IS NOTICE ENOUGH: MITIGATING THE RISKS OF SMARTPHONE DATA SHARING

Rebecca Balebako
Cristian Bravo-Lillo
Lorrie Faith Cranor[1*]

I. INTRODUCTION

The benefits to using smartphones are increasingly clear to consumers. A variety of entertainment and productivity apps, from calendars to restaurant reviews to GPS mapping, offer benefits that smartphone users find compelling. Over half of the US mobile market now is using smartphones.[2] At the same time, apps, platforms, and telecommunication carriers are collecting increasing amounts of data and transmitting it to other parties. While the benefits of data sharing may be clear to smartphone users, the potential risks and harms are not as clear.

Privacy advocates and security researchers have looked at which aspects of data collection are the most concerning to users.[3] Security experts have found security holes

---

* Rebecca Balebako and Cristian Bravo-Lillo are Engineering & Public Policy Ph.D. students at Carnegie Mellon University. Lorrie Faith Cranor is an Associate Professor of Computer Science and Engineering & Public Policy at Carnegie Mellon University, where she also directs the CyLab Usable Privacy and Security Laboratory and co-is director of the MSIT-Privacy Engineering masters program. She is also the co-founder of Wombat Security Technologies, Inc.

We thank all the experts who participated in this project by volunteering their time and knowledge. This research was funded in part by NSF grant DGE0903659 and a Bertucci Graduate Fellowship.

[2] ANDREW LIPSMAN & CARMELA AQUINO, 2013 MOBILE FUTURE IN FOCUS (2013).

[3] Zinaida Benenson et al., Poster: Attitudes to IT-Security When Using a Smartphone (2012); Erika Chin et al., *Measuring User Confidence in Smartphone Security and Privacy*, *in* PROCEEDINGS OF THE EIGHTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 1–16 (2012); Noam Asher et al., On the Need for Different Security Methods on Mobile Phones, 465–473 (2011), http://dx.doi.org/10.1145/2037373.2037442 (last visited Dec 15, 2013); ADRIENNE PORTER FELT, SERGE EGELMAN & DAVID WAGNER, I'VE GOT 99 PROBLEMS, BUT VIBRATION AIN'T ONE: A SURVEY OF SMARTPHONE USERS' CONCERNS; JAN LAUREN BOYLES, AARON SMITH & MARY MADDEN, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (2012); Ildar Muslukhov et al., *Understanding Users' Requirements for Data Protection in Smartphones*, http://lersse-dl.ece.ubc.ca/record/271 (last visited Dec 11, 2013); Jialiu Lin et al., Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy Through Crowdsourcing, in Proceedings of the 2012 ACM Conference on Ubiquitous Computing 501–510 (2012); Patrick Gage Kelley, Lorrie Faith Cranor & Norman Sadeh, Privacy As Part of the App Decision-making Process, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 3393–3402 (2013); Serge Egelman,

in smartphone platforms and have proposed solutions.[4] Yet, the literature lacks a holistic analysis of the harms, from tangible damages to privacy concerns, that can come to users as a result of smartphone data collection. This study tries to assess the real harms, and the intervention points where policy can make a difference by mitigating these harms. In this work, we use expert interviews to evaluate the privacy and security harms that occur to users due to smartphone data sharing. Based on a series of interviews with 20 experts from 10 stakeholder groups, we enumerate the major risks to smartphone users from data sharing and the solutions proposed to mitigate these risks. We use the understandings gained through these interviews to evaluate current policy efforts.

Current policy efforts are focused on transparency, and alerting smartphone users to data collection practices. Our work addresses the question of whether the notice approach is the right place to focus attention. We ask whether the status quo is sufficient, and conclude that while current efforts are useful, other areas need more attention.

In the next section, we provide background on smartphone data sharing. In section III, we describe the methodology for performing the expert interviews and analyzing the results. In section IV, we itemize the harms and concerns identified by the experts, and in section V we discuss the interventions that can mitigate these harms. In section VI we discuss and synthesize our findings, offering suggestions about what risk mitigations public policy can address, and how risk communications can be improved.

II. Background and Related Work

In this section, we provide a brief background on policy in the United States regarding smartphone data collection. We discuss the characteristics of smartphones that contribute to data collection risks. We describe current smartphone users' concerns about smartphone security and privacy, and describe advice currently being given to consumers. We explain how expert interviews can be used to understand the actual risks to consumers.

A. Public Policy

We provide an overview of three major attempts to define consumer privacy principles before discussing the policies specific to mobile devices and smartphones.

Adrienne Porter Felt & David Wagner, *Choice Architecture and Smartphone Privacy: There's a Price for that, in* Workshop on the Economics of Information Security (2012).

[4]Michael C. Grace et al., Unsafe Exposure Analysis of Mobile In-app Advertisements, in Proceedings of the Fifth ACM Conference on Security and Privacy in Wireless and Mobile Networks 101–112 (2012); enck-iciss11.pdf, , http://www.enck.org/pubs/enck-iciss11.pdf (last visited Dec 15, 2013); Michael Dietz et al., Quire: Lightweight Provenance for Smart Phone Operating Systems, arXiv:1102.2445 [cs] (2011), http://arxiv.org/abs/1102.2445 (last visited Dec 15, 2013); William Enck et al., A study of Android application security, in In Proc. USENIX Security Symposium (2011).

Over 30 years ago, the Organization for Economic Cooperation and Development (OECD) published the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[5] Most of the OECD's eight principles focus on the data collector's responsibility, including limited collection of data, and collection of data limited to specified purposes.[6]

In 1998, The Federal Trade Commission (FTC) released the Fair Information Practice Principles (FIPPs). These are a subset of the OECD's principles and focus on the consumer's role in managing their data.[7] The principles as defined by the FTC are summarized here.

1. Notice/Awareness: This prerequisite for other rights says notices should inform consumers about data collection.
2. Choice/Consent: Consumers should have options about data collection.
3. Access/Participation: Consumers should be able to view data about themselves and ensure accuracy.
4. Integrity/Security: Collectors must take steps to maintain accurate data and secure it from unauthorized access.
5. Enforcement/Redress: There must be a means to enforce the above rights.[8]

The first three rights place responsibility on both the consumer and the data collector to manage their data and privacy. Data collectors should provide notice and choice, while consumers should read notices, be aware of their choices, and participate in ensuring the data is accurate. Integrity/Security is the only FIPP in which the expectations are solely on the data collector.

In 2012, the White House issued a Consumer Privacy Bill of Rights,[9] which advanced seven rights for consumers over their electronic data. These rights are:

1. Control
2. Transparency
3. Respect for Context
4. Security
5. Access and Accuracy
6. Focused Collection
7. Accountability

---

[5] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980).

[6] Idem.

[7] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS (2002).

[8] Idem.

[9] THE WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY (2012).

These overlap with the FTC FIPPs; all five of the FTC FIPPs are represented in the Consumer Privacy Bill of Rights.[10] Transparency is similar to notice and awareness, and accountability is similar to enforcement and redress. The Consumer Privacy Bill of Rights adds two elements.[11] One is "Respect for Context," defined as: "Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." The second is Focused Collection defined as: "Consumers have a right to reasonable limits on the personal data that companies collect and retain."[12] Like the OECD principles, both of these imply that there should be some limit to the amount of data collected, based on context and the specific users of the data.

Solove and Hertzog argue that the FTC is the most powerful and influential body in privacy jurisdiction, and that notice and choice is one of the "most central aspects" of the jurisprudence.[13] In 2013, the FTC issued a report on Mobile Privacy Disclosures, which included specific guidelines that app developers, smartphone platforms, and advertising networks could use to improve notice to smartphone uses about data collection.[14] The FTC has also endorsed "Do Not Track" a simplified mechanism allowing consumers to indicate if they wish to receive targeted ads.[15]

The California Attorney General issued privacy guidelines for several stakeholders in mobile device ecosystem, including notice and limiting collection of personally identifiable information.[16] The CA AG also threatened to fine app developer that collected personal information but who did not provide a privacy notice.[17]

In 2012, the Department of Commerce's National Telecommunications and Information Administration (NTIA) launched a multi-stakeholder initiative on Mobile Application Transparency.[18] This group created a code of conduct for app developers that included a standardized short-form privacy notice for mobile devices.[19]

While most policy efforts have focused on notice, some attention has been given to the other privacy principles of security and data collection minimization. Both the FTC

---

[10] *Id.* at 10-23.
[11] *Id*. at 15.
[12] *Id*. at 21.
[13] Daniel Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, COLUMBIA L. REV. (forthcoming 2014).
[14] FEDERAL TRADE COMMISSION, MOBILE PRIVACY DISCLOSURES, BUILDING TRUST THROUGH TRANSPARENCY (2013).
[15] FEDERAL TRADE COMMISSION, FTC STAFF ISSUES PRIVACY REPORT, OFFERS FRAMEWORK FOR CONSUMERS, BUSINESSES, AND POLICYMAKERS (2010).
[16] CALIFORNIA DEPARTMENT OF JUSTICE & PRIVACY ENFORCEMENT AND PROTECTION UNIT, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM.
[17] Melissa J. Krasnow, Mobile Application Privacy Policy Enforcement by the California Attorney General, http://www.irmi.com/expert/articles/2012/krasnow11-cyber-privacy-risk-insurance.aspx (2002).
[18] NATIONAL TELECOMMUNICATION AND INFORMATION ADMINISTRATION, PRIVACY MULTISTAKEHOLDER PROCESS: MOBILE APPLICATION TRANSPARENCY (2013).
[19] *Id*.

and the California Attorney General have provided such advice,[20] without describing a means of enforcement.

