NORTH CAROLINA JOURNAL OF LAW & TECHNOLOGY
15 N.C. J.L. & TECH. ON. 240 (2014)

MOBILE APP PRIVACY: DEVELOPING STANDARD AND EFFECTIVE PRIVACY TOOLS FOR CONSUMERS

Daniel Parisi*

Everyone knows what "apps" are (or they will know soon). Apps fill our smartphones, tablets, and computers; apps will fill our cars and control our homes. Apps of all varieties have been downloaded billions of times by sophisticated technologists and grandparents alike. These apps are collecting and sharing data in previously unimaginable ways. Developing standard and effective privacy tools for apps is essential to protect consumers and to encourage the growth of a transparent and trusted app industry. The National Telecommunications and Information Administration, the Federal Trade Commission, and Congress have all proposed guidelines and rules, but have fallen short of creating standard and effective privacy tools. This Recent Development will examine privacy tools and mobile app privacy regulatory efforts, and recommend changes that are needed to protect consumer data privacy.

I. INTRODUCTION

Not long ago, the word "app" was merely a technical term, short for an application program such as a word processing or spreadsheet application.[1] With the explosion of smartphones and tablets, the word "app" has become a cultural term[2] for the bite-sized, software applications that are readily downloadable to

* J.D. Candidate, University of North Carolina School of Law, 2015.

[1] *See, e.g.*, *App (noun)*, ONLINE ETYMOLOGY DICTIONARY, http://etymonline.com/index.php?term=app (last visited Mar. 23, 2014).

[2] The American Dialect Society named "app" to be the word of the year for 2010. *"App" Voted 2010 Word of the Year by the American Dialect Society (UPDATED)*, AMERICAN DIALECT SOCIETY (Jan. 8, 2011), http://www.americandialect.org/app-voted-2010-word-of-the-year-by-the-american-dialect-society-updated.

phones, tablets, and other devices.[3] These apps are used to find local restaurants, view location-aware maps, watch videos, and play games, among countless other functions.[4]

The Apple App Store, Google Play, and Windows Store all host hundreds of thousands of apps for instant download.[5] Most apps are free or cost less than a dollar.[6] In 2012, the average mobile phone subscriber had installed forty-one apps.[7] Consumers further download and discard apps on a monthly basis.[8] Considering the fast food nature of apps and the sheer number of apps used by the average app consumer, it is not surprising that consumers do not wish to invest a disproportionate amount of time figuring out the privacy implications of downloading each individual application by reading through a labyrinth of privacy policy legalese.[9] Yet, these applications can collect sensitive data

---

[3] *See, e.g.*, *App (noun)*, DICTIONARY.COM, http://dictionary.reference.com/browse/app (last visited Mar. 23, 2014).

[4] *See* Collection of Mobile App Reviews, PC MAG, http://www.pcmag.com/reviews/mobile-apps (last visited Mar. 23, 2014) (reviewing a wide variety of more than one thousand apps).

[5] Apps have been downloaded over 50 billion times from the Apple App Store alone. *Cumulative Number of Apps Downloaded from the Apple App Store from June 2008 to October 2013*, STATISTA, http://www.statista.com/statistics/263794/number-of-downloads-from-the-apple-app-store/ (last visited Mar. 23, 2014).

[6] Mary Ellen Gordon, *The History of App Pricing, and Why Most Apps Are Free*, FLURRY (July 18, 2013), http://blog.flurry.com/bid/99013/The-History-of-App-Pricing-AndWhy-Most-Apps-Are-Free. As of April 2013, the average Android app cost six cents, the average iPhone app cost nineteen cents, and the average iPad app cost fifty cents. *Id.*

[7] *State of the Appnation—A Year of Change and Growth in U.S. Smartphones*, NIELSEN (May 16, 2012), http://www.nielsen.com/us/en/newswire/2012/state-of-the-appnation-%C3%A2%C2%80%C2%93-a-year-of-change-and-growth-in-u-s-smartphones.html.

[8] *See Average App Download per Month*, MODUS OPERANDI, http://www.mobimatter.com/average-app-download-per-month/ (last visited Mar. 23, 2014) (charting the average number of app downloads per month by device type).

[9] *See* SHANNON WHEATMAN & MICHELLE GHISELLI, KINSELLA MEDIA, PRIVACY POLICIES: HOW TO EFFECTIVELY COMMUNICATE WITH CONSUMERS AND AVOID JUDICIAL AND REGULATORY SCRUTINY (2012), *available at* http://www.kinsellamedia.com/privacypolicies.pdf (demonstrating that privacy

such as a user's location, device identification, pictures, contacts, calendar, search terms, emails, and files, and can access a device's camera and microphone as well.[10] Additionally, each platform and app has its own privacy settings, and these settings frequently change. This lack of usability poses significant privacy problems for all users.

Because apps collect private data, a lack of consumer awareness is also a problem.[11] Consumers are surprised that their favorite and most trusted apps collect and share their data.[12] Toss It,[13] Angry Birds,[14] and Dictionary.com[15] have all been found to

---

policies are not written in plain language and take an average of seven minutes to read compared to an average website visit of forty-two seconds).

[10] *See Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books*, FED. TRADE COMM'N (Feb. 1, 2013), http://www.ftc.gov/news-events/press-releases/2013/02/path-social-networking-app-settles-ftc-charges-it-deceived (demonstrating the collection of personal information from mobile address books); Brian X. Chen & Nick Bilton, *Et Tu, Google? Android Apps Can Also Secretly Copy Photos*, N.Y. TIMES: BITS (Mar. 1, 2012, 1:08 PM), http://bits.blogs.nytimes.com/2012/03/01/android-photos/?_php=true&_type=blogs&r=0 (explaining how photos on a mobile phone can be collected).

[11] FED. TRADE COMM'N, MOBILE PRIVACY DISCLOSURES 10 (2013), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-privacy-disclosures-building-trust-through-transparency-federal-trade-commission-staff-report/130201mobileprivacyreport.pdf [hereinafter FTC MOBILE PRIVACY DISCLOSURES REPORT]. Consumers often do not know about or understand mobile data collection and sharing practices and, therefore, do not look for privacy options to control data collection and sharing. *Id.* When consumers do learn about data collection and sharing practices, they are often surprised and view the practices as "underhanded." *Id.*

[12] *See Apps Ratting You Out?*, CARNEGIE MELLON UNIV., http://www.cmu.edu/homepage/society/2013/spring/apps-ratting-you-out.shtml (last visited Mar. 23, 2014). Researchers at Carnegie Mellon University analyzed the top 100 apps for Android mobile devices and found that "most users were surprised to find the Pandora radio app accessing their contact lists . . . and Horoscope using their location information." *Id.*

[13] *See* Jason Hong, *Analysis of Toss It for Android*, JASON HONG'S CONFABULATIONS (Nov. 30, 2012, 12:09 AM), http://confabulator.blogspot.com/2012/11/analysis-of-toss-it-for-android.html (showing the percentage of people who were surprised by the data collection and sharing practices of the

collect and share data. The full extent of app data collection and sharing is the subject of much research and debate.[16] Even the simplest apps collect data. The Brightest Flashlight Free app was one of the most popular apps for Android mobile devices.[17] The app essentially turns the lights on a smartphone on and off to transform a smartphone into a handy flashlight.[18] The Federal Trade Commission ("FTC") determined that the app collected user location information and unique device IDs, and transmitted this data to advertising networks and other third-parties.[19] When even the simplest apps share user data in often surprising and sometimes underhanded ways, standard and effective privacy tools are needed to protect user privacy.

The app industry's data collection and sharing practices risk more than dignitary harm to consumers. With an average of forty-

---

popular Toss It app). The Toss It app allows a user to toss a digital crumpled ball of paper into a wastebasket. *Id.*

[14] *See* Jason Hong, *Analysis of Angry Birds for Android*, JASON HONG'S CONFABULATIONS (Nov. 29, 2012, 11:30 PM), http://confabulator.blogspot.com/2012/11/analysis-of-angry-birds-for-android.html. The Angry Birds app allows a user to take control of angry birds as they take revenge on the greedy pigs who stole their eggs. *Id.*

[15] *See* Jason Hong, *Analysis of Dictionary.com for Android*, JASON HONG'S CONFABULATIONS (Nov. 30, 2012, 12:05 AM), http://confabulator.blogspot.com/2012/11/analysis-of-dictionarycom-for-android.html. The Dictionary.com app allows a user to look up the definition of a word in a digital dictionary. *Id.*

[16] *See generally* APPTHORITY, APP REPUTATION REPORT 2–11 (2013), *available at* https://www.appthority.com/app-reputation-report/report/APPReputationReport072713.pdf (discussing research on risky app behavior); Brian Prince, *Google Android Vs. Apple iOS: The Mobile App Privacy War*, SECURITY: DARK READING (July 8, 2013), http://www.darkreading.com/privacy/google-android-vs-apple-ios-the-mobile-a/240157894 (discussing research by Bitdefender using its Clueful app).

[17] *Android Flashlight App Developer Settles FTC Charges It Deceived Customers*, FED. TRADE COMM'N (Dec. 5, 2013), http://www.ftc.gov/news-events/press-releases/2013/12/android-flashlight-app-developer-settles-ftc-charges-it-deceived.

[18] Complaint at 1, Goldenshores Techs., LLC, File No. 132-3087, 2013 WL 6512819 (F.T.C. Dec. 5, 2013), *available at* http://www.ftc.gov/sites/default/files/documents/cases/131205goldenshorescmpt.pdf.

[19] *Id.* at 3–4.

one apps installed per mobile app device,[20] and with even the simplest apps collecting and sharing personal information, each app represents a potential source of economic and emotional harm from a data security breach leading to identity theft. Having already collected and aggregated the personal information of consumers, app businesses are tantalizing targets for identity thieves.[21] In December 2013, a national retailer, Target, announced that the company had a data security breach affecting an estimated 70 to 110 million consumers.[22] The data stolen included payment data, names, phone numbers, home addresses, and email addresses.[23] Target was the source of a data security breach this time; tomorrow, you may receive a data security breach notification letter from your favorite and most trusted app, informing you that your name, home address, email address, financial information, or health information has been stolen.[24] The list of personal information at risk is only limited by the types of data that a particular app collects.

Identity theft causes victims to experience "financial, credit, and relationship problems and severe emotional distress."[25] Moreover, the question of whether any individual will be the

---

[20] *State of the Appnation*, *supra* note 7.

[21] J. Craig Anderson, *Identity Theft Growing, Costly to Victims*, USA TODAY (Apr. 14, 2013, 4:38 PM), http://www.usatoday.com/story/money/personalfinance/2013/04/14/identity-theft-growing/2082179/. "The most successful identity thieves have learned that it's more lucrative to hack into businesses, where they can steal card numbers [or personal information] by the thousands or even millions." *Id.*

[22] Elizabeth A. Harris & Nicole Perlroth, *For Target, the Breach Numbers Grow*, N.Y. TIMES (Jan. 10, 2014), http://www.nytimes.com/2014/01/11/business/target-breach-affected-70-million-customers.html.

