involvement with opt-in/opt-out options and excessive policy lengths that render consumer notice impossible to reasonably understand. With respect to third-party disclosures, legislation is too loosely regulated and will need to be remedied before any kind of adequate notice and choice can be presented to the consumer.

Technological tools and legislative remedies offer options and the possibility for reasonable notice and choice in the app environment, however, until government makes the effort to enact effective information privacy laws current to the digital information age, these potential solutions will only remain useful suggestions. The right to privacy will only continue to erode as information technology becomes progressively more advanced. The traditional approach to information-sharing practices has been proven to be ineffective and will remain so until legislation is current and flexible with technological capabilities, resembling the GDPR directive. An unorthodox approach to consumer protection and collective legislation flexible with technological advancements of permissions will need to be adopted globally if consumers have any hope of controlling their information. Until that change is actively pursued, the disparity of consumer's personal information lays unbound by the unrestricted spread of multiparty collection in the mobile environment.