Solove describes privacy law's focus on transparency and control as "self-management."[21] He argues that this is problematic, due to users' cognitive and structural limitations.[22] The structural limitations include the scale of data collection, data aggregation, and users' difficulties in assessing harm.[23] Cranor provides an overview of 15 years of notice and choice initiatives for online privacy, and argues that they have not been sufficient to protect users due to lack of incentives to participate and the lack of enforcement.[24] Ben-Sharar and Schneider argue that mandated disclosures in general (not just privacy) are ignored or misunderstood.[25] Calo recognizes the problems of typical privacy notices and argues for trying visceral notices instead of the standard textual privacy notices.[26]

In this work, we use several of the rights or practices described above to categorize the harms and interventions suggested by our expert interviewees. In particular we look at notice, choice, security, and data minimization.

B. Privacy and Security on Smartphones

Smartphones have characteristics that distinguish them from personal computers (PCs), and impact the harms and concerns from data sharing. Smartphones are smaller than PCs, and users tend to carry them wherever they go. This allows for a greater chance of loss and theft. Smartphone sensors (e.g. microphone or GPS) permit increased data collection, which allow inferences about the users' behavior[27] and increase the

---

[20] Mobile App Developers: Start with Security | BCP Business Center, http://business.ftc.gov/documents/bus83-mobile-app-developers-start-security (last visited Dec 14, 2013).; National Telecommunication and Information Administration, Privacy Multistakeholder Process: Mobile Application Transparency (2013).

[21] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma,* 126 Harv. L. Rev. 1880, 1880 (2013).

[22] *Id.*

[23] *Id*. at 1888-1893. *See also*, Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE Security & Privacy 26 (2005); Acquisti, Alessandro, and Jens Grossklags. *What Can Behavioral Economics Teach Us About Privacy*, *in* Digital Privacy (2007).

[24] Lorrie Faith Cranor, *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice,* 10 J. on Telecomm. and High Tech. L. 273 (2012).

[25] Omri Ben-Shahar & Carl E. Schneider, *The Failure of Mandated Disclosure,* 159 U. of Penn. L. Rev. 647 (2011).

[26] M. Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027 (2012).

[27] Jun Han, Emmanuel Owusu, Thanh-Le Nguyen, Adrian Perrig & Joy Zhang, *ACComplice: Location Inference Using Accelerometers on Smartphones*, Proc. of the 4th Int'l Conf. on Comm. Sys. & Networks (2012); Roman Schlegel et al., Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones (2011); Nan Xu et al., *Stealthy Video Capturer: A New Video-based Spyware*

possibilities of eavesdropping.[28] Smartphones are a relatively new technology, and many of the security and privacy techniques users have learned for PCs do not apply to smartphones.[29] Smartphones can be susceptible to particular malware attacks that use a smartphone's ability to call premium-rate numbers and other direct access to financial information as mobile money usage increases.[30] Additionally, battery and memory limitations reduce the capacity of smartphone security solutions.[31] Smartphones also have small screen sizes, which limits the ability to communicate complicated ideas or show security icons such as SSL indicators.[32]

The major smartphone platforms in the United States are currently Google's Android, and Apple's iPhone. Apps for Android are available in Google's app market. Since 2012, new apps added to the market are automatically scanned for malware.[33] Apple's screening of market apps is a bit different: Apple requires developers to register for a developer ID before submitting apps to their app store, and Apple reviews apps that are submitted before allowing them to be available in the app store.[34]

Apple and Google rely on the carriers to provide system and security updates to their users' phones. Recently the American Civil Liberties Union (ACLU) filed a complaint with the FTC stating that the carriers fail to provide prompt updates.[35]

On Android phones, the standard privacy notice for apps consists of a notification when an app is installed about which permissions the app can access. This notification lists which of 130 possible permissions, including location and network communication, that the app has requested.[36] Users may either accept all the permissions and install the app, or they may choose to stop the install. Research on Android permissions finds that

---

in 3G Smartphones, in PROCEEDINGS OF THE SECOND ACM CONFERENCE ON WIRELESS NETWORK SECURITY 69–78 (2009).

[28] Mariantonietta La Polla, Fabio Martinelli & Daniele Sgandurra, *A Survey on Security for Mobile Devices*, 15 IEEE COMM. SURVEYS & TUTORIALS 446–471 (2013).

[29] Reinhardt A. Botha, Steven M. Furnell & Nathan L. Clarke, *From Desktop to Mobile: Examining the Security Experience*, 28 COMPUTERS & SECURITY 130–137 (2009).

[30] Reinhardt A. Botha, Steven M. Furnell & Nathan L. Clarke, *From Desktop to Mobile: Examining the Security Experience*, 28 COMPUTERS & SECURITY 130–137 (2009); M. Becher et al., *Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices*, *in* 2011 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 96–111 (2011).

[31] M. Becher et al., *Mobile Security Catching Up? Revealing the Nuts and Bolts of the Security of Mobile Devices*, *in* 2011 IEEE SYMPOSIUM ON SECURITY AND PRIVACY 96–111 (2011); Mariantonietta La Polla, Fabio Martinelli & Daniele Sgandurra, *A Survey on Security for Mobile Devices*, 15 IEEE COMM. SURVEYS & TUTORIALS 446–471 (2013).

[32] Chaitrali Amrutkar, Patrick Traynor & Paul C. van Oorschot, *Measuring SSL Indicators on Mobile Browsers: Extended Life, or End of the Road?, in* INFORMATION SECURITY (2012).

[33] Hiroshi Lockheimer, ANDROID AND SECURITY GOOGLE MOBILE BLOG, http://googlemobile.blogspot.com/2012/02/android-and-security.html (last visited Dec 11, 2013).

[34] Apple, OS X Mavericks - It's built to Keep your Mac Safe., http://www.apple.com/osx/what-is/security.html (last visited Dec 11, 2013).

[35] ACLU Android FTC Complaint, http://www.aclu.org/files/assets/aclu_-_android_ftc_complaint_-_final.pdf (last visited Dec 15, 2013).

[36] Idem.

the current install system is not effective in informing users about permissions, due to lack of user attention and comprehension.[37] Android version 4.3 offered a hidden privacy control that allowed users to set granular permissions on apps, allowing them to disallow specific permissions for installed apps. However, this feature was removed in version 4.4, as Google claimed it was only released by accident.[38]

The iPhone system displays notifications the first time certain data, such as location, is accessed by an app. iPhone also includes several additional privacy settings. One setting allows users to control whether each app can have access to a short list of permissions, such as location and contacts.[39] Another setting allows users to "limit ad tracking," which stops sending the phone's unique id and prevents tracking across apps.[40]

C. CONSUMERS' PERCEPTION AND ADVICE

Research has also been done to understand users' perceptions of smartphone security and privacy. A Pew Internet Study found that smartphone users have concerns about sharing personal information, reporting "57% of all app users have either uninstalled an app over concerns about having to share their personal information, or declined to install an app in the first place for similar reason."[41] Urban et al. found that 78% of mobile phone users felt the data on their mobile phones was at least as sensitive as the data on their home computers, and that they were unwilling to share the contact information for advertising purposes.[42] Chin et al. examined how smartphone users perceived security and privacy on their smartphones and found that users were concerned with physical theft of their data, malware, and wireless network attacks.[43] A survey on smartphone users' concerns regarding unauthorized access by smartphone apps found

---

[37]Adrienne Felt et al., *Android permissions*, *in* PROCEEDINGS OF THE EIGHTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 1–14 (2012); Patrick Gage Kelley, Lorrie Faith Cranor & Norman Sadeh, Privacy As Part of the App Decision-making Process, in Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 3393–3402 (2013).

[38] Peter Eckersley, GOOGLE REMOVES VITAL PRIVACY FEATURE FROM ANDROID, CLAIMING ITS RELEASE WAS ACCIDENTAL ELECTRONIC FRONTIER FOUNDATION, https://www.eff.org/deeplinks/2013/12/google-removes-vital-privacy-features-android-shortly-after-adding-them (last visited Dec 16, 2013).

[39]There are 8 types of data that iOS warns users about and allows them to control: location, contacts, calendars, reminders, photos, Bluetooth, microphone, and motion activity. In addition, users are warned if apps request access to social accounts such as Facebook or Twitter.

[40]iPhoneHacks, HOW TO MANAGE PRIVACY SETTINGS ON YOUR IPHONE, IPAD, OR IPOD TOUCH IN IOS6, http://www.iphonehacks.com/2012/10/ios-6-manage-privacy-settings-iphone-ipad-ipod-touch.html (last visited Dec 10, 2013).