[23] *Id.*

[24] *See* Ariana Tobin, *"We're Sorry You Got Hacked": Target's Letter to Unlucky Shoppers*, MARKETPLACE (Jan. 16, 2014, 11:34 AM), http://www.marketplace.org/topics/business/numbers/were-sorry-you-got-hacked-targets-letter-unlucky-shoppers (providing the text of the data breach notification letter sent to Target customers).

[25] ERIKA HARRELL & LYNN LANGTON, BUREAU OF JUSTICE STATISTICS, U.S. DEPT. OF JUSTICE, VICTIMS OF IDENTITY THEFT, 2012 1 (2013), *available at* http://www.bjs.gov/content/pub/pdf/vit12.pdf.

victim of identity theft is not a question of if, but when.[26] In 2012, more than sixteen million people in the United States, or seven percent of all U.S. residents age sixteen or older, were victims of identity theft in a single year.[27] Identity thieves can use stolen personal information to file fraudulent tax returns, open credit card accounts, and apply for mortgages.[28] Identity theft can result in massive debts, ruined credit scores, bankruptcy, and eviction from homes.[29] Harm is also done in less drastic cases. As an identity theft victim, Kellie Droste's personal information was stolen and used to file a fraudulent tax return.[30] As a result, she could not file her true tax return.[31] She reported the fraud to the proper tax authority, but was told that "it would take at least six months to sort out the matter."[32] Because of the identity theft, Kellie had to manage her finances without her $2,700 tax refund for a significant length of time.[33] Safe and effective privacy tools can play an important role in limiting app data as a source of identity theft.

This Recent Development will focus on mobile app privacy guidelines and rules; legislation at the federal level in the United States; and the development of standard and effective privacy tools. Part II provides background on the rapidly changing landscape of app privacy regulation, and a primer on existing and emerging privacy tools. Part III provides an introduction to the three development paths for privacy tools at the federal level. Part IV examines the progress, and ultimately, the shortcomings found along each development path. Part V discusses the need for new app privacy legislation and suggests ideas for new and improved privacy tools. Already behind, it is unclear if the law can keep pace with technology.

---

[26] Anderson, *supra* note 21 ("Security analysts say everyone should prepare to be a victim at some point.").
[27] HARRELL & LANGTON, *supra* note 25, at 1.
[28] Anderson, *supra* note 21.
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*

II. THE RAPIDLY CHANGING LANDSCAPE OF APP PRIVACY REGULATION

Regulating mobile app privacy and data collection has proven to be a challenge. Apps are a new technological innovation full of uncertainty and change,[34] and are already an important part of the economy.[35] Businesses seek growth by offering new and innovative app services.[36] The app industries of the United States and the European Union are each estimated to be $23 billion in size, and the European app market is forecast to grow to $86 billion in the next five years, with similar results expected in the United States.[37] "[T]he App Economy now [in 2012] is responsible

---

[34] Mobile apps have moved beyond smartphones, tablets, laptops, and desktops. Apps are used on car consoles and to control home appliances too. Natasha Baker, *'Internet of Things' Is Growing, Starting with Your Washer*, MSN NEWS (Apr. 22, 2013), http://news.msn.com/science-technology/internet-of-things-is-growing-starting-with-your-washer; *see also* Darrell Etherington, *Apple's New CarPlay System Will Turn Tens of Millions of Cars into iPhone Accessories*, TECH CRUNCH (Mar. 3, 2104), http://techcrunch.com/2014/03/03/apples-new-carplay-system-will-turn-tens-of-millions-of-cars-into-iphone-accessories/ (announcing Apple's new CarPlay service for car information systems). Samsung already sells smart, app-controlled washers and dryers. *See* Natt Garun, *Demoing the App-Controlled Samsung Smart Washer and Dryer*, DIGITAL TRENDS (Aug. 3, 2012), http://www.digitaltrends.com/mobile/demoing-the-app-controlled-samsung-smart-washer-and-dryer/ (describing some of the features and benefits of app-controlled washers and dryers); *see also Samsung Smart Appliances*, SAMSUNG, http://www.samsung.com/us/smartappliances/ (last visited Mar. 23, 2014) (providing screenshots and demos of the apps used to control appliances).

[35] Haydn Shaughnessy, *Fast Growing Opportunity in Europe's $86 Billion App Economy*, FORBES (Feb. 13, 2014, 7:53 AM), http://www.forbes.com/sites/haydnshaughnessy/2014/02/13/the-86-billion-opportunity-in-apps/.

[36] Eilene Zimmerman, *Even Small Players Can Seize the Day with an App Strategy*, N.Y. TIMES (Oct. 10, 2012), http://www.nytimes.com/2012/10/11/business/smallbusiness/small-companies-seek-to-push-sales-and-marketing-with-own-apps.html?_r=0.

[37] Shaughnessy, *supra* note 35; *see also* Matt Hamblen, *App Economy Expected to Double by 2017 to $151B*, COMPUTER WORLD (July 15, 2013, 11:41 AM), https://www.computerworld.com/s/article/9240794/App_economy_expected_to_double_by_2017_to_151B (predicting rapid growth in the size of the U.S. app economy).

for roughly 466,000 jobs in the United States, up from zero in 2007. . . ."[38] Businesses also make profits from selling app data to data brokers.[39] Unfortunately, these new business opportunities have often come at the cost of consumer data privacy. Surveys show that individuals are concerned about their privacy online, and having their personal information sold to amorphous third-parties without notice of how their personal information will be used.[40] So far, these concerns have been largely outweighed by the desire of consumers to enjoy the benefits and convenience of apps at their fingertips.[41] However, a new report on consumer trust warns the app industry against complacency, citing a lack of trust as "the number one barrier to the growth of mobile content and commerce."[42]

---

[38] MICHAEL MANDEL, TECHNET, WHERE THE JOBS ARE: THE APP ECONOMY 1 (2012), *available at* http://www.technet.org/wp-content/uploads/2012/02/TechNet-App-Economy-Jobs-Study.pdf.

[39] Katy Bachman, *Big Data Added $156 Billion in Revenue to Economy Last Year [Updated]*, AD WEEK (Oct. 14, 2013, 9:17 AM), http://www.adweek.com/news/technology/big-data-added-156-billion-revenue-economy-last-year-153107.

[40] Sophie Curtis, *Three Quarters of Consumers Concerned About Privacy Online*, CIO (June 25, 2013), http://www.cio.com/article/735431/Three_Quarters_of_Consumers_Concerned_About_Privacy_Online; *see also* Kristina Knight, *TRUSTe: Most People Concerned About Online Privacy*, BIZREPORT (Sept. 19, 2013), http://www.bizreport.com/2013/09/truste-most-people-concerned-about-online-privacy.html ("Two in three [consumers] say they 'have concerns' about how their personal information is used and how their online actions and purchases are tracked.").

[41] The number, variety, and time spent using apps all continue to grow rapidly. *See, e.g.*, *State of the Appnation—A Year of Change and Growth in U.S. Smartphones*, *supra* note 7; David Murphy, *Social Apps Gaining Popularity, Mobile Games Reaching Saturation*, PC MAG (Apr. 28, 2012, 5:25 PM), http://www.pcmag.com/article2/0,2817,2403715,00.asp; Jasmine Pennic, *Infographic: The Rising Popularity of Mobile Health & mHealth Apps*, HIT CONSULTANT, http://www.hitconsultant.net/2013/08/21/infographic-the-rising-popularity-of-mobile-health-mhealth-apps/ (last visited Mar. 23, 2014).

[42] *MEF Report Warns Against Complacency on Consumer Trust*, MEF (Feb. 20, 2014), http://www.mefmobile.org/News/mef-news/237/mef-report-warns-against-complacency-on-consumer-trust.

There are three separate federal-level development paths for privacy tools: the National Telecommunications and Information Administration ("NTIA"), the FTC, and Congress. Before discussing these three paths, a primer on privacy tools will establish the foundation for later assessing each path and the need for new privacy legislation.

A. *Existing and Emerging Privacy Tools Leading Towards the Development of Standard and Effective Privacy Tools*

Two basic, and frequently used, privacy tools are icons and badges.[43] Privacy icons appear during personal data transmission to let the user know that such transmission is occurring (e.g. an arrow appears in the upper-right-corner of a device's screen during the transmission of location information).[44] Both Apple and Google devices use icons to indicate when a user's location is being accessed.[45] Trade associations have developed privacy badges that are used in app advertisements or in the apps themselves to indicate app features such as "No Ads" or "Has In-App Purchases."[46] The "No Ads" badge indicates that an app does not use advertising within the app.[47] The "Has In-App Purchases" badge indicates that additional purchases for app features, beyond paying for the app itself, may be made through the app after install.[48]

Privacy policy generators are tools that help app developers create privacy policies.[49] Through a privacy policy generator website, developers answer a number of questions describing their data collection practices such as: what personal information is collected, who has access to the personal information, and what

---

[43] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 17–18, 25–26.
[44] *Id.* at 17–18.
[45] *Id.*
[46] *Id.* at 26.
[47] *Id.*
[48] *Id.*
[49] *Id.* at 27.

security measures are used to protect the personal information.[50] Using the answers given, the software-based generator creates a privacy policy for the app developer.[51] However, app developers must be careful when using privacy policy generators because the misuse of privacy policy generators can lead to legal liability, rather than legal protection.[52] The deceptive simplicity of a privacy policy generator may lead an app developer to forgo the hard work and expense of performing a proper information-handling-practices audit or hiring an attorney to create an adequate privacy policy.[53] If a company decides to risk using a privacy policy generator, the company should know that some privacy policy generators are more sophisticated than others.[54] Data collection and sharing practices often involve complex business transactions and relationships, and improper disclosure can lead to enforcement action by the FTC, if a promise is made, but not kept.[55] Privacy policy generators at least help some app developers to provide privacy policies, who otherwise would not. More importantly,

---

[50] *Id.*

[51] *Id.*

[52] *See* Keith P. Enright, *Privacy Audit Checklist*, BERKMAN CTR. FOR INTERNET AND SOC'Y AT HARVARD UNIV., https://cyber.law.harvard.edu/ecommerce/privacyaudit.html (last visited Mar. 23, 2014) (warning that an improper assessment of a company's information handling practices can lead to legal liability rather than legal protection).

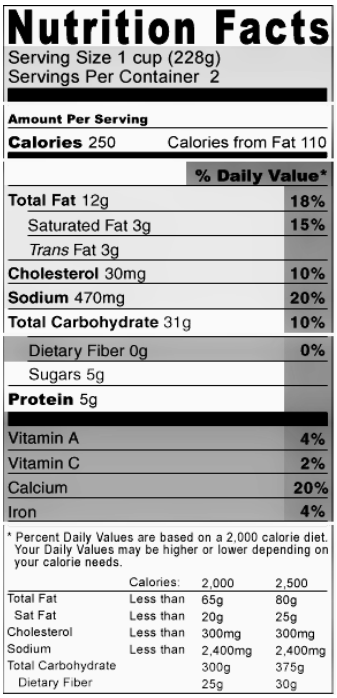
[53] *Id.*; *see also* Vangie Beal, *Ecommerce Content: Writing a Good Privacy Policy*, IT BUSINESS EDGE (May 5, 2010), http://www.ecommerce-guide.com/article.php/3880376/Ecommerce-Content--Writing-a-Good-Privacy-Policy.htm (offering advice to companies choosing the do-it-yourself route to creating a privacy policy).