[41]JAN LAUREN BOYLES, AARON SMITH & MARY MADDEN, PRIVACY AND DATA MANAGEMENT ON MOBILE DEVICES (2012).

[42] Jennifer Urban, Chris Hoofnagle & Su Li, *Mobile Phones and Privacy*, UC BERKELEY PUB. L. RESEARCH PAPER NO. 2103405 (2012).

[43]Erika Chin et al., *Measuring User Confidence in Smartphone Security and Privacy*, *in* PROCEEDINGS OF THE EIGHTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 1–16 (2012).

that the greatest concerns were contacts being deleted, premium text message being sent, or calls to 1-900 numbers.[44] Passwords and GPS tracking information are also considered sensitive information.[45]These studies are complimentary to ours in that they look at user perceptions, while we look at a range of expert perceptions.

Non-profits, government agencies, and media outlets have offered advice to smartphone users on protecting their smartphone privacy and security. For example, the European Network and Information Agency's advice on smartphone security includes automatically locking the smartphone with a password to prevent unauthorized access, checking the reputation of apps or services to avoid malware, and clearing the phone's data ("reset and wipe") before disposing of the phone.[46] A Forbes.com article advising readers about smartphone privacy includes the above advice, as well as updating apps for security patches, using smartphone privacy settings to limit location tracking and access to other information, and limiting access by closing apps when they aren't being used.[47] The Privacy Rights Clearinghouse, a non-profit consumer advocacy group, released a fact sheet titled "Privacy in the Age of the Smartphone," which informs readers that criminals, advertisers, and the government all want to "snoop" on their smartphone. In addition to protecting the phone with a password and researching apps before downloading, the privacy tips offered to consumers include contacting carriers to opt-out of data collection and advocacy such as writing to their congressional representatives to advocate for better laws.[48]

We hope our research will help improve advice to consumers and other stakeholders by highlighting the harms and providing solutions to reduce the risk of the harms.

E. EXPERT ELICITATIONS

Expert elicitations have been used to inform public policy in a number of areas, particularly those where the risks are difficult to quantify, such as biological invasions by non-native species,[49] the use of biofuels,[50] and other areas investigated by the

---

[44] ADRIENNE PORTER FELT, SERGE EGELMAN & DAVID WAGNER, I'VE GOT 99 PROBLEMS, BUT VIBRATION AIN'T ONE: A SURVEY OF SMARTPHONE USERS' CONCERNS (2012).

[45] Ildar Muslukhov et al., *Understanding Users' Requirements for Data Protection in Smartphones*, http://lersse-dl.ece.ubc.ca/record/271 (last visited Dec 11, 2013).

[46] Giles Hogben & Marnix Dekker, SMARTPHONES: INFORMATION SECURITY RISKS, OPPORTUNITIES AND RECOMMENDATIONS FOR USERS (2010).

[47] Caroline Mayer, Don't Be Dumb About Smartphone Privacy, FORBES, http://www.forbes.com/sites/nextavenue/2013/03/05/dont-be-dumb-about-smartphone-privacy/2/ (last visited Dec 14, 2013).

[48] PRIVACY RIGHTS CLEARINGHOUSE, FACT SHEET 2B: PRIVACY IN THE AGE OF THE SMARTPHONE (2012).

[49] David M Lodge et al., *Biological Invasions: Recommendations for U.S. Policy and Management*, 16 ECOL APPL 2035–2054 (2006).

Environmental Protection Agency.[51] Expert interviews have also been used in computer security.

Sheng et al. used expert elicitations to determine the risks of phishing to users. They interviewed 31 experts on phishing and malware prevention using open-ended questions. They looked for recurring themes across the experts to synthesize high-level findings about risks and options to stakeholders. They identified several places where the stakeholder most able to fight phishing had little incentive to do so.[52]

Bravo-Lillo et al. interviewed both users with advanced security knowledge, and average or novice users about their reactions to security warnings. They found several key differences between advanced and novice users. For example, novice users usually decide to trust a site or software based on its look-and-feel, while advanced users would only use look-and-feel as a warning against trusting a site or software. The authors mention the importance of mitigating risks where feasible, as opposed to relying on warnings.[53]

Expert elicitations have been used to create risk notifications and communications. An effective risk communication should focus on issues that people at risk need to know but currently ignore.[54] Thus, risk communications should inform the public about the risks of a technology based on an understanding of both the actual and the perceived risks. Current smartphone notices inform users about data sharing, but not about the consequences and actual risks of data sharing.[55] This suggests that risk communication for smartphone data sharing can be improved.

Morgan et al. outline a method for creating effective risk communication for many areas of public policy. The method focuses on one risk at a time, and includes five steps: creating an expert model, conducting open-ended mental model interviews, conducting structured confirmatory interviews, drafting an appropriate risk communication, and evaluating the communication. The authors recommend observing the frequency with which new concepts emerge with each interview. In most cases, after between 20 and 30 interviews no new concepts will emerge.[56] Similarly, Meyer provides guidelines for conducting expert elicitations,[57] and Kynn et al. discusses how to counter

---

[50]Giulia Fiorese et al., *Advanced Biofuels: Future Perspectives from an Expert Elicitation Survey*, 56 ENERGY POLICY 293–311 (2013).

[51]U.S. ENVIRONMENTAL PROTECTION AGENCY, EXPERT ELICITATION TASK FORCE WHITE PAPER (2011).

[52] S. Sheng et al., *Improving Phishing Countermeasures: An Analysis of Expert Interviews*, *in* ECRIME RESEARCHERS SUMMIT, 2009. ECRIME '09. 1–15 (2009).

[53]Cristian Bravo-Lillo et al., *Bridging the Gap in Computer Security Warnings: A Mental Model Approach*, 9 IEEE SECURITY & PRIVACY, 2011, at 18–26.

[54] Granger Morgan et al, RISK COMMUNICATION: A MENTAL MODEL APPROACH (2001).

[55] For example, the Android permission "Internet" is explained with the following text: "Allows applications to open network sockets." One warning for iOS is "[App name] would like to use your current location."

[56]GRANGER MORGAN ET AL, Op. Cit.

[57] MARY A. MEYER, ELICITING AND ANALYZING EXPERT JUDGMENT A PRACTICAL GUIDE (2001).

some of the heuristics and biases in expert elicitations. For example, experts (and non-experts) tend to be overconfident in their estimations.[58]

Our study informs the creation of an expert model of the multiple risks and harms that may affect smartphone users. In order to find those risks that experts agree that lay users face, we used a large pool of experts (20) from different backgrounds, and report on those risks mentioned by five or more experts. While we believe this approach allows for some consistency in identified risks, further work is necessary to determine the statistical occurrence of these risks in the smartphone ecosystem.

III. METHODOLOGY

We interviewed 20 experts on privacy and security from 10 different stakeholder groups involved in smartphone data sharing. The anonymous interviews were typically one hour long. Experts were not compensated for their time. The interviews were recorded, transcribed verbatim, and coded for themes regarding harms, risks and interventions.

A. STAKEHOLDER SELECTION AND RECRUITMENT

In order to get a broad range of opinions and perspectives, we first identified ten stakeholder groups from which to select participants. All participants were working in privacy or security, and typically had experience with mobile or smartphone privacy or security. We classified experts based on their current or recent employers as follows:

- *Academia* - Researchers and professors in university or research lab settings who conduct research on smartphone security or privacy.
- *Application Industry* - App developers or app industry representatives.
- *Platform providers* - Developers or managers in companies building smartphone operating systems or platforms.
- *Telecommunications providers* - Researchers or managers in companies providing telecommunication services.
- *Security Experts* - Developers or managers in companies providing security solutions, or managing the security branches of IT companies.
- *Aggregator or advertiser* - Developers or managers in companies aggregating data or providing ads based on smartphone data.
- *Consumer advocates* – Representative of non-profit agencies advocating for consumer privacy.

---

[58]Mary Kynn, *The "Heuristics and Biases" Bias in Expert Elicitation*, 171 JOURNAL OF THE ROYAL STATISTICAL SOCIETY: SERIES A (STATISTICS IN SOCIETY) 239–264 (2008).

- *Industry* - Representatives from online advertising and other stakeholder industry associations as well as attorneys who represent multiple industry stakeholders
- *Government* - Public policy specialists working for federal regulatory agencies.
- *Privacy Industry* - Developers or managers in companies providing consumer privacy tools.

We looked for experts who had been involved in recent public policy efforts on mobile transparency such as the NTIA's Privacy Multi-stakeholder Process on Mobile Application Transparency (NTIA MSHP), who had published papers on mobile privacy and security, or who had been recommended by other experts. We recruited experts using a personalized email, asking them to volunteer one hour to participate in the interview on mobile privacy and security. Participants were told that they would be anonymous and were not expected to represent their employers. We interviewed 20 experts representing all of the stakeholders above. Some experts fell into two categories, due to the range of their experience and their self-descriptions. For example, an expert who worked in one field for a number of years and then recently switched employers, or an expert whose job includes multiple roles, could represent two stakeholder groups. For experts who fell into two categories, we use a participant id based on which experience was longer (Table 1).