[54] *Compare Get a Privacy Policy for Your Mobile App: It's Simple, Fast, and Free*, TRUSTE, http://www.truste.com/free-mobile-privacy-policy/ (last visited Mar. 23, 2014), *with Privacy Policy Generator*, FREEPRIVACYPOLICY.ORG, http://www.freeprivacypolicy.org/generator.php (last visited Mar. 23, 2014) (showing that some privacy policy generators are more sophisticated than others).

[55] *FTC Settlement Puts an End to "History Sniffing" by Online Advertising Network Charged with Deceptively Gathering Data on Consumers*, FED. TRADE COMM'N (Dec. 5, 2012), http://www.ftc.gov/news-events/press-releases/2012/12/ftc-settlement-puts-end-history-sniffing-online-advertising.

privacy policy generators would work especially well for creating mandatory, standard privacy "nutrition labels."

Figure 1: Sample Nutrition Facts Label from the U.S. Food and Drug Administration



Nutrition Facts

Serving Size 1 cup (228g)
Servings Per Container 2

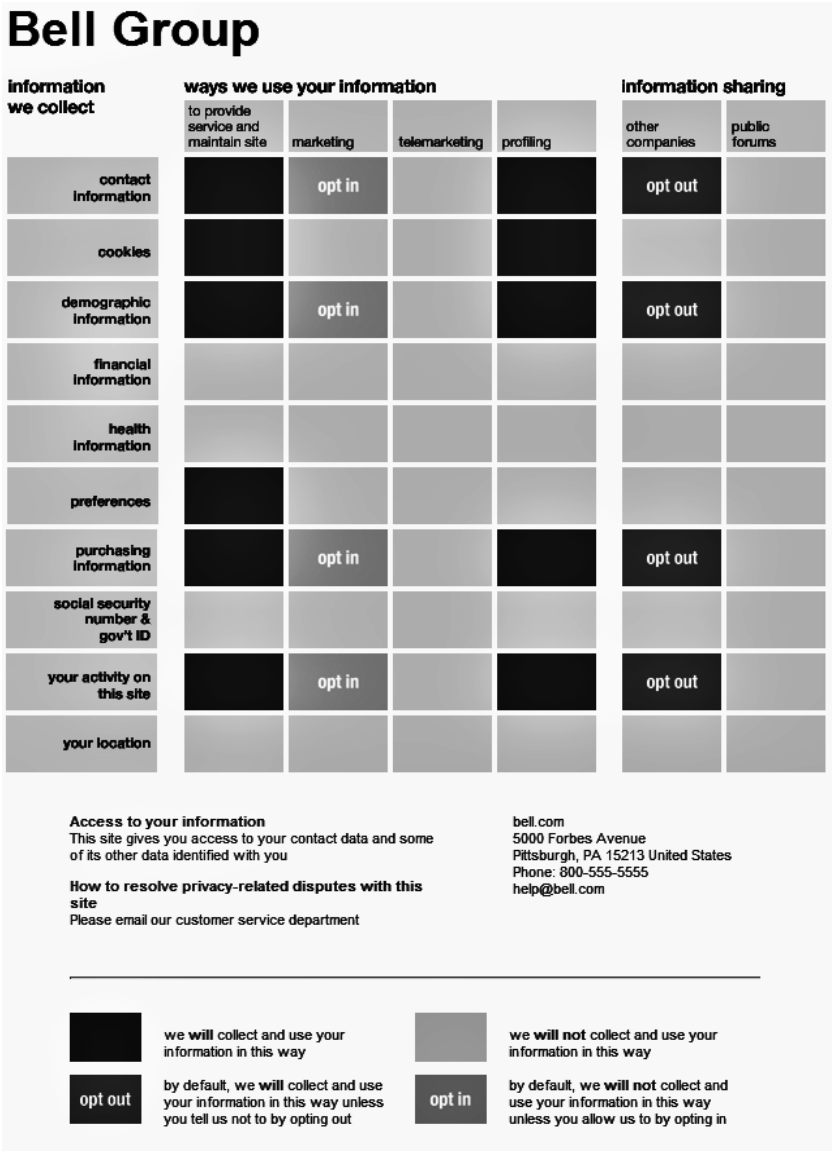
Amount Per Serving	
Calories 250	Calories from Fat 110
	% Daily Value*
Total Fat 12g	**18%**
Saturated Fat 3g	**15%**
Trans Fat 3g	
Cholesterol 30mg	**10%**
Sodium 470mg	**20%**
Total Carbohydrate 31g	**10%**
Dietary Fiber 0g	**0%**
Sugars 5g	
Protein 5g	
Vitamin A	**4%**
Vitamin C	**2%**
Calcium	**20%**
Iron	**4%**

* Percent Daily Values are based on a 2,000 calorie diet. Your Daily Values may be higher or lower depending on your calorie needs.

	Calories:	2,000	2,500
Total Fat	Less than	65g	80g
Sat Fat	Less than	20g	25g
Cholesterol	Less than	300mg	300mg
Sodium	Less than	2,400mg	2,400mg
Total Carbohydrate		300g	375g
Dietary Fiber		25g	30g

Source: http://www.fda.gov

Figure 2: Sample Privacy Nutrition Label Developed by the CyLab Usable Privacy and Security Laboratory at Carnegie Mellon University



Source: http://cups.cs.cmu.edu

Privacy nutrition labels are additional privacy tools that function much like the nutrition labels on packaged foods at the grocery store.[56] A food nutrition facts label lists the amount of calories, total fat, cholesterol, sodium, and total carbohydrates that a packaged food contains per serving in a standard table format.[57] Analogously, a privacy nutrition label lists standard types of personal information and how they are used and shared, in a standard grid format, providing for quick and easy review by the consumer.[58] Carnegie Mellon University's CyLab ("CyLab") has done extensive research on privacy nutrition labels over many years.[59] They have created a highly effective privacy nutrition label format; research has shown that consumers find CyLab's privacy nutrition label format to be easy to use and understand.[60]

CyLab developed the privacy nutrition label by using an iterative design process and drawing upon lessons learned from other labeling systems.[61] Rather than using a table format, a privacy nutrition label uses a grid format.[62] On the vertical axis and to the left side of the grid, the label lists categories of data collection such as location, contacts, and photos with one category per line.[63] Across the top of the grid and on the horizontal axis, the label (1) lists categories of data uses, such as marketing,

---

[56] PATRICK GAGE KELLEY ET AL., CARNEGIE MELLON UNIV. CYLAB, A "NUTRITION LABEL" FOR PRIVACY §§ 2.1, 3.4 (2009), *available at* http://cups.cs.cmu.edu/soups/2009/proceedings/a4-kelley.pdf (researching the effectiveness of a privacy nutrition label based in part on the design of a traditional food nutrition label).

[57] *How to Understand and Use the Nutrition Facts Label*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/Food/IngredientsPackagingLabeling/LabelingNutrition/ucm274593.htm (last visited Mar. 23, 2014).

[58] *See Bell Group*, CARNEGIE MELLON UNIV. CYLAB, http://cups.cs.cmu.edu/privacylabel-05-2009/current/1.php (last visited Mar. 23, 2014) (providing a newer version of the privacy nutrition label from the Kelley et al. study); *see also* KELLEY ET AL., *supra* note 56, fig.5 (original privacy nutrition label).

[59] *Privacy Nutrition Labels*, CARNEGIE MELLON UNIV. CYLAB, http://cups.cs.cmu.edu/privacyLabel/ (last visited Mar. 23, 2014).

[60] KELLEY ET AL., *supra* note 56, § 6.

[61] *Id.* § 3.

[62] *Bell Group*, *supra* note 58.

[63] *Id.*

telemarketing, and profiling; and then (2) lists categories of data sharing, such as other companies and public forums.[64] Each square of the grid represents the cross-section of a single data type and a single data use.[65] Different colors indicate whether a grid square is affirmatively selected or not.[66] CyLab's research has shown that privacy nutrition labels are more comprehensible and easier to use than natural language privacy policies.[67] In a CyLab study, participants who read privacy nutrition labels found privacy information more quickly and accurately and enjoyed the experience more, compared to the participants who read natural language privacy policies.[68] The National Science Foundation recently awarded a grant to a team led by Carnegie Mellon University researchers to continue research on privacy nutrition labels.[69]

Lastly, privacy dashboards are privacy tools that serve as centralized points of privacy management.[70] When driving a car, a

---

[64] *Id.*

[65] *Id.*

[66] *Id.* Opt-in and opt-out options are also disclosed by superimposing text on a colored square and altering the shade of the color. *Id.*

[67] KELLEY ET AL., *supra* note 56, § 6.

[68] *Id.*

[69] Sam Pfeifle, *A Look at the Future of Privacy Notices (If They Have a Future)*, INT'L ASS'N OF PRIVACY PROF'LS (Sept. 4, 2013), https://www.privacyassociation.org/publications/a_look_at_the_future_of_privacy_notices_if_they_have_a_future. The National Science Foundation's Web Privacy Notice Project's lead investigator explains the need for better privacy notices:

> [T]here's been a rush to the bottom in terms of privacy practices, and the idea of self-regulation and that people would start competing on privacy policies, well, that was wishful thinking and that remains wishful thinking. But if one day you can instill all this information so that it's much easier for a user to digest, then maybe you find yourself with [competition on privacy policies] actually happening.

Id. (quoting Norman Sadeh, the lead investigator for the National Science Foundation's Web Privacy Notice Project, and a professor at Carnegie Mellon University).

[70] *See* FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 16–17 (discussing dashboards and the different approaches taken by Apple and Google).

driver can view and access the car's notices and controls through the car's dashboard located directly in front of the driver. Car notices include the car's speed, oil pressure, and the engine check light. Car controls include the defroster switch and the radio volume dial. These notices and controls are simple so that the driver may use these notices and controls while safely operating the vehicle. These car tools are standard and effective. Privacy dashboards have not reached this level of standardization and effectiveness, but technology companies have made progress in applying the car dashboard concept to privacy tools.[71] Privacy dashboards exist both for online data and for managing apps on devices.[72] For example, Microsoft's dashboard for its online services allows a user to access and modify a personal profile including name, gender, birthday, and contact information.[73] Microsoft's dashboard also allows a user to disable personalized ads.[74] Similarly, Apple offers a privacy dashboard for managing apps on an Apple device.[75] In Apple's iOS 7, under "Settings" and then "Privacy," Apple lists data categories such as contacts, calendars, photos, and microphone.[76] Under each data category, Apple then lists each app that has requested access to that type of data and offers a "per app" option to disable access to that data.[77] Although dashboards promise centralized access to privacy settings and ease of use, current dashboards offer only limited

---

[71] *See Personal Data Dashboard*, MICROSOFT, http://www.microsoft.com/security/online-privacy/personal-data-dashboard.aspx (last visited Mar. 23, 2014). Microsoft is developing a privacy dashboard for customers to manage some of the online data collected, shared, and stored by Microsoft. *Id.*

[72] *Id.* (discussing a dashboard for managing online data); FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 16–17 (discussing dashboards for managing apps).

[73] *Personal Data Dashboard*, *supra* note 71.

[74] *Id.*

[75] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 16–17.

[76] *See iPhone User Guide: For iOS 7*, APPLE, 35–36 (Oct. 2013), http://manuals.info.apple.com/MANUALS/1000/MA1565/en_US/iphone_user_guide.pdf (explaining the privacy settings for Apple's iOS 7 operating system).

[77] *Id.*

centralized access and can be difficult to use.[78] Dashboards often use unfamiliar terms that must be researched to understand, such as the terms, "Compass Calibration" and "Popular Near Me," listed under "Location Services" and then "System Services" in Apple's iOS 7.[79] Consumers must find a link to an explanation of the terms or consult Apple's iOS 7 user guide. Yet consumers may not understand what functionality is gained or lost by turning these privacy settings on and off. The ease of use and understanding provided by dashboards is lost.[80]

B. *The International Association of Privacy Professionals Tool*

The International Association of Privacy Professionals ("IAPP") is a global association of privacy professionals and a valuable resource in the field of privacy law and policy.[81] IAPP has recently developed a tool to serve as a centralized resource for mobile app privacy guidelines from legal authorities, think tanks, and industry associations at the state, federal, and international levels.[82] The IAPP tool is an interactive tool that permits three layers of sorting through the many available privacy guidelines.[83] Guidelines are sorted by: (1) category—such as data collection, data retention, notice, and accountability; (2) audience—such as app developers, platform developers, ad networks, and mobile service providers; and (3) source—such as the FTC, the NTIA, the State of California, the European Union, the Future of Privacy

---

[78] *See* Andrew Couts, *Are Apple's iOS 7 Privacy Settings Purposefully Misleading, or Just a Mess?*, DIGITAL TRENDS (Sept. 29, 2013), http://www.digitaltrends.com/mobile/apple-your-ios-7-privacy-settings-are-a-mess/ (explaining the difficulty of using the privacy settings in Apple's iOS 7 operating system).

[79] *Id.*

[80] *Id.*

[81] *About the IAPP*, INT'L ASS'N OF PRIVACY PROF'LS, https://www.privacyassociation.org/about_iapp (last visited Mar. 23, 2014).

[82] *See Comparison of Mobile Application Guidelines*, INT'L ASS'N OF PRIVACY PROF'LS, https://www.privacyassociation.org/resource_center/comparison_of_mobile_application_guidelines (last visited Mar. 23, 2014) (providing an interactive web-based tool for examining mobile app privacy guidelines).

[83] *Id.*

Forum, and the Groupe Speciale Mobile Association ("GSMA").[84] The end result of a three-layer sort is a focused set of guidelines from a single source.[85] For example, an app developer seeking to learn about the mobile privacy principles regarding notice, as expressed by the GSMA, would (1) select the "Notice and Transparency" category first-layer tab; (2) select the "App Developers" audience second-layer tab; and (3) select the "GSMA Mobile Privacy Principles" source third-layer tab.[86] The app developer would be advised, according to the focused set of guidelines, to "[i]dentify yourself to users," specifying that "[u]sers must have easy access (via a link or menu item) to brief contact details of the organization."[87]

III. INTRODUCTION TO THE THREE FEDERAL-LEVEL DEVELOPMENT PATHS FOR PRIVACY TOOLS

There are three separate federal-level development paths for privacy tools: the NTIA, the FTC, and Congress. Each path will be introduced briefly in this section, with the necessary background to launch the discussion, and will be explored further in Part IV.

A. *The National Telecommunications and Information Administration Development Path*

The NTIA is an executive branch agency serving as the President's principal advisor on telecommunications policy with a focus on national economic and technological advancement.[88] The NTIA engages in policymaking and research on matters such as the

---

[84] *Id.*
[85] *Id.*
[86] *Id.*
[87] *Id.* (resulting from the following three-layer sort: (1) select the "Notice and Transparency" category first-layer tab; (2) select the "App Developers" audience second-layer tab; and (3) select the "GSMA Mobile Privacy Principles" source third-layer tab.)
[88] 47 U.S.C. § 902 (2012).

internet domain name system, broadband internet access, and the federal government's use of the wireless spectrum.[89]

In February 2012, the Obama Administration released *Consumer Data Privacy in a Networked World*,[90] a whitepaper that created a "multistakeholder process" to develop codes of conduct to regulate consumer data privacy as an alternative to traditional regulation.[91] The multistakeholder process brings private and public interest groups together to create voluntary agreements on privacy standards.[92] The White House designated the NTIA to be the facilitator of the process.[93] The stakeholders are a broad and open group of interested parties including technical experts, companies, trade groups, privacy advocates, academics, state Attorneys General, federal law enforcement representatives, and international partners.[94] Mobile industry stakeholders began

---

[89] *About NTIA*, NAT'L TELECOMMS. & INFO. ADMIN., http://www.ntia.doc.gov/about (last visited Mar. 23, 2014).

[90] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD, (2012), *available at* http://www.whitehouse.gov/sites/default/files/privacy-final.pdf [hereinafter WHITE HOUSE WHITEPAPER].

[91] *Id.* at 23–27 (describing the multistakeholder process).

[92] *Id.* As defined in the whitepaper, the three stages of the multistakeholder process are: (1) deliberation, (2) adoption, and (3) evolution. *Id.* at 26–27. First, during the deliberation stage, the NTIA enlists stakeholders and holds meetings. *Id.* The stakeholders themselves establish the operating procedures and processes. *Id.* The deliberation stage concludes with a draft code representing the non-binding agreement of the stakeholders. *Id.* Second, the adoption stage begins and continues indefinitely. *Id.* Companies can voluntarily adopt the code or they can choose not to. *Id.* at 27. The FTC, exercising its enforcement authority against unfair and deceptive business practices, can only enforce the code against companies that have voluntarily adopted the code. *Id.*; *see also* Federal Trade Commission (FTC) Act, 15 U.S.C. § 45 (2012) (establishing the FTC's enforcement authority against unfair and deceptive business practices). Third, the evolution stage allowing for revisions to the code of conduct can occur at any time. WHITE HOUSE WHITEPAPER, *supra* note 90, at 27. A revision process occurs when stakeholders decide that a code of conduct no longer provides effective consumer data privacy protections. *Id.* Adoption of a revised code of conduct is again voluntarily. *Id.*

[93] WHITE HOUSE WHITEPAPER, *supra* note 90, at 26.

[94] *Id.* at 23. The FTC may choose to be involved in the NTIA process and may offer its own suggestions during the stakeholder proceedings. *Id.* at 29–30.

meeting in July 2012[95] to develop a mobile app privacy code of conduct, and agreed to a code of conduct in July 2013.[96] The agreement ended the deliberation stage of the multistakeholder process and began the adoption stage.[97] Part IV.A–B focuses on the July 2013 NTIA Code of Conduct.

B. *The Federal Trade Commission Development Path*

Unlike the NTIA, the FTC is an independent agency[98] whose purpose is to prevent deceptive and unfair business practices, to enhance informed consumer choice, and to do so without unduly burdening legitimate business activity.[99] The FTC has been active in the regulation of mobile app privacy for many years.[100]

---

[95] *See Privacy Multistakeholder Process: Mobile Application Transparency*, NAT'L TELECOMMS. & INFO. ADMIN. (Nov. 12, 2013), http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-process-mobile-application-transparency (providing background information on the mobile app transparency multistakeholder process and many useful links).

[96] NAT'L TELECOMMS. & INFO. ADMIN. MULTISTAKEHOLDER PROCESS, SHORT FORM NOTICE CODE OF CONDUCT TO PROMOTE TRANSPARENCY IN MOBILE APP PRACTICES (2013), *available at* http://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf [hereinafter NTIA MOBILE APP NOTICE CODE OF CONDUCT] (as agreed to by the stakeholders on July 25, 2013, resulting in the end of deliberations on the code of conduct).

[97] *See supra* note 92 and accompanying text. On February 24, 2014, AVG Technologies announced that it plans to deploy short form privacy notices over the current year making the company among the first to adopt the code of conduct. *AVG Technologies Among the First to Debut Short Data Privacy Notice for Mobile Apps*, BLOOMBERG (Feb. 24, 2014), http://www.bloomberg.com/article/2014-02-24/arnc4Xcr5Vo0.html.

[98] Federal Trade Commission (FTC) Act, 15 U.S.C. § 41 (2012). The President's power to dismiss FTC Commissioners is limited and, therefore, presidential control of the FTC is limited. *Id.*

[99] *About the FTC: Our Mission*, FED. TRADE COMM'N, http://www.ftc.gov/about-ftc (last visited Mar. 23, 2014).

[100] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at i ("The [FTC] has worked on privacy issues for more than forty years, and in 2000 began considering the privacy implications raised by consumers' growing use of mobile devices."); *see also* FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE i (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privac

However, the FTC does not have the direct authority to regulate privacy tools.[101] Instead, the FTC releases guidelines to the mobile app industry and to app consumers in the form of policy reports, testimony, law enforcement actions, consumer education, and workshops.[102] In May 2012, the FTC held a workshop on mobile privacy disclosures and, in February 2013, released a post-workshop mobile privacy disclosures report.[103] Part IV.C–D focuses on this February 2013 FTC Mobile Privacy Disclosures Report and earlier FTC reports.

C. *The Congressional Development Path: The Application Privacy, Protection, and Security Act of 2013*

The Application Privacy, Protection, and Security Act of 2013 ("APPS Act")[104] was introduced in the House in May 2013.[105] If passed, the APPS Act will be the first federal statute mandating mobile privacy disclosures to all consumers.[106] While introducing

---

yreport.pdf (calling on companies to implement best practices to protect consumer privacy).

[101] The FTC brings actions against companies who make promises to consumers and who fail to uphold those promises under its Section 5 authority against unfair and deceptive business practices. 15 U.S.C. § 45 (2012).

[102] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 1.

[103] *See In Short: Advertising & Privacy Disclosures in a Digital World*, FED. TRADE COMM'N (May 30, 2012), http://www.ftc.gov/news-events/events-calendar/2012/05/short-advertising-privacy-disclosures-digital-world (describing the FTC workshop); FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11.

[104] H.R. 1913, 113th Cong. (2013).

[105] *See H.R.1913—APPS Act of 2013: Summary*, CONGRESS.GOV, http://beta.congress.gov/bill/113th-congress/house-bill/1913?q=%7B%22search%22%3A%5B%22the+apps+act%22%5D%7D (last visited Mar. 23, 2014) (tracking the APPS Act of 2013 since the bill's introduction in the House on May 9, 2013).

[106] H.R. 1913 § 2; *see also* Cara Buchanan, *The APPS Act: Mobile Privacy Concerns Before the NSA Scandal*, POLICY INTERNS (June 13, 2013), http://policyinterns.com/2013/06/13/the-apps-act-mobile-privacy-concerns-before-the-nsa-scandal/ (explaining that the APPS Act is needed to require app developers to provide privacy notices to users regarding the collection and sharing of personal information). The Children's Online Privacy Protection Act ("COPPA") already requires children-focused apps to notify parents of any data

the APPS Act, Rep. Hank Johnson explained that "we lack basic rights to control how and how much of our data is collected on our phones, iPads and tablets."[107] The APPS Act proposes substantive measures such as requiring notice, consent, and the withdrawal of consent for data collection and sharing, as well as procedural measures such as enforcement by the FTC and state Attorneys General.[108] The APPS Act grants the FTC the direct enforcement authority that it has lacked in its mobile app privacy enforcement efforts.[109] However, the APPS Act provides for a problematic safe harbor provision, in which a company could be shielded from liability by following a code of conduct developed through the NTIA multistakeholder process, even though the requirements of that code of conduct may fall far below the substantive requirements of the APPS Act.[110] Part IV.E–F focuses on the APPS Act.