Ten experts were invited but did not agree to be interviewed, citing time constraints (4), constraints due to their employer or profession (2), did not provide a reason (1), or did not respond to multiple requests (3). These experts represented all of the stakeholder groups, except industry and government. Therefore, we feel that there was not a stakeholder selection bias in participation.

Table 1 gives an overview of the participants and the stakeholder they represented. The experts were typically well-seasoned: 13 experts had over 15 years of experience, and only two had 5 or fewer years of experience. Half (10) of the experts were participants in the NTIA MSHP.

ID	Stakeholder
AC1	Academia
AC2	Academia
AC3	Academia
SE1	Security Expert & Academia
SE2	Security Expert & Platform Provider
AD1	Aggregator or Advertiser
AD2	Aggregator or Advertiser & Industry
AP1	Application Industry
AP2	Application Industry
CA1	Consumer advocate

CA2	Consumer advocate
L1	Industry
L2	Industry
G1	Government
G2	Government
PL1	Platform Provider
PL2	Platform Provider
PI1	Privacy Industry
TE1	Telecommunications Provider & Application Industry
TE2	Telecommunications Provider

TABLE 1 : PARTICIPANTS WHO WERE INTERVIEWED, INCLUDING STAKEHOLDER GROUP. THE NUMBERS USED IN THE IDS DO NOT CORRESPOND TO THE ORDER IN WHICH PARTICIPANTS WERE INTERVIEWED.

If the expert agreed to the interview, they were asked to fill out an anonymous consent form, as required by Carnegie Mellon University Institutional Review Board. The researcher then contacted them by phone or in person for a one-hour interview. The experts were all advised that they would remain anonymous. All experts were told they would be provided with the final report, but they were not given the option to modify or change the results. The interviews took place in the first quarter of 2013, before the eruption of news regarding government surveillance due to the Snowden leaks.

B. INTERVIEW DESIGN

The interviews were "standardized open-ended interviews,"[59] also known as "semi-structured interviews." The interview script contained ten open-ended questions regarding harms and risks of smartphone data sharing, the possibilities for reducing risks, future directions, and vulnerable populations. The researcher-interviewer asked clarifying questions or detailed questions as needed throughout the interview. The interview script is provided in Appendix A.

Great care must be taken in designing the questions for expert elicitations to ensure that experts will be able to interpret them correctly. We conducted pilot tests with four graduate students involved in privacy and security research. An additional pilot test was conducted with a graduate student with experience running expert interviews on risks in a different domain (nuclear energy). Finally, we shared our interview script with an expert on expert elicitation for risk communication to gather feedback on the questions

[59] Daniel W. Turner, *Qualitative Interview Design: A Practical Guide for Novice Investigators*, 15 THE QUALITATIVE REPORT 754–760 (2010).

and coding methodology. These steps allowed us to refine the interview questions, both helping with the flow of questions, the wording of the questions, and the amount of time required to complete the interview.

We designed our questions to be neutral and open-ended. In our pilot tests, we found that when interviewees were asked about what a user can do to avoid risk, they were able to respond better to a specific scenario than a general question. Therefore, we framed the question about what the user can do to prevent harms and risks as, "My mother recently got a smartphone. What should she do to protect herself from the harms we discussed?" Furthermore, our pilot tests indicated that experts struggled to rank the harms in terms of likeliness or harmfulness. Therefore, we made the question less precise and asked the experts to identify which harms were the "most" harmful and the "most" likely.

Despite our attempt to be neutral, some experts were concerned that we only asked about the risks or harms of data sharing from smartphones, instead of asking about the benefits as well. However, our goal was to identify all harms and concerns in a holistic manner, so that the appropriate mitigations can be considered, and smartphone users can continue to enjoy the benefits of smartphones.

The same researcher conducted all interviews from February to April, 2013. In some interviews a second researcher took notes. Five interviews were done in person, in private offices. All other interviews were conducted remotely. We recorded the audio of all interviews, except for two participants who declined to be recorded. The interviewer refrained from offering personal opinions or reacting emotionally to responses, and tried to take notes consistently throughout the interview. If the interviewer was unclear about a response, she tried to re-phrase it neutrally and give the interviewee a chance to respond and clarify.

C. Results Coding

To code the results, we used "emergent coding" to create a list of themes.[60] Two researchers independently reviewed the notes and transcripts of 15 interviews to create coding sheets for themes. Then, they compared the two sets of codes to resolve differences and create a consolidated list of themes. A third researcher with experience coding expert interviews acted as a moderator to help define the major themes.

One researcher then coded the transcripts using the themes identified in the above process. The transcripts were marked to identify salient quotes, frequency of comments, and also to identify which stakeholders discussed which themes.

D. Limitations

[60] Jonathan Lazar, Jinjuan Heidi Feng & Harry Hochheiser, Chapter 11: Analysing Qualitative Data, Research Methods in Human-Computer Interaction (2010), 281-303.

Qualitative interviews allow for in-depth analysis that cannot be obtained through quantitative surveys. However, the small sample size necessarily limits the conclusions that can be drawn. We found that very few new themes emerged after 15 interviews, regardless of the stakeholder. Therefore, our selection of 20 experts appears to be sufficient to get a broad representation of possible harms and interventions. However, it does not provide a large enough sample to evaluate differences between stakeholders. In addition, there were some themes that emerged in the second half of the interview process that inspired additional questions to subsequent participants. We do not know how the earlier participants would have responded if asked directly about those themes.

Furthermore, it is difficult to elicit probabilities associated with risk when the chances of harms are extremely small, or extremely dependent on context. Therefore, we avoided asking for or performing quantitative evaluations of risk.

IV. Harms and Concerns

In this section we describe the risks and harms identified by the experts. First, we describe the major themes that were identified. We then describe which harms were considered either likely or harmful.

A. Definition of Data Sharing

As a warm-up question, and to make sure that experts were using similar definitions, we began the interview by asking the experts to define "data sharing" from smartphones. Experts typically defined the term as data that is sent from the phone to any other party, including app developers, phone carriers, the OS or platform providers, and any third-parties with whom data is further shared.

Harm	Examples	# Experts
Social problems & embarrassment	Embarrassment, problems with social relations, spamming friends, social boundaries crossed (employer see something they shouldn't), sensitive data being viewed by others, cyber-bullying	17
Direct financial harm	Malware, thieves discover house location, id theft, premium texting	16
Surveillance & monitoring	Government surveillance, location monitoring (whether or not physical harm/stalking results), activity monitoring	13
Privacy concerns	Strangers/enemies find location, sensitive data being viewed by someone else, identified based on biometrics	13
Financial discrimination	Price discrimination, job discrimination, insurance discrimination, redlining	11
Physical harm/stalking	Strangers find location, stalking, physical harm due to location being known, harm due to knowledge about physical vulnerability	9
Behavioral advertising	Unwanted marketing	8
Resource usage	Spam, downloading unwanted software, battery drain	8
Health discrimination	Medical insurance discrimination, discrimination based on disability	5
Harm to society	Phone converted to botnet, filter bubble	4

TABLE 2: THEMES FOR HARMS, RISKS, AND PRIVACY CONCERNS, ORDERED BY THE NUMBER OF EXPERTS THAT MENTIONED THEM.

B. Identifying Harms and Concerns

The goal of the first part of the interview was to brainstorm all the possible harms or concerns that could impact a smartphone user. We then used follow-up questions to identify which they consider most likely or harmful. Some experts expressed reservations with the word "harm." They were particularly concerned about whether "harm" included only things could be proven harmful in a court of law. Our goal was to open the field so that all possible concerns could be aired. We asked experts to consider not just "harms," but also concerns. When one expert said that laws already protect users (such as against identity theft), we asked him to discuss what was possible, assuming that a lawsuit or other action was less desirable than preventing the harm.

Using emergent coding, we identified several major themes to describe the harms or concerns that could impact smartphone users as a result of data sharing. These themes are listed in Table 2. The examples are those specifically mentioned by experts.

Experts' responses included a range of high-level themes, such as those in the left column of Table 2, or very specific examples of harms and how they are caused. Some themes overlapped with other themes, but the examples given for each justified treating them separately. For example, physical harm and stalking could also be related to surveillance and monitoring, in that stalking implies monitoring. However, there were sufficiently different examples in each group. Being monitored was described as harm in itself, whether or not it leads to a physical attack.[61] Physical attacks were a significant concern that could result from stalking, but could also occur as a result of other types of data releases.

C. Evaluating Risks of Harms

We asked experts to tell us which of the harms they identified was the "most harmful," and which was the "most likely." Many experts did so, but several experts said that this was difficult as it may depend on the context, the user, or a specific scenario. G1 expressed his concern as follows: "It ends up not being super helpful to talk about what's most likely and what's most dangerous because you don't know anybody's individual situation, and I think there's a wide diversity of situations out there and contexts in which that calculus might change." SE2 expressed a concern about quantifying the level of harm or risk: "One of the biggest risks in smartphones and data and big data is that we don't fully understand the implications of the data, so the harms are un-quantified." Due to the difficulty in identifying whether harms are likely, these experts often identified causes of harms (such as being infected by malware or unexpected data sharing) rather than harms to the user (such as financial theft) when identifying which was the most likely harm.