IV. ANALYSIS OF THE THREE FEDERAL-LEVEL DEVELOPMENT PATHS FOR PRIVACY TOOLS

The NTIA, the FTC, and Congress have each made individual efforts to address mobile app privacy, and have proposed guidelines and rules. Each effort has made progress, but has also suffered from significant shortcomings. This section will examine each of these three efforts in turn.

A. *The NTIA Code of Conduct: Progress*

The NTIA code of conduct sets standards for "short form privacy notices" for mobile apps in contrast to the traditional long

---

collection and sharing of the personal information of children under the age of thirteen. 15 U.S.C. §§ 6501–6506 (2012).

[107] Buchanan, *supra* note 106 (quoting Rep. Hank Johnson, *Hank Introduces the APPS Act*, YOUTUBE (May 9, 2013), https://www.youtube.com/watch?v=4l7DSwlAeM4).

[108] H.R. 1913 §§ 2–3.

[109] *Id.* § 3.

[110] *Id.* § 5.

form privacy policy notices often found on websites.[111] The code makes progress by establishing standard categories of data collection and sharing.[112] Data collection categories include (1) "Biometrics (information about your body, including fingerprints, facial recognition, signatures and/or voice print);" (2) "Browser History (a list of websites visited);" and (3) "Location (precise past or current location or where user has gone)."[113] Data sharing categories include (1) "Ad Networks (companies that display ads to you through apps);" (2) "Consumer Data Resellers (companies that sell consumer information to other companies for multiple purposes including offering products and services that

[111] NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 1. In general, no federal law requires websites to have privacy policies. However, the Children's Online Privacy Protection Act (COPPA) is the exception. 15 U.S.C. §§ 6501–6506 (2012). Regulations under COPPA require websites that collect personal information from children under the age of thirteen to post privacy policies. Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013). Only a single state, California, requires websites to have a privacy policy, although certain condition must be met. California's Online Privacy Protection Act (CalOPPA), CAL. BUS. & PROF. CODE § 22575 (West 2014). "An operator of a commercial Web site or online service that collects personally identifiable information" from California residents must post a privacy policy. *Id.* The privacy policy must "[i]dentify the categories of personally identifiable information that the operator collects . . . and the categories of third-party persons or entities with whom the operator may share the personally identifiable information." *Id.* Any process maintained to allow customers to access their collected personal data must be described. *Id.* The policy must also describe how customers are notified of revisions to the privacy policy and must list the policy's effective date. *Id.* Personally identifiable information ("PII") is defined as "individually identifiable information about an individual consumer collected online by the operator from that individual and maintained by the operator in an accessible form" and includes an individual's name, address, email address, telephone number, social security number, and "any other identifier that permits the physical or online contacting of a specific individual." *Id.* § 22577.

[112] NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 2–3. The data collection categories include: biometrics, browser history, phone/text log, contacts, financial info, health/medical/therapy, location, and user files. *Id.* The data sharing categories include: ad networks, carriers, consumer data resellers, data analytics providers, government entities, operating systems and platforms, other apps, and social networks. *Id.* at 3.

[113] *Id.* at 2.

may interest you);" and (3) "Social Networks (companies that connect individuals around common interests and facilitate sharing)."[114] Using standard categories for notices will lead to improved consumer understanding and awareness, and to a reduction in consumer surprise regarding how consumer data is collected and shared. "Surprise minimization" is one of the key goals of privacy notices and controls because consumer surprise demonstrates a lack of effective notice and consent.[115]

B. *The NTIA Code of Conduct: Shortcomings*

The NTIA code of conduct falls short for four specific reasons. First, adoption of the code is voluntary,[116] which will reduce the number of companies that follow the code. A company that does not like a provision of the code, can choose not to adopt the code, and instead choose to unofficially implement the code without following the provision that it finds undesirable. However, deploying a privacy notice that may mislead consumers into believing that a company has adopted the code of conduct could be viewed by the FTC as a deceptive practice. Therefore, companies choosing not to adopt the code will likely create substantially dissimilar privacy notices, thereby, perpetuating the lack of uniformity in privacy notices. Because the code is voluntary, some companies will continue to provide no privacy notices at all.

Second, the code allows for too much variation in privacy notice interface design.[117] An interface is the graphical representation of a privacy notice and any functionality with which the user interacts.[118] Six sample interface designs were developed during the NTIA multistakeholder process as examples of how

---

[114] *Id.* at 3.

[115] CAL. OFFICE OF THE ATT'Y GEN., PRIVACY ON THE GO 5 (2013), *available at* http://oag.ca.gov/sites/all/files/pdfs/privacy/privacy_on_the_go.pdf.

[116] NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 1.

[117] *See id.* at 4–6 (establishing guidelines for short form privacy notice design).

[118] *See, e.g.*, *User Interface Definition*, DICTIONARY.COM, http://dictionary.reference.com/browse/user+interface (last visited Mar. 23, 2014).

companies may want to design privacy notices.[119] Five of the six sample interface designs are intentionally similar to demonstrate minor variations on a common theme.[120] However, the NTIA code of conduct allows for far greater flexibility in interface design.[121] For example, the code allows for the use of inconsistent icons for representing data categories and does not require the consistent use of text to explain each category.[122] The sixth sample interface design, created by the Association for Competitive Technology, demonstrates how varied these notices can be.[123] Consistency is important in interface design.[124] While some variety in app design is otherwise acceptable or even desirable between apps, privacy notices should be identical to facilitate quick understanding and easy side-by-side comparisons. Identical elements, such as icons, text, and layout, across user interfaces, indicate to a user that the

---

[119] *See* NAT'L TELECOMMS. & INFO. ADMIN. MULTISTAKEHOLDER PROCESS, NTIA MOBILE APP TRANSPARENCY—UI COMPOSITIONS (2013), *available at* http://www.ntia.doc.gov/files/ntia/publications/ntia_ui_comps_update_7.23.pdf [hereinafter NTIA UI COMPOSITIONS] (providing five of the six sample user interface compositions); *see also NTIA User Interface Mockups*, FUTURE OF PRIVACY FORUM, http://www.futureofprivacy.org/2013/07/25/ntia-user-interface-mockups/ (last visited Mar. 23, 2014) (providing a link to the sixth sample user interface, which was designed by the Association for Competitive Technology).

[120] *See* NTIA UI COMPOSITIONS, *supra* note 119. The five sample user interfaces are each labeled according to the variation demonstrated by the sample interface. *Id.*

[121] NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 4–6 (allowing for flexibility in short form privacy notice design).

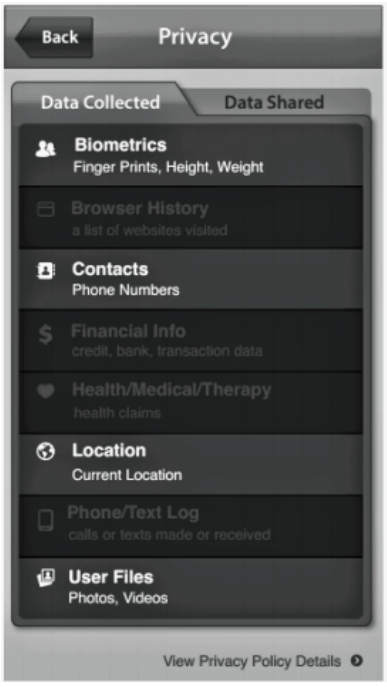
[122] *Id.* at 5.

[123] *See Awesome App: Privacy Dashboard*, ASS'N FOR COMPETITIVE TECH., http://privacydashboard.s3.amazonaws.com/index.html (last visited Mar. 23, 2014) (illustrating the design elements intended for a short form privacy notice); *see also ACT: Privacy Dashboard*, ASS'N FOR COMPETITIVE TECH., http://actonline.org/projects/privacy-dashboard/ (last visited Mar. 23, 2014) (showing the same user interface as it appears on a mobile phone).

[124] *iOS Human Interface Guidelines: Design Principles—Consistency*, APPLE, https://developer.apple.com/library/ios/documentation/UserExperience/Conceptual/MobileHIG/Principles.html#//apple_ref/doc/uid/TP40006556-CH4-SW1 (last visited Mar. 23, 2014).

elements will have the same function and meaning.[125] Likewise, people assume that non-identical elements have different uses and meanings.[126] A user's time is wasted, and a user interface is unnecessarily confusing, when a user must spend time discovering that the functions of non-identical elements are in fact the same.[127]

Figure 3: One of the First Five Sample Privacy Notice User Interfaces Developed Based on the NTIA Code of Conduct for Mobile App Transparency



Source: http://www.ntia.doc.gov

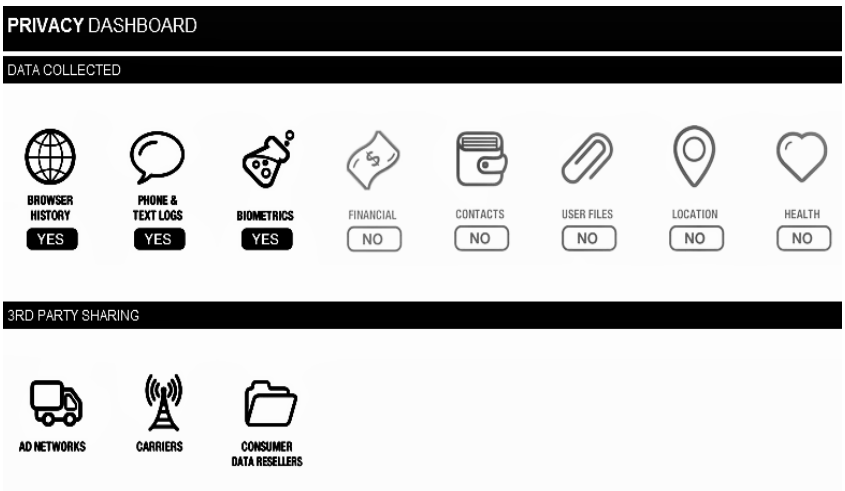
---

[125] *Id.*

[126] *iOS Human Interface Guidelines: Layout—As Much as Possible, Avoid Inconsistent Appearances in Your UI*, APPLE, https://developer.apple.com/library/ios/documentation/UserExperience/Conceptual/MobileHIG/LayoutandAppearance.html#//apple_ref/doc/uid/TP40006556-CH54-SW1 (last visited Mar. 23, 2014).

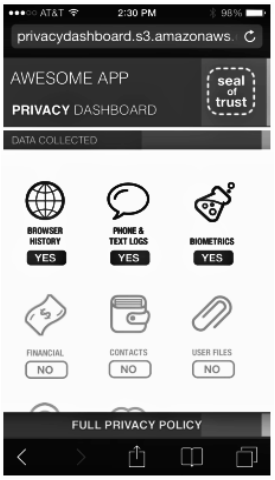
[127] *Id.*

Figure 4: Sample Privacy Notice User Interface Developed by the Association for Competitive Technology Based on the NTIA Code of Conduct (Full View)



Source: http://actonline.org

Figure 5: Sample Privacy Notice User Interface Developed by the Association for Competitive Technology Based on the NTIA Code of Conduct (Mobile View)



Source: http://actonline.org

For example, the user interface ("UI") in Figure 3 uses an icon displaying two human heads to symbolize biometrics, while the UI in Figure 4 uses a bubbling lab beaker to symbolize biometrics. The UI in Figure 3 provides additional text describing biometrics as fingerprints, height, and weight, while the UI in Figure 4 provides no descriptive text. Biometrics is listed first in the UI in Figure 3, and listed third in the UI in Figure 4. The UI in Figure 4 is internally inconsistent because it lists all data collection categories whether used or not and with a visible yes/no status, while only listing the data sharing categories that are affirmatively used and without a visible yes/no status. Confronted with inconsistent UIs, consumers will have to figure out the format of each privacy notice when shopping for apps and making privacy decisions. Analogously, comparing the nutrition labels on packaged foods would be more difficult, if the amount of Trans Fat was listed in a different place with a different appearance on each package of food. It would be even worse if it was unclear whether Trans Fat even had the same meaning across packages of food.

Third, the code contains vague, anti-transparency exceptions.[128] For example, no notice is required for the sharing of data with third-parties if the use of the data is contractually limited "to provid[ing] a service to or on behalf of the app."[129] No definitions or examples are provided to clarify or limit this exception.[130] It is not clear, for instance, if a health app would be allowed to share a person's health information with a third-party insurance company without notice, so that the health app could provide the consumer with an insurability score. For the sake of transparency, no instances of data sharing should be secret. Consumers cannot make privacy decisions when kept in the dark. Justice Brandeis's insight

[128] *See* NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 1–6. The "Exceptions" section does not cover all of the exceptions in the code of conduct. *Id.* at 4. Additional exceptions are spread throughout the code. *Id.* at 1–6.

[129] *Id.* at 3.

[130] *Id.*

into the power of transparency a century ago is just as true today: "Sunlight is said to be the best of disinfectants."[131]

Additionally, no notice is required for collecting data that is promptly de-identified[132] as long as "reasonable steps are taken to prevent the data from being re-associated with a specific individual."[133] But, taking reasonable steps is circularly defined as taking "reasonable measures to de-identify the data" along with making a commitment not to try to re-identify the data.[134] It is not clear, for example, if removing a limited amount of personally identifiable information ("PII") such as a person's name, address, and phone number, while keeping a person's zip code and IP address, is enough to qualify as reasonable measures to de-identify, or if all PII must be removed.[135] If all PII must be removed, it is not clear which state or federal definition of PII should be used.[136]

---

[131] Famous quote by U.S. Supreme Court Justice Louis D. Brandeis talking about the power of transparency. Louis D. Brandeis, *What Publicity Can Do*, HARPER'S WKLY., Dec. 20, 1913, *reprinted in* LOUIS D. BRANDEIS, OTHER PEOPLE'S MONEY, AND HOW THE BANKER'S USE IT 92, 92 (1914), *available at* http://www.law.louisville.edu/library/collections/brandeis/node/196.

[132] Identified means that the data can be associated with a specific person. De-identified means that the identifying information has been removed to an extent such that the identification of an individual would be sufficiently hard, according to a defined standard, to effectively give an individual anonymity. Identification could then only occur through the process of re-identification. *See* 45 C.F.R. § 164.514 (2013) (defining the Health Insurance Portability and Accountability Act ("HIPAA") standard for the de-identification of health information).

[133] NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 4.

[134] *Id.*

[135] The NTIA Code of Conduct does not adequately define a de-identification standard. *Compare id.*, *with* 45 C.F.R. § 164.514 (demonstrating the wide discrepancy between the vague code of conduct standard for de-identification and the highly rigorous and detailed standard in the HIPAA regulations).

[136] The NTIA Code of Conduct does not provide a definition of PII. NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 4. No universal definition of PII exists. NAT'L INST. OF STANDARDS & TECH., GUIDE TO PROTECTING THE CONFIDENTIALITY OF PERSONALLY IDENTIFIABLE INFORMATION (PII) § 2 (2010), *available at* http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf (discussing what information "may" be considered to be PII at the federal level). California provides its own state-level definition of PII.

Moreover, notice may even be withheld for an act of willful blindness.[137] No notice is required "if the entity providing the notice does not affirmatively authorize such collection or sharing and does not have actual knowledge of, or *deliberately* avoid [sic] obtaining actual knowledge of, such collection or sharing before it occurs."[138] Interestingly, the last two exceptions were absent from the earlier drafts of the code of conduct from April and May 2013.[139] The appearance of such striking exceptions may have been necessary for stakeholders to reach a final agreement on the Code of Conduct.[140]

Fourth, the Code of Conduct is surprisingly limited in scope. The Code only addresses one type of notice: short form privacy

---

California's Online Privacy Protection Act (CalOPPA), CAL. BUS. & PROF. CODE § 22577 (West 2014); *see supra* note 111 and accompanying text (providing a summary of the CalOPPA definition of PII).

[137] *See* NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 4. Deliberately avoiding the obtainment of actual knowledge is the definition of willful blindness, although the term is most commonly used in a criminal context. *See, e.g.*, *Willful Blindness (Noun)*, DICTIONARY.FINDLAW.COM, http://dictionary.findlaw.com/definition/willful-blindness.html (last visited Mar. 23, 2014).

[138] NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 4 (emphasis added).

[139] *Compare* NAT'L TELECOMMS. & INFO. ADMIN. MULTISTAKEHOLDER PROCESS, NTIA CODE OF CONDUCT: APRIL 29, 2013 DRAFT (2013), *available at* http://www.ntia.doc.gov/files/ntia/publications/mobileappdraftapril29_2013_draft1b_fs.pdf (draft code of conduct as of April, 29, 2013), *and* NAT'L TELECOMMS. & INFO. ADMIN. MULTISTAKEHOLDER PROCESS, NTIA CODE OF CONDUCT: MAY 16, 2013 DRAFT (2013), *available at* http://www.ntia.doc.gov/files/ntia/publications/mobileappdraftmay16_2013_industry_redline.pdf (draft code of conduct as of May 16, 2013), *with* NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 4 (demonstrating the appearance of exceptions absent from earlier drafts of the July 25, 2013 Code of Conduct agreed to by the stakeholders).

[140] *See, e.g.*, Grant Gross, *Privacy Groups Question NTIA's Focus on Mobile Privacy Transparency*, IT WORLD (July 12, 2012, 2:40 PM), http://www.itworld.com/it-managementstrategy/285876/privacy-groups-question-ntias-focus-mobile-privacy-transparency (demonstrating the level of disagreement and frustration at the beginning of the multistakeholder process and confusion about the process itself).

notices.[141] Additionally, notice is only one of the five fair information practice principles ("FIPPs") of notice, choice, access, security, and enforcement.[142] Privacy advocates were vocal from the beginning that focusing on notice alone, without examining whether certain data collection and sharing practices should be limited or allowed at all, was of little value to consumers.[143] No privacy choices for consumers were developed.[144] Codes of conduct covering choice, access, security, and enforcement are still needed, yet no multistakeholder processes have been announced for these aspects of mobile app privacy. Based on the full year taken to develop the first code of conduct, it will take many years to develop a minimal set of codes to protect consumer data privacy. Although a second multistakeholder process focusing on facial recognition technology has begun,[145] based on reports from the first meeting, the process faces many of the same challenges as the first multistakeholder process as well as an increased skepticism in light of the results of the first multistakeholder process.[146]

C. *The FTC Mobile Privacy Disclosures Report: Progress*

The FTC has made progress by encouraging the development of standard application programming interfaces ("APIs") for privacy notices and controls.[147] Apps must run on app platforms

---

[141] NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 1.

[142] FED. TRADE COMM'N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE 3–5 (2000), *available at* http://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission-report/privacy2000.pdf (describing the five fair information practice principles).

[143] Gross, *supra* note 140.

[144] *See* NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 1–6.

[145] Notice of Open Meetings, Multistakeholder Process to Develop Consumer Data Privacy Protection Code of Conduct Concerning Facial Recognition Technology, 78 Fed. Reg. 73502 (Dec. 6, 2013).

[146] Alexei Alexis, *NTIA Gathers Stakeholders for Facial Recognition Talks*, BLOOMBERG BNA (Feb. 10, 2014), http://www.bna.com/ntia-gathers-stakeholders-n17179881997/.

[147] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 15.

consisting of an operating system and a device.[148] Because companies such as Apple and Google develop and control app platforms, and also control access to their respective app stores, Apple and Google serve as gatekeepers between app developers and consumers.[149] The FTC encourages app platforms to provide developers with APIs to implement standard privacy notices and controls.[150] APIs are a means for developers to access the built-in functionality of an app platform's operating system, such as Apple's iOS operating system ("iOS").[151] For example, Apple could design the appearance and function of a privacy notice.[152]

---

[148] One common definition for a platform is an operating system and the underlying hardware, but the appropriate definition depends on the context. *Definition of: Platform*, PC MAG, http://www.pcmag.com/encyclopedia/term/49362/platform (last visited Mar. 23, 2014). The term "app platform" can also be used in a broader sense to refer to an entirely vertically-integrated app environment including an app company, an app store, an operating system, and a device, such as Apple, Inc., the Apple App Store, the Apple iOS, and the Apple iPhone. FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 14.

[149] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 14.

[150] *Id.* at 14–21. The California Attorney General's Office also focuses on app platforms with its regulatory efforts. *Attorney General Kamala D. Harris Secures Global Agreement to Strengthen Privacy Protections for Users of Mobile Applications*, CAL. OFFICE OF THE ATT'Y GEN. (Feb. 22, 2012), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-secures-global-agreement-strengthen-privacy. In 2012, the California Attorney General reached an agreement with the major app platforms on a statement of privacy principles to help improve app industry compliance with California's Online Privacy Protection Act (CalOPPA). Joint Statement of Principles by the California Attorney General and Mobile App Market Companies, CAL. OFFICE OF THE ATT'Y GEN. (Feb. 22, 2012), http://ag.ca.gov/cms_attachments/press/pdfs/n2630_signed_agreement.pdf; CAL. BUS. & PROF. CODE §§ 22575–22579 (West 2014).

[151] *See, e.g.*, *API—Application Program Interface*, WEBOPEDIA, http://www.webopedia.com/TERM/A/API.html (last visited Mar. 23, 2014); *Definition of: API*, PC MAG, http://www.pcmag.com/encyclopedia/term/37856/api (last visited Mar. 23, 2014); Ross Alderson, Instructional Video, *What Is an API?*, YOUTUBE (Sept. 21, 2011), https://www.youtube.com/watch?v=QSUnBPv4iQ0.

[152] *See generally* David Orenstein, *QuickStudy: Application Programming Interface (API)*, COMPUTER WORLD (Jan. 10, 2000, 12:00 PM), https://www.computerworld.com/s/article/43487/Application_Programming_Interface (providing a brief introduction to APIs).