D. Likely Harms

When asked to describe likely harms, experts included both the harms and causes of harms. We coded the responses into the harm themes described above. Five or more experts identified the following issues as being likely:

- Infection by malware (10 experts)
- Unexpected or excessive data sharing (8 experts)
- Social problems and embarrassment (5 experts)

Experts identified infection by malware most frequently. For example, L2 described malware with the following examples: "I think that there is a real risk that cyber criminals will find ways just as they try to phish today. Or for that matter, that foreign governments may try to compromise mobile devices and turn them into bot nets. Certain malware-based mischief is probably the biggest risk." Many experts identified

---

[61] *See, e.g.,* Neil Richards, *The Dangers of Surveillance*, 126 Harv. L. Rev. 1934 (2013).

malware as leading to financial harms to users. Some thought malware could also result in other types of harms, such as harm to society caused by bot nets (AC1) or resource use caused by spam (PL2).

Two experts said that although malware was currently not that frequent on smartphones, they expected malware to increase in the future due to financial incentives. SE1 said, "As far as malware goes on phones, it's still a pretty small problem, especially compared to the PC malware. However, mobile devices are increasingly ubiquitous. So I don't think anybody's questioning that it's gonna be a big problem in the future."

Eight experts identified unexpected or excessive data sharing as likely. This includes data sharing with apps, or with third-parties. PI1 explained the high probability of data sharing, "The immediate threat to look at is the opposite of data minimization by apps right now, in terms of are they collecting only what they need for their particular process, or are they taking more data they're trying to find a secondary use for later." However, some experts said that although this was likely, it did not necessarily lead to a direct harm. AP1 said, "The most likely is the data sharing with others, but not necessarily leading to your identity being stolen."

Social problems and embarrassment were described as occurring either because of poor user interfaces (UI), or the user not being aware of the possible use or re-use of their data. L1 described the poor UI problem: "I do think people are inadvertently posting, sharing, having trouble with the UI... I'm making decisions to share or not share with UIs that aren't always well designed, and so I may be over-sharing, either because of social network or just because of posting, tweeting, contacting, messaging."

E. HARMS THAT COULD CAUSE THE MOST DAMAGE

The most damaging concerns identified by five or more experts were:

- Financial (12 experts)
- Physical (5 experts)
- Social Harms (5 experts)

Financial harms, typically resulting from direct financial theft, phishing, identify theft, or malware, were identified the most frequently as harmful. PL1 expressed this concern: "I believe that the one that is most harmful is the direct theft of financial data because that has a direct financial impact on the user."

Physical harm from stalking or location being known was also identified as harmful. AP2 described it, "The most harmful would be stalking, leading to ultimate dire consequences." G2 said, "Stalking isn't that likely but the damages are so great."

Social harms covered a range of social issues, from divorce to loss of job. Embarrassment also fell into this category. G2 expressed that this could fall within a range of very harmful to not harmful, "Embarrassment sounds like it should be low on

the list but people do lose their jobs from information that's found out, and marriages break up and things based on information getting out that people didn't intend to get out. And that happens a lot so … it's a pretty wide spectrum from just small embarrassment to something getting sent that you didn't want, a picture getting out that you didn't have out there to losing a job or losing out on an opportunity or because something got out there that was taken out of context."[62]

V. INTERVENTIONS

We were interested in what could be done to prevent the harms and concerns described by experts. We identified three groups who could help protect the user: smartphone users themselves, app developers, and platform or OS developers. Several experts also described what the government or regulation could do to mitigate harms, and we specifically asked the government stakeholders about the role of regulation in mitigating harms. We describe the mitigation themes that were mentioned most frequently by experts.

A. INTERVENTIONS BY USERS

Five or more experts mentioned each of the following four ways smartphone users themselves could mitigate harms.

- Education (17 experts)
- Lighted Streets (15 experts)
- Protect Phone (7 experts)
- Reduce Functionality (5 experts)

Education: Experts suggested that smartphone users need to become better educated about a variety of topics including privacy settings, how location works, or the data ecosystem. Some experts felt users should understand app origin and behavior. AP1 said the entire ecosystem needed to be better understood: "No amount of improvement in

---

[62] Some research has been done on embarrassment and regret on social networks such as Facebook or Twitter. See WANG, YANG, GREGORY NORCIE, SARANGA KOMANDURI, ALESSANDRO ACQUISTI, PEDRO GIOVANNI LEON, AND LORRIE FAITH CRANOR. "I regretted the minute I pressed share: A qualitative study of regrets on Facebook." In *Proceedings of the Seventh Symposium on Usable Privacy and Security*, p. 10. ACM, 2011. And SLEEPER, MANYA, JUSTIN CRANSHAW, PATRICK GAGE KELLEY, BLASE UR, ALESSANDRO ACQUISTI, LORRIE FAITH CRANOR, AND NORMAN SADEH. "i read my Twitter the next morning and was astonished: a conversational perspective on Twitter regrets." In *Proceedings of the 2013 ACM annual conference on Human factors in computing systems*, pp. 3277-3286. ACM, 2013.

logical interface, better icons, better information flow will prevent the problem, which is that people lack context. Therefore even something that fully notifies them – unless they understand its implications or what it means – it's still pointless."

Some experts stressed that smartphone users needed to understand the risks behind different phone features. AP1 described the issue: "The larger question is that if you share, but by sharing you put yourself at risk because you shared too broadly, you didn't understand the full complexity of what you're sharing or how it's being shared, There exists some risks there."

Experts stressed that it was the users' responsibility to educate themselves. PL1 said, "You [the smartphone user] have to be smart about it and you have to know where the app is coming from and try to know as much as possible about what the app is doing."

Previous research found evidence of the need for smartphone user education. Mylonas et. al investigated users' awareness of smartphone security, and how it impacts their decision-making about app downloads. They found that users who are not security-savvy, or are unaware of smartphone malware are more likely both to trust app repositories and to store personal data in their phones. [63] Thus, the need for education for less aware smartphone users becomes especially important.

Play on the Lighted Streets: experts frequently mentioned that users needed to download only trusted apps or use only trusted app stores. We borrow the title of this theme from AC3, who said: "The best thing I can tell you is to play on the lighted streets, and by that I mean that for the most part, the popular applications are safer because they receive more scrutiny." PL2 also stated, "The first thing is ... have some notion of which apps are trusted."

Following this advice typically requires that users download apps only from well-known brands or manufacturers. PL1 explained, "One of the biggest things that I always look for and I always encourage my friends to look for is a trusted vendor. If that vendor or manufacturer misuses my data, what do they stand to lose?" AP2 echoed that a user should rely on well-known brands, such as, "large brand companies with reputational risks attached to their name. Usually publicly-traded companies, which are traded on the Stock Exchange, or companies with a brand name, are more likely to be responsive to consumers and therefore, easier to trust because press accounts or journalistic inquiries about their practices are likely to create more scrutiny of the company."[64]

---

[63] ALEXIOS MYLONAS, ANASTASIA KASTANIA, DIMITRIS GRITZALIS, Delegate the smartphone user? Security awareness in smartphone platforms, Computers & Security, Volume 34, May 2013, Pages 47-66, ISSN 0167-4048,

64 There is some evidence supporting experts' intuition. See for example Rahul Telang & Sunit Wattal, An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price, IEEE Transactions on Software Engineering, Vol. 33, No. 8, August 2007, Pages 544-557.

Other advice in this category also included that users should only download apps from major app stores. G1 stated, “I think the number one thing that she should do, is she should only download apps from marketplaces, and really she should only download apps from whatever the ... relevant OS marketplace is for her phone.”

Experts also advised that users only download popular apps that have been downloaded many times before. APL1 said, “So when you’re installing apps, try not to be like the first one to install an app.” AP1 advised reading the app store reviews, “So be cognizant of the reviews, what the number of stars are. Simple things like that can at least help to some degree. Is it a solution? No… Does it mitigate? Yes.”

Protect Phone: Protecting the phone involves installing protective software or physically safeguarding the phone, typically against the phone being stolen or physically intercepted. AC1 said, “The types of precautions is to guard physical control of the phone and to think of it as just as sensitive as your computer, and that means you put a password on it and you don’t leave it lying around for your suspicious father to search through.”

Suggested software protections include a remote finder in case the phone is lost, setting a secure phone password, using a password manager with encryption, using secure VPN, setting up a remote wipe, and backing up the phone’s data.

However, G1 cautioned that this type of protection was not sufficient, “PINS and passwords are not going to be guaranteed security against a really determined criminal or guaranteed security against law enforcement when they’re trying to access your device, but they’re like door locks. They keep honest people honest, and keeping honest people honest can be really helpful when many privacy risks come from people you know.”

Reduce Functionality: Experts mentioned specific functionality that should be turned off in order to reduce data sharing. These included turning off Bluetooth (AC2 and SE2), location (AC2), using airplane mode (L1), network settings (SE2), and avoiding public Wi-Fi networks (SE2, AP2). Turning off these functions may limit the usability of the phone for certain apps or usages, but it also limits the data being sent, or limits when or where it is transmitted.

SE2 described how a smartphone user could protect herself: “She should take a look at the network settings and disable anything she doesn’t use... For example, if she has no intention of using a Wi-Fi network, turn off Wi-Fi. There’s no reason to have it on.” AP2 said, “She probably should not use a public Wi-Fi network when sending or transmitting any sensitive information.”

One example of this is that brick-and-mortar stores are currently using public Wi-fi to track their shoppers’ movements indoors, often without their knowledge or

permission. The advice the popular press has given to those who wish to avoid this is to, "turn their phone off and take the battery out."[65]

Nothing: Four experts expressed concern that there wasn't much the user could do to prevent the harms discussed. While this was not a frequent theme, we mention this issue as an important concern. G1 said, "In terms of mitigating the risk, reducing the risk, attempting to prevent the risk... There's a bunch of stuff she can do. But in terms of actually outright preventing the risk, get rid of the Smartphone." CA2 expressed concerns about the data sharing ecosystem, "It's gonna be very hard to escape the system. Almost impossible." All four of these experts did suggest at least one of the interventions mentioned above in addition to expressing skepticism that real protection was possible.

B. Interventions by App Developers

Five or more experts identified each of the following ways app developers could mitigate harms.

- Transparency (15 experts)
- Best Security Practices (8 experts)
- Priority (7 experts)
- Data Minimization (6 experts)
- Understand APIs (5 experts)
- Customer Relationship (5 experts)

Transparency: Fifteen experts mentioned that app developers needed to be more transparent about their data sharing practices through disclosures to users. This included disclosing the purpose of the data collection. G2 said app developers should disclose, what data they're collecting for themselves and what data they're planning on collecting and sharing for other purposes." This was echoed by AP2 and PL10, who were concerned about what data was being collected, why it was being collected, and with whom it was being shared.

SE2 felt transparency would address privacy concerns by removing surprises, "I have a hunch that the majority of people's concern about privacy on the web and on smartphones has to do with the lack of transparency. They just don't know what's going on, so when they find out it's a surprise 'cause they assumed it wasn't."

The CA Attorney General has also been addressed this mitigation in the recommendation for app developers to, "Develop a privacy policy that is clear, accurate, and conspicuously accessible to users and potential users." [66]

---

[65] Lee Jae-Won, Retail stores track consumers' smartphones through Wi-Fi, http://rt.com/business/smartphone-us-store-wifi-112/ (last visited Dec 14, 2013).

Ten experts also mentioned concerns about the efficacy of transparency. They felt transparency would not be effective if users were not interested in nor had the time to learn about or read privacy policies. When discussing privacy notices, AD2 stated that many consumers would reject notices, "They don't want a bunch of disclosures and notices and stuff that either they don't understand or they don't particularly care about. I think there is a percentage of people who do care a lot about that [...] [b]ut I think the majority of people don't want to click through all that stuff." G1 had a similar statement, "there is always going to be either a majority or a super majority of these folks who simply aren't going to read the stuff and aren't going to take the time to compare anyway." AC2 stated a similar concern about balancing the right amount of information on small screens with consumers' limited attention, "This is a tension for us, as user interface designers too, which is we can put in a lot of nuance in terms of what's going on, but how much will people actually read?" CA1 put it bluntly, "I don't know what [a link to a privacy policy] gets you because no one reads the damn things."

Best Security Practices: Eight experts said app developers should be following known best security practices. SE2 posited that secure code was the foundation for protecting users' privacy and security: "If you don't have a secure application you can't guarantee privacy at all. It's impossible. If I write the most awesome privacy preserving software... there's a bug in my code and somebody can exploit my software and make it eavesdropable, ...that's completely useless. So I think building secure code is the foundation of all privacy and data control." Examples of secure code given by experts include using SSL and proper encryption of data.

There are resources for app developers on developing best security practices. These include guidelines on mobile web from a standards consortium,[67] and guidelines for each platform from the platform developers.[68]

AP1, an app developer, recommended that app developers create a privacy policy as part of best practices, "In fact, the generation or creation of a privacy policy is something that often leads to more insight about your product. The developer might view the creation of a privacy policy as something for his customers, but in fact its real value is for himself and his developer team, or herself and her developer team."

---

[66] CALIFORNIA DEPARTMENT OF JUSTICE & PRIVACY ENFORCEMENT AND PROTECTION UNIT, PRIVACY ON THE GO: RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM.

[67] MOBILE WEB APPLICATION BEST PRACTICES, W3C Recommendation 14 December 2010, http://www.w3.org/TR/mwabp/

[68] Guidelines for iOS developers are available at from Apple at "INTRODUCTION TO SECURE CODING GUIDE" https://developer.apple.com/library/ios/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html,
Guidelines for Android developers are available at "BEST PRACTICES FOR SECURITY & PRIVACY" http://developer.android.com/training/best-security.html

Priority: Seven experts said that app developers may not make privacy and security a priority, but they should. Some explained this as a lack of resources. For example, PL1 said, "[App developers] are working with very few resources and they're trying to develop complex applications in very short time frames in order to try to make some money."

AC1 had a similar explanation, "I think often privacy and security is one of the things they plan to do. It's on a later day, and their primary or their first order of concern is to get a running app that does something valuable, and they're gonna think about things like privacy and security much later, perhaps when they make money or otherwise are more successful."

Through interviews with and surveys of app developers, Balebako et. al found app developers did not prioritize privacy and security, and found in particular that smaller app companies were less likely to exhibit privacy and security best practices.[69]

Data Minimization: Five stakeholders, including both of the app developer stakeholders, discussed the need to minimize the data that was collected. SE2, a lawyer, put it succinctly, "Don't ask for privileges you don't need. It's a liability." AP1, an app developer, said, "If the developer or the application or the carrier isn't collecting the information, then no potential security risk exists if the information is leaked because there's nothing to leak. That often is referred to as data minimization. Data minimization is a way to use privacy to try to enhance security. If I don't have it, I can't leak it."

Understand Third-Party Libraries: Five experts discussed that app developers often use third-party libraries, Application Programmer Interfaces (APIs), and code toolkits. App developers should reveal to users what data is collected by these third parties, but they often do not, in part because developers themselves may not know what information is being collected by this code. G1 said, "App developers really need to be aware. And some app developers weren't really good at this and some don't give it a second thought.... When they are using widgets or modular pieces of code or third-party services in order to provide portions of their app, that they need to pass on those disclosures concerning those which are modular pieces of code and third-party services to the users."

L2 felt that third-parties had a responsibility to disclose their data collection practices. "It would be good for third parties who collect a lot of information through apps to put up a kind of standardized notice so information can be sent along and populate the little short privacy notice that ideally the mobile apps will provide." Other experts thought that app developers maintained responsibility for understanding third-

---

[69] REBECCA BALEBAKO, ABIGAIL MARSH, JIALIU LIN, JASON HONG & LORRIE FAITH CRANOR. THE PRIVACY AND SECURITY BEHAVIORS OF SMARTPHONE APP DEVELOPERS, Workshop on Usable Security 2014

party code. Balebako et. al found that app developers did not always read or understand the terms of service or privacy policies of the companies or tools they used.[70]

Customer Relationship: Five experts said that app developers need to understand the role of privacy and security in their customer relationships. Often, this was tied to the need for transparency. PL1 said, "App developers need to understand that users will partly choose to use their app or not use their app based on whether they trust them. And they need to make sure that they do the right things in order for users to trust them. So a lot of that, again, comes down to being upfront with the user in terms of what an application is doing and why." G2 stated that app developers, unlike the platform developers, have a more direct relationship with the user and therefore had increased responsibilities to be transparent, "because app developers have a direct relationship with users. They need to be able to utilize that direct relationship. So, especially when they're dealing on the sensitive data, financial apps, kids' apps."

AP1 emphasized that this is more an issue of trust than privacy: "Trustworthiness is a category under brand, and so having an educated populace that sees your product as more trustworthy because it provides either better control or limits stuff. You never ever, ever will ever make money selling privacy."

Interventions by Platform Developers

Several themes emerged when we asked experts what platform developers or OS providers should be doing to protect the smartphone user from harm. Typically, platform or OS developers are also app store providers.

- Transparency (17 experts)
- Improve UI Control (10 experts)
- Security Improvements (7 experts)
- Work with App Developers (6 experts)

Transparency: Seventeen experts argued for more transparency about data sharing from platform developers. Three experts were concerned about location sharing (AC1, L1 and G2). L1 suggested that location should have a notification every time it was shared. L1 was also concerned about sharing the phone's unique id.