Apple would then write software code in the form of an API, as part of the iOS, which would display an otherwise generic privacy notice plus the specific notice settings provided by an app developer.[153] For example, an app developer could tell the operating system whether or not a privacy notice should indicate that an app collects biometric information, and the operating system would display the correct notice. As a technical matter, an app developer would programmatically send the specific notice settings to the API to be a part of a particular instance of a privacy notice.[154] To create a privacy notice, the app developer would call the iOS's API by its proper name and pass the notice-setting data to the API.[155] The API would then display a privacy notice of standard appearance and function containing the correct notifications regarding the app developer's data collection and sharing practices.[156] For example, a biometrics icon would appear highlighted rather than greyed-out depending on whether the app developer programmatically told the API that the app collects biometric information. The end result would be that the privacy notices on a single app platform would have the same appearance and function to the extent that app developers used the privacy notice API.

---

[153] *See How to Get Started Programming with the Windows API (LONG)—What is the Windows API?*, MICROSOFT, http://support.microsoft.com/kb/190000 (last visited Mar. 23, 2014) (describing the Windows API and its purpose to allow developers to create programs consistent in appearance and function with the Windows environment). The concepts are the same for the Apple iOS API.

[154] *See generally* Ornstein *supra* note 152 (providing a brief introduction to APIs).

[155] *See How to Get Started Programming with the Windows API (LONG)—How to Call a Windows API Function*, MICROSOFT, http://support.microsoft.com/kb/190000 (last visited Mar. 23, 2014) (describing how to call and pass parameters to an API function in a Windows environment).

[156] *See How to Get Started Programming with the Windows API (LONG)—What is the Windows API?*, *supra* note 153 ("[Y]ou can call the appropriate functions in the Windows API and let the operating system create those components.").

D. *The FTC Mobile Privacy Disclosures Report: Shortcomings*

The FTC recommendations fall short by being both voluntary and reliant on APIs with their inherent limitations.[157] First, the FTC's recommendations are voluntary to the extent that noncompliance by the mobile app industry can only result in an FTC enforcement action when a mobile app company's business practices rise to the level of being unfair or deceptive acts.[158] Mobile app industry compliance with FTC recommendations has been persistently low even in the exceptional case of children-focused apps, in which certain business practices are clearly defined as unfair or deceptive acts.[159] The Children's Online Privacy Protection Act ("COPPA")[160] defines an app developer's failure to provide notice to parents and to obtain parental consent, when collecting personal information from a child under the age of thirteen, as an unfair or deceptive act.[161] However, FTC surveys show a continued lack of compliance by the app industry with the FTC's recommendations for privacy notices for children-focused apps.[162] In February 2012, an FTC survey of 400 children-focused

---

[157] *See* FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 13–21 (making the recommendations that rely on APIs).

[158] Federal Trade Commission (FTC) Act, 15 U.S.C. § 45 (2012); *see supra* notes 100–103 and accompanying text (providing background on the FTC's enforcement authority).

[159] *See* Children's Online Privacy Protection Act (COPPA), 15 U.S.C. § 6502 (2012) (defining a violation of the requirements of COPPA as an unfair or deceptive act); *see also* Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013) (implementing COPPA and known as "the COPPA Rule"); Children's Online Privacy Protection Rule, 78 Fed. Reg. 3972, 4008–14 (Jan. 17, 2013) (to be codified at 16 C.F.R. § 312) (providing the final amended COPPA Rule effective as of July 1, 2013).

[160] 15 U.S.C. § 6501–6506 (2012).

[161] *Id.* § 6502.

[162] FED. TRADE COMM'N, MOBILE APPS FOR KIDS: CURRENT PRIVACY DISCLOSURES ARE DISAPPOINTING 1–2 (2012), *available at* http://www.ftc.gov/sites/default/files/documents/reports/mobile-apps-kids-current-privacy-disclosures-are-disappointing/120216mobile_apps_kids.pdf [hereinafter FTC MOBILE APPS FOR KIDS DISAPPOINTING] (providing survey results from Feb. 2012); FED. TRADE COMM'N, MOBILE APPS FOR KIDS: DISCLOSURES STILL NOT MAKING THE GRADE 1 (2012), *available at* http://www.ftc.gov/sites/default/

apps showed that the apps provided "little or no information to parents about their privacy practices."[163] Following the survey, the FTC made specific recommendations to app stores, app developers, and third-parties directing them to provide better information to parents,[164] such as notifying parents if a children-focused app connects with social media or uses targeted advertising.[165] During the summer of 2012, the FTC performed a follow-up survey of 400 apps hosted by the two leading app stores which showed that the children-focused app industry had "made little or no progress in improving its disclosures since the first kids' app survey," despite the FTC's specific recommendations.[166] The later FTC study also found that children-focused apps shared the personal information of children with third-parties without notice.[167] The lack of compliance by the app industry with the FTC's recommendations in the exceptional case of children-

files/documents/reports/mobile-apps-kids-disclosures-still-not-making-grade/121210mobilekidsappreport.pdf [hereinafter FTC MOBILE APPS FOR KIDS STILL NOT MAKING THE GRADE] (providing the results of a follow-up survey from summer 2012).

[163] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 7; *see also* FTC MOBILE APPS FOR KIDS DISAPPOINTING, *supra* note 162, at 10 ("In most instances, [FTC] staff was unable to determine from the information on the app store page or the developer's landing page whether an app collected *any* data, let alone the type of data collected, the purpose for such collection, and who collected or obtained access to such data.").

[164] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 7.

[165] FTC MOBILE APPS FOR KIDS DISAPPOINTING, *supra* note 162, at 3.

[166] FTC MOBILE APPS FOR KIDS STILL NOT MAKING THE GRADE, *supra* note 162, at 5–6.

[167] *Id.* at 1. The FTC has, in particular cases, brought enforcement actions against unfair or deceptive business practices, under the Children's Online Privacy Protection Act. *See* 15 U.S.C. § 6502 (2012). In February 2013, the social networking company, Path, paid $800,000 to settle charges that it had illegally collected personal information from children without parental consent. Path had access to children's personal journals, photos, written "thoughts," and exact locations and collected children's address books that contained the names, addresses, phone numbers, email addresses, and dates of birth of other children. *Path Social Networking App Settles FTC Charges it Deceived Consumers and Improperly Collected Personal Information from Users' Mobile Address Books*, *supra* note 10.

focused apps, despite the FTC's clear authority to take enforcement actions to protect children under the age of thirteen, shows that both mandatory requirements and strong enforcement provisions are needed to provide consumers with adequate mobile app privacy.

Second, the FTC's recommendation to use APIs falls short in protecting consumers because APIs have significant limitations as a method to control privacy.[168] Critical information regarding data collection and sharing is not captured by APIs.[169] An operating system ("OS") only reliably "knows" what data is collected and shared when an app developer uses an OS's APIs to accomplish this task.[170] For example, when an app developer uses an API to collect the contact information from a user's address book, the OS knows that it has been directed to access the contact information from the user's address book.[171] The OS can report this knowledge to the user in the form of a notice.[172] However, the OS cannot know what information is being collected directly from the user through an app (i.e. the app has its own address book), or what information is being shared with third-parties after the OS's API has been used to collect the information.[173] For example, an app can use an API to collect contact information from a user's address book, but can

---

[168] *See* FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 18 (discussing the problems with a reliance on APIs).

[169] *Id.*

[170] *Id.*; *see generally* Orenstein, *supra* note 152 (providing a brief introduction to APIs).

[171] *See generally Mac Developer Library—About Developing for Mac*, APPLE, https://developer.apple.com/library/mac/documentation/MacOSX/Conceptual/OSX_Technology_Overview/About/About.html#//apple_ref/doc/uid/TP40001067 (last visited Mar. 23, 2014) (providing a brief introduction to the Apple OS X architecture and APIs).

[172] *See W3C: Device API Privacy Requirements—2.1 Notice*, W3C (June 29, 2010), http://www.w3.org/TR/2010/NOTE-dap-privacy-reqs-20100629/ (providing guidelines that require an API to notify a user when data is collected through the API including identifying the app and the precise data collected).

[173] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 18; *see generally* Orenstein, *supra* note 152 (providing a brief introduction to APIs).

later send that information to a third-party without using an API.[174] Additionally, the OS cannot know and report the purposes of data collection or sharing because the OS has no way of knowing how data is used after it has been sent from a device.[175] In short, app developers can bypass API-based privacy tools by not using APIs to collect and share data, and an OS cannot discern higher-order information such as the purposes of data collection.

E. *The APPS Act of 2013: Progress*

The APPS Act makes progress by creating several new substantive and mandatory requirements.[176] App developers must provide users "with notice of the terms and conditions governing the collection, use, storage, and sharing of the personal data."[177] The APPS Act mandates notice of the categories of data collection and sharing, which is significant in its own right.[178] But the APPS Act goes further by requiring notice of the uses of the data by the collector and third-parties.[179] For example, an app developer would have to disclose whether data will be used for targeted advertising, consumer behavioral research, tracking location, or soliciting business from the contacts in an address book.[180] This requirement

---

[174] Moreover, data that is collected legitimately through APIs can be misused at any time after the data has been collected or shared. FREDERICK HIRSCH, INTERNET PRIVACY WORKSHOP POSITION PAPER: PRIVACY AND DEVICE APIS 1 (2010), *available at* http://www.iab.org/wp-content/IAB-uploads/2011/03/frederick_hirsch-revised.pdf.

[175] *Id.*

[176] APPS Act of 2013, H.R. 1913, 113th Cong. § 2 (2013).

[177] *Id.*

[178] *Id.* If passed, the APPS Act will be the first federal law mandating mobile app privacy notifications and the disclosure of data collection and sharing practices to all consumers in contrast to the voluntary requirements of the NTIA code of conduct and FTC recommendations and the limits of COPPA. *See supra* note 106 and accompanying text (discussing the significance of the APPS Act's mandatory substantive requirements).

[179] H.R. 1913 § 2.

[180] *See Millennial Media's Mobile Audience Solutions*, MILLENNIAL MEDIA, http://www.millennialmedia.com/advertise/targeting/ (last visited Mar. 23, 2014) (explaining how Millennial Media uses its first- and third-party data assets to deliver "precise audience and cross-screen targeting solutions").

to disclose the uses and purposes of data collection and sharing[181] increases consumer awareness and choice. The requirement of notice of the terms of storage further helps consumers by requiring app developers to disclose how long data is stored and whether the data is stored in an encrypted form.[182] Consumers can reduce their risk of identity theft by avoiding app developers who unnecessarily store data for long periods of time or in an unencrypted form.

The APPS Act also provides for the withdrawal of user consent.[183] Users would have the option to end data collection and to request the deletion of data that has already been collected.[184] An app developer must provide an app user with the means to "notify[] the developer that the user intends to stop using the application."[185] The app developer must allow the user to request that the developer "refrain from any further collection of personal data."[186] The APPS Act further mandates two user options regarding the data that an app has already collected.[187] At a user's request, app developers must either "delete any personal data collected by the application," or "refrain from any further use or sharing of such data."[188] Data deletion is limited to the data collected by a particular app and is only required to the extent practicable.[189] The option to request the deletion of data that has already been collected is similar to a "right to be forgotten,"[190] although in a limited form.