Several experts emphasized that telling users what permissions were being used was not sufficient, but they also needed to know why, how often, and where data was being shared. AP2 said, "There should be a clear statement about what's collected, why it's collected, and who it's shared with... And I think there should be clear benefit

---

[70] *Id.*

statements about what benefit the consumer receives, paired up with the what, why, and with whom." AC2 said, "It'd be nice if it could just sort of categorize, 'We're using your data for this reason.' It'd also be nice if it could say how often it's doing it too, like is it doing it automatically or is it doing it in the background every five minutes or so on? So these are things that right now there's no easy way of trying to determine."

Suggestions for improving transparency in the user interface included the app store and the operating system itself. Two experts suggested just-in-time notifications (AP1 and CA1). AC3 also discussed the need to develop notifications for smaller mobile devices. "You can't just take what kind of works from the desktop, throw it on to the platform with totally different visual characteristics and pretend that it's going to work. It doesn't even work for expert users. What hope do regular users have?"

However, many experts expressed doubt about whether users want additional notices, and whether users would be willing to read or learn enough to understand them. P19 said, "It's probably a good practice to allow consumers access to that information when they want it but not in a way that undermines the experience of the app itself. People come to the app to use the app, not to read about a bunch of information practices that really won't impact them."

Improve UI Control: Ten experts suggested that platforms should improve the privacy and security controls in the user interface (UI). Two experts said that both a simple set of controls and a more fine-grained set of controls should be available. SE2 explained, "The OS vendors have to be really careful to provide for the people that don't wanna think about it by securing things as best they can by default. Then provide the cues for people who wanna dig into it a little bit and maybe make a more informed risk decision."

Three experts said they would like to see a "do not track" setting implemented, or that they believed it would be implemented, although one was concerned that do not track was still not defined.[71]

Security improvements: Seven experts said that platforms should also implement security best practices. These best practices were considered to be well known, but some experts offered specific advice. SE2 said, "OS developers can protect their software that they're building and figure out what people want for security and privacy and do that by default." G1 suggested remote wiping: "The remote wiping is a use case that happens all the time, and it's something that third-party apps provide." AC1 mentioned the need to push out security updates: "So many Android phones are in an insecure state because the carriers aren't pushing out OS updates."[72]

---

[71] The W3C web standards body has a working group chartered to define Do-Not-Track for the web, which has been on-going since 2011. See http://www.w3.org/2011/tracking-protection/

[72] see ACLU Android FTC Complaint, http://www.aclu.org/files/assets/aclu_-_android_ftc_complaint_-_final.pdf (last visited Dec 15, 2013).

Eight experts mentioned that finding and removing malware from app stores was an important part of platforms' role in protecting users. For example, AC2 said, "One thing they could do is try to find this malware faster or do better testing and all, and I know they are trying to do that too." AC3 said, "All of the markets, the major markets, are pretty vigilant in keeping the absolute worst stuff out and they have strong financial incentives to do that."

Work with App Developers: Six experts said that platforms should provide app developers with tools and education to enable improved privacy and security. Stakeholders said that solutions could include more example code for security (AC3), making it easier to implement security features such as SSL (AC2), better toolkits (AC2), a security checklist (AC2), and enabling app developers to be transparent (SE2) by giving them tools to let users know about apps' data requirements.

The platform industry stakeholders agreed with this. PL1 said, "I think one thing that we can do as an industry is make it easier for developers to secure their applications and give them tools and libraries to do that, because if we expect developers to put in the time and the effort necessary in order to create their own security, they're often going to mess it up. Or in most cases, honestly, they just won't do it at all because they don't have the time to and they don't have the incentives to." PL2 said, "Every app developer should be doing privacy by design. But I think realistically, the other players have more resources to raise privacy awareness... than the app developers."

AP2 said that responsibility needed to be shifted from just the app developers to the platforms as well, "Shared responsibility would lessen the burdens on apps, and actually would assign responsibility for developing private tools and notices, and helping educate consumers, and helping consumers achieve the goals that they set out to when they use the phone. [This is] better than leaving all the responsibilities for app developers themselves. And so I consider it a systemic failure that we're all experiencing right now."

Nothing: Only one participant thought platforms had no room for improvement. AD2 said "I think actually in some ways that they're more restrictive than they could be with respect to data sharing in a way that undermines competition and probably limits offerings to consumers."

C. Role of Government

Seven experts said the government can aid in mitigating risks and harms, and five of them brought up government intervention without being explicitly asked about government's role. However, not all experts were asked about the role of the government; this theme emerged naturally through the interviews. The interviewer specifically asked the government stakeholders what they perceived as government's role in mitigating risk, but other interviewees were not asked.

The two government representatives, G1 and G2, thought that any policy should be sensitive to company needs and innovation. G2 said that the government should "promote ways for companies to work together to come up with good practices. It helps the marketplace in general and trying to convince companies that working together to do that with government is gonna be more successful than just hearing about these cases of the bad actors." G1 was concerned about how to set up regulation that did not stifle innovation, "So government has to walk a really fine line as it does in many areas in terms of technology between imposing responsibilities to ensure that consumers are protected, while at the same time promoting innovation in the space."

Suggestions from other stakeholders included new regulation, promoting best practices, intervening when companies do not meet security best practices, working internationally, and developing standardized notices. CA2, a consumer advocate and participant in the NTIA process, described the NTIA MSH goal: "To develop a code of conduct or mobile apps to cover so-called transparency. Which is a very limited approach and only is one." CA2 also felt that, "What's needed is the FTC to promulgate regulations and legislation passed by Congress to empower users to opt in to all this data collection and use."

One stakeholder (TE1) expressed concern that the legislative process did not allow the time or communication needed to understand the technical details and create a quality standard. This stakeholder emphasized that self-regulation efforts within industry allowed the companies to "get technical input and to really get into the nitty-gritty of the words and what they mean in a way that's impossible in a legislative environment. You know, [in a legislative environment] you might have one meeting with the bill sponsor that you can maybe make one point. You can't wordsmith a document… So it's just unlikely to be timely and effective when it's done through legislation."

Several stakeholders felt that policy should not be focused on app developers but on other stakeholders, such as data brokers, platforms, and app stores. AP2 wanted to see limitations on data and collection and use by data brokers and advertisers, saying, "while we spend a lot of time publicly debating what apps should be doing, we've spent almost no time discussing and debating limitations on those other entities and their data usage." AC1 specifically supported the California Attorney General's approach in attempting to "police the elephants – the carriers – rather than all the little mice who are making these apps."

Many of the experts we interviewed were at the time of the interview participating in a government led process, the NTIA MSHP on mobile transparency. Therefore their views are likely somewhat reflective of their opinions on that process. There is likely a correlation between participating in a government process on mobile transparency and believing that government processes can be useful but difficult.

D. VULNERABLE POPULATIONS

In order to understand whether specific interventions are needed for different groups, we asked experts what populations are most vulnerable to harms from smartphone data sharing. We also asked experts whether any of the harms discussed were different for children. Most agreed that harms were different for children. As PL1 said, "Adults are generally more aware of the long-term implications of their actions, whereas children don't necessarily have that same level of awareness. AC1 and AD1 said that teenagers might be more sensitive to social embarrassment or bullying. PL2 said that children might not be as vulnerable to financial exploitation since they have fewer financial resources. Obtaining parental consent was discussed as a difficulty for apps. Several experts mentioned that parents were also vulnerable to mistakes made by their children while using their parent's phone.

We also asked if there were any vulnerable populations besides children. Thirteen experts cited the elderly, but some noted that not all elderly are vulnerable. Experts mentioned that some elderly may be less technologically savvy, may have trouble seeing small screens, or may have trouble manipulating small devices. Notice and choice interventions may need to take into account such needs.

Other vulnerable populations mentioned were: battered women, mentally or emotionally disabled, visually disabled, those living in countries without due process, members of the military who would be at greater risk if their location was revealed, those in financial situations where they can't purchase apps without advertising or technological protections, groups that were not previously exposed to PC technology, those with language barriers (e.g. non-English speaking in the US), and minorities who could be unfairly targeted for unhealthy or undesirable products.

F. INTERVENTIONS AND THE PRIVACY PRINCIPLES

We looked at how the interventions discussed by experts related to the FTC's Fair Information Practice Principles.[73] Several interventions are related to the notice and choice principles. Security was also frequently mentioned as an intervention. Experts did not frequently mention the other two principles: participation and enforcement. In addition to notice, choice, and security, data minimization was also mentioned. Data minimization is not part of the FTC's principles, although it is part of other sets of fair information principles, including the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.[74] The security principle described by the FTC

---

[73] FEDERAL TRADE COMMISSION, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE, A REPORT TO CONGRESS (2002).

[74] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980).

focuses on preventing unauthorized parties from accessing data, while data minimization includes reducing the amount of data collected, even by authorized parties. Some experts stated that data minimization is a part of security best practices. We highlight data minimization as a separate category as experts found it to be an important intervention.