---

[181] H.R. 1913 § 2.

[182] *See id.* Data encryption is a fundamental "term[] and condition[] applicable to storage." *Id.*

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.*

[187] *Id.*

[188] *Id.*

[189] *Id*.

[190] *See* Jeffrey Rosen, *The Right to Be Forgotten*, 64 STAN. L. REV. ONLINE 88, 88–89 (2012), http://www.stanfordlawreview.org/sites/default/files/online/topics/64-SLRO-88.pdf. "The intellectual roots of the right to be forgotten can be found in French law, which recognizes *le droit à l'oubli*—or 'the right of oblivion.' " *Id.* at 88. Despite its origin in France, the right to be forgotten has

F. *The APPS Act of 2013: Shortcomings*

The APPS Act falls short by both failing to include a data deletion option for data that has already been shared with third-parties, and undermining itself by including the safe harbor provision based on an NTIA code of conduct.[191] First, the APPS Act's data deletion option following the withdrawal of consent fails to include data already shared with third-parties.[192] The APPS Act identifies the app data "stored by the developer" as the data to be deleted.[193] But third-parties are ultimately the entities building personal profiles on individuals for targeted advertising and other purposes, and are a primary source of privacy concern for consumers.[194] The APPS Act deletion option does not require the data stored by third-parties to be deleted.[195]

Second, the APPS Act's safe harbor provision is flawed because it presumes an equivalency between the NTIA code of conduct and the substantive provisions of the APPS Act. In reality, a great discrepancy exists.[196] "The developer of a mobile application may satisfy the requirements of this act . . . by adopting and following a code of conduct for consumer data privacy. . . ."[197]

---

been a source of controversy in the EU and has significant First Amendment implications in the U.S. *Id.* at 88–91; *see also* Giles Tremlett, Angelique Chrisafas & Kate Connolly, *Forget Me Not: Campaigners Fight For Control of Online Data*, THE GUARDIAN (Apr. 4, 2013, 7:41 AM), http://www.theguardian.com/technology/2013/apr/04/right-forgotten-internet-campaign (arguing that a right to be forgotten makes sense when online data is often "out-of-date, misleading, and downright wrong").

[191] *See generally* H.R. 1913 §§ 2, 5 (the two sections at issue here).

[192] *Id.* § 2.

[193] *Id.*

[194] Inderscience Publishers, *Shopping Online, Privacy, Data Protection and Third-Party Tracking*, SCIENCE DAILY (Apr. 7, 2011), http://www.sciencedaily.com/releases/2011/04/110406161037.htm.

[195] H.R. 1913 § 2.

[196] *Compare id.*, *and* Part IV.E, *with* NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 1–6, *and* Part IV.B (demonstrating the wide discrepancy in the substantive requirements for privacy tools, between the APPS Act and the NTIA code of conduct).

[197] H.R. 1913 § 5.

The code of conduct must meet two conditions.[198] First, the code of conduct must have been developed in an NTIA multistakeholder process as described in *Consumer Data Privacy in a Networked World*.[199] Second, the code of conduct must have been approved by the FTC as satisfying the regulations implementing the APPS Act.[200] The FTC would face the choice of approving or rejecting the code of conduct. Unfortunately, this is a poor choice for the FTC. If the FTC were to reject the NTIA code of conduct as insufficient, the safe harbor provision would be ineffectual, and companies would be without a code of conduct to rely upon for certainty in their compliance efforts. If the FTC were to accept the NTIA code of conduct, the safe harbor provision would undermine the substantive protections of the APPS Act and the Consumer Privacy Bill of Rights.[201]

One solution to preserve the safe harbor provision, albeit to a limited extent, would be to modify the safe harbor provision to give the FTC the flexibility to both adopt a code of conduct and to add requirements ensuring that the substantive requirements of the APPS Act are met. However, this solution is contrary to the all-or-nothing approach taken by the safe harbor provision and the recommendations for privacy legislation made in the White House whitepaper, *Consumer Data Privacy in a Networked World*.[202] The whitepaper recommends that the FTC would "limit its review authority to approving or rejecting a code that reflects the

---

[198] *Id.*

[199] *Id.*; *see also* WHITE HOUSE WHITEPAPER *supra* note 90, at 26–27 (describing the NTIA multistakeholder process).

[200] H.R. 1913 § 5.

[201] *See generally* WHITE HOUSE WHITEPAPER, *supra* note 90, at 9–22 (defining a Consumer Privacy Bill of Rights).

[202] *See id.* at 35–39 (making the recommendations for privacy legislation); *see also* Letter from Rep. Henry C. Johnson, Jr. to President Barack Obama (Oct. 24, 2013), *available at* http://apprights-hankjohnson.house.gov/Letter%20to%20White%20House%20and%20Commerce%20on%20Privacy.pdf (demonstrating Rep. Hank Johnson's intention, as the sponsor of the APPS Act, that the APPS Act will enact the White House's recommendations for privacy legislation).

consensus of all participants in the multistakeholder process."[203] This all-or-nothing approach, requiring the FTC to approve or reject the NTIA code of conduct as a whole, does not work well with the shortcomings of code of conduct produced by the NTIA multistakeholder process.

V. LOOKING FORWARD

Mandatory and consistent privacy notices and controls across all apps, platforms, and devices should be the ultimate goal for consumers and the app industry.[204] Privacy tools should be easy to use, increase consumer awareness, and provide privacy choices such as the withdrawal of consent and the deletion of previously collected data.[205] A person cannot be expected to maintain the privacy settings across dozens of apps installed on each of a growing number of devices, without some powerful tools.[206]

Unfortunately, an analysis of the three federal-level development paths for privacy tools reveals that these efforts have not resulted in standard and effective privacy tools.[207] The NTIA code of conduct is voluntary, and falls too short in substantive requirements and scope to provide for standard and effective privacy tools.[208] While the FTC has made many strong recommendations for mobile app privacy, the FTC lacks the direct authority needed to mandate compliance.[209] FTC studies have demonstrated a lack of compliance by the app industry with FTC

---

[203] WHITE HOUSE WHITEPAPER, *supra* note 90, at 37.

[204] Currently, the same app downloaded from Apple, Google, and Microsoft is managed in three different ways. Notices and controls should be consistent across phones, tablets, computers, and car consoles. Many consumers already own multiple devices running a mix of Apple's iOS, Google's Android OS, and Microsoft's Windows OS.

[205] *See* H.R. 1913 § 2 (mandating the withdrawal of consent and data deletion options).

[206] *See* Baker, *supra* note 34 (predicting that the average household will own fifty internet-connected devices by the year 2022 with a corresponding increase in the number of apps each person must manage).

[207] *See supra* Part IV.A–F.

[208] *See supra* Part IV.B.

[209] *See supra* Part IV.D.

recommendations even in the case of children-focused apps.[210] The APPS Act undermines its strong substantive requirements by allowing for a safe harbor provision based on the NTIA code of conduct.[211] Thus, at this time, new legislation is required to generate standard and effective privacy notices and controls.

The privacy dashboards, like those being developed by Microsoft and Apple, and the privacy nutrition labels, being developed at Carnegie Mellon University's CyLab, provide a solid foundation on which to build standard and effective privacy tools.[212] Legislation should embrace these privacy tools. Congress should also grant the FTC strong and direct authority to enforce privacy legislation due to the FTC's long history of protecting consumer privacy and many years spent focusing on mobile app privacy.[213] Legislation should include the progress made by past privacy tool development efforts, and overcome past shortcomings, by requiring: (1) mandatory notice and consent;[214] (2) standard data collection and sharing categories;[215] (3) listing the purposes of data collection;[216] and (4) a mandatory privacy nutrition label format as a component of full privacy disclosure.[217]

Congress should mandate that a "Privacy App" be built into the primary interface of every device. This Privacy App would connect to a privacy dashboard to provide powerful, centralized access to all of the privacy settings available on a device.[218] The Privacy App would be a highly visible and universal privacy tool, thereby, increasing consumer awareness and the ease of use of privacy tools. Congress should also mandate that consumers be permitted

---

[210] FTC MOBILE APPS FOR KIDS DISAPPOINTING, *supra* note 162, at 10; FTC MOBILE APPS FOR KIDS STILL NOT MAKING THE GRADE, *supra* note 162, at 5–6.
[211] *See supra* Part IV.E–F.
[212] *See supra* Part II.A.
[213] FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at i.
[214] *See supra* Part IV.E.
[215] *See supra* Part IV.A.
[216] *See supra* Part IV.E.
[217] *See supra* Part II.A.
[218] *See* FTC MOBILE PRIVACY DISCLOSURES REPORT, *supra* note 11, at 16–17 (discussing privacy dashboards).

to download and view privacy notices before app purchase and separately from downloading and installing an app.[219] The FTC supports separately downloadable privacy notices because the FTC recognizes that privacy notices are less useful after apps have already been paid for and may have already started collecting and disclosing information to third-parties.[220] The NTIA code of conduct encourages app developers to offer separately downloadable privacy notices, although it does not require app developers to do so.[221] As an additional benefit, separate privacy notice downloads would facilitate side-by-side comparisons. Congress should mandate that a "Privacy Notice Viewer App" be developed to facilitate the viewing of privacy notices side-by-side, especially on larger format interfaces such as tablets, laptop and desktop computers, and televisions. Side-by-side comparisons and a Privacy Notice Viewer App would increase privacy policy competition among app developers. The requirement for mandatory privacy nutrition labels would make these side-by-side comparisons even easier and more effective for consumers.

VI. CONCLUSION

Apps fill our smartphones, tablets, and computers; soon, they will fill our cars and control our homes. This is good news for the app industry and can be good news for consumers, but only if standard and effective privacy tools are developed first. The app industry is an important and rapidly growing segment of the U.S. economy. Yet every new revelation of underhanded and objectionable data collecting and sharing practices undermines consumer trust and, ultimately, the app industry itself. Moreover, the data being collected by each app represents a potential source of identity theft and the emotional and economic harm that results from this insidious crime.

---

[219] *See* FTC MOBILE APPS FOR KIDS STILL NOT MAKING THE GRADE, *supra* note 162, at 7 (supporting privacy notice downloads before app purchase).

[220] *Id.*

[221] NTIA MOBILE APP NOTICE CODE OF CONDUCT, *supra* note 96, at 1.

Self-regulation of the app industry has not led to standard and effective privacy tools. Mandatory requirements are needed to protect consumer data privacy. Congress should mandate that a Privacy App be installed on the primary interface of every device to increase consumer awareness and the ease of use of privacy tools. Congress should mandate the availability of privacy notice downloads before app purchase, and the development of a Privacy Notice Viewer App to allow for side-by-side comparisons of privacy notices, and to ignite privacy policy competition in the app industry. Privacy dashboards and privacy nutrition labels have emerged to lead the way towards standard and effective privacy tools, yet Congress has not mandated the use of these tools, and technology continues to speed forward. The time to pass legislation establishing standard and effective privacy tools is now. Our apps are busy collecting data, silently and relentlessly. Indeed, an unimaginable amount a data is being collected without standard and effective privacy tools while you read this sentence.