Principles	Interventions		
	By users	**By app developers**	**By platform developers**
Notice	• Education	• Transparency • Customer relationship	• Transparency
Control			• Improve control
Security	• Protect phone • Play in the lighted streets	• Best security practices • Prioritize security and privacy • Understand APIS	• Security • Work with app developers
Data minimization	• Reduce functionality	• Data minimization • Understand APIs	

TABLE 3: INTERVENTIONS GROUPED BY WHO IS RESPONSIBLE AND WHETHER IT WILL LEAD TO IMPROVED NOTICE, CONTROL, SECURITY, OR DATA MINIMIZATION

WE SHOW HOW EACH INTERVENTION RELATES TO A PRIVACY PRINCIPLE IN

Principles	Interventions		
	By users	**By app developers**	**By platform developers**
Notice	• Education	• Transparency • Customer relationship	• Transparency
Control			• Improve control

Security	• Protect phone • Play in the lighted streets	• Best security practices • Prioritize security and privacy • Understand APIS	• Security • Work with app developers
Data minimization	• Reduce functionality	• Data minimization • Understand APIs	

Table 3. We further explain the categorizations below. Some interventions fall into several categories. For example, app developers making privacy and security a priority could lead to improved notice, control, and data minimization. Making privacy and security a priority is a prerequisite for most of the other interventions, and recognizing the importance of customer relationships is an incentive to improve privacy and security.

Notice: Notice about data sharing can be improved through transparency, education, or standard notices. Notice may lead to improved user decision-making. Users who educate themselves are paying attention to notices and other available information, and can make more informed choices about the data they share. App developers and platforms have a role in improving transparency and providing better notices.

Notices should go beyond stating what data was shared, and should include purpose and secondary uses, and also take into account third-party libraries. Several experts said notices about data collection should include why data is collected and with whom it will be shared. Notices providing this information can help to reduce surprise from unexpected data sharing and embarrassment caused by data sharing, while also helping users understand why some data uses are necessary. Including notices about the data practices of third-party libraries will help insure that the notices provided by apps are complete. Platform providers should provide tools that will assist in conveying notices in a standardized format.

We also recommend user education about malware. The greatest risks come to users from malware. Some experts indicated that users should use only apps from well-known companies, but this may discriminate against legitimate but less well-known companies. Smaller app companies may desire a way to indicate trustworthiness. While the major platforms are taking steps to scan their app markets for malware, there may be room for a notice or indication that an app has been scanned and can be trusted.

Control: Control over data sharing can be improved by making existing controls more usable and by adding additional controls. While control does not necessarily imply

notice – it is possible to add control through new interfaces that users don't see or don't understand – we assume that control options would be well implemented and usable, and that the user understands the control mechanisms.

Platforms could provide better control, allowing users to make decisions according to their privacy and security preferences. This could mitigate privacy concerns, stop location monitoring (which can lead to stalking or physical harm), allow users to turn off behavioral advertising, and control resource usage.

Security: Two user interventions can improve security: 1) users can protect the phone so that others will have less access to it or the information within, and 2) playing on the lighted streets could result in fewer malware downloads, and data shared with fewer malicious third-parties. Many of the app developer mitigations, including best security practices, data minimization, and understanding APIs, can improve security. This in turn can reduce the risks of data reaching unintended audiences, reducing harms such as physical harm, surveillance, financial harm, and social problems. Platforms can work with app developers to improve security practices. Security in the platform or app store could lead to less malware, fewer data breaches, less unencrypted data transmittal, and fewer coding mistakes that allow unintended transmission of data. Therefore, security can mitigate the most harmful risks.

Data Minimization: Data minimization requires sending, collecting, and storing the minimum amount of information that is needed. When users choose to reduce functionality, they will trade some usability or functionality in order to share less information, which minimizes the data shared. Data minimization also addresses many of the same harms as security. If there is less data to transmit and protect, there is less chance of unauthorized access. If the authorized data collector's purpose in collecting data is to profile and to make decisions about the consumer, financial and health discrimination may result. Reducing collected data may help prevent the discrimination, as there is less information to create profiles.

VI. LINKING THE MITIGATIONS TO THE HARMS

In this section, we analyze the relationship of the risks and harms to each of the FIPPs discussed above. We classify how the harms identified by the experts can be mitigated through notice, control, security, or data minimization. As Table 4 shows, most harms are not mitigated through notice or control alone, but require security and data minimization. We explain these classifications and provide examples.

The harms that can be mitigated by notice alone – social problems and embarrassment, or privacy – tend to be highly personal. In these cases, users can reduce the risk of harm by changing their behaviors, such as not installing an app, or not posting

information. In these cases, notice of the data sharing or collection may suffice and may be the only appropriate mechanism.

Other harms can be mitigated if users have both notice and control over the data collection or sharing. In these cases, notice is an important pre-condition for control, but the control itself allows the user to make the decision that mitigates the risk. For example, users may be able to specify with whom data is shared through a control. We illustrate this through the scenario of a woman who is concerned that an abusive ex-partner will stalk her if he has access to location information. She could share her location with friends who might be concerned about her, but could disallow the abusive ex-partner from accessing the location information. In this example, control allows the user to apply their personal or situational information to mitigate harms, while still taking advantage of the benefits of information sharing.

Some risks cannot be addressed by notice and control. In these cases, there may be a malicious party, or a party motivated to act against the interest of the user. The malicious party may circumvent notice and choice, deliberately hiding their access to information or preventing the user to control the data sharing. For example, a party that is interested in causing financial harm to the user will try to do so in a way that the user cannot control through notice or control. Similarly, discrimination is not likely to be an explicit option from which users can opt-out. In these cases, users are not able to mitigate the harm. As most app developers are not trained in security and privacy[75] and are thus unlikely to put much effort in implementing security or privacy features, platform developers are probably in a better position to protect users as long as this protection does not encourage users to switch to other platforms (as it may happen if users felt annoyed by added, unusable privacy or security interfaces). Hence, these harms should be mitigated through security (not allowing malicious users to get access to the information by protecting the data with encryption), or data minimization (not creating or storing data).

	Notice	Control	Security	Data minimization
Social Problems and Embarrassment	X	X	X	X
Privacy Concerns	X	X	X	X
Behavioral advertising	X	X		X

[75] Balebako et al., Op. Cit., "The Privacy and Security of Smartphone App Developers".

Surveillance and Monitoring	X	X	X	X
Physical harm		X	X	X
Stalking		X	X	X
Harm to society			X	X
Direct financial harm			X	X
Financial discrimination				X
Resource Usage				X
Health discrimination				X

Table 4: Harms mitigated by notice, control, security, or data minimization. In cases where both notice and control are needed, we show control as a mitigation, as notice alone would not suffice.

We classify discrimination as being mitigated only by data minimization, we assume the party collecting the data is motivated by interests that contradict the smartphone owners' best interest, resulting in a possible harm. Price discrimination may result in corporate profit but consumer loss. Security won't protect the user, as the party that causes harm may have unmitigated access to information, regardless of best security practices protecting the data from access from other parties. Price or product discrimination is likely to be perceived as harmful even by users who wish to receive targeted ads. For example, in September 2000 an Amazon's customer discovered that if he removed the cookies in his computer, he obtained consistently a lower price for a DVD that was offered to him.[76]

If users are informed about behavioral advertising, they can use various tools to opt-out of advertising[77]. In those cases in which users do not want to receive targeted ads

---

[76] CNN Law Center, "Web sites change prices based on customers' habits", http://edition.cnn.com/2005/LAW/06/24/ramasastry.website.prices/. Retrieved on April/3/2014.

[77] Some work has found that these tools could be more usable and clear to users. See PEDRO GIOVANNI LEON, BLASE UR, REBECCA BALEBAKO, RICH SHAY YANG WANG AND LORRIE FAITH CRANOR. "Why Johnny Can't Opt Out: A usability evaluation of tools to limit online behavioral advertising." In *Proceedings of Computer Human Interaction*. ACM, 2012. Other work has investigated whether the existing notifications are effective, finding that the current AdChoices icon could be improved. See PEDRO GIOVANNI LEON, JUSTIN CRANSHAW. LORRIE FAITH CRANOR, JIM GRAVES, M. HASTEK, BLASE UR, G. XU. "What Do Online Behavioral Advertising Privacy Disclosures Communicate to Users?" Workshop on Privacy in the Electronic Society (WPES). October 2012.

and are not given a mechanism to opt out of data collection, data minimization is the remaining mitigation option.

To summarize, notice alone may help mitigate harms only in situations in which users have control. Notice and control can be helpful to mitigate harms in the cases when there is not a malicious party who is motivated to circumvent notice and choice.

VI. WHY IS PUBLIC POLICY FOCUSED ON TRANSPARENCY?

In previous sections we argued that in some common scenarios, harm to users cannot be mitigated by notice and choice alone: in those cases the amount of data collection should be minimized, and access to collected data by second or third parties should also be reduced. Six experts recommended that app developers implement best security practices for protecting user data, and seven experts suggested that platforms implement security practices such as pushing system updates to users frequently and monitoring the app stores for malware. Five experts specifically mentioned that app developers minimize the data collected. While most experts also identified transparency and notice, either by app developers or platforms, as a necessary mitigation, ten experts also discussed the concerns about relying on notice and the difficulty in getting user attention on privacy policies. The question then becomes why public policy is currently focusing on notice and choice, as opposed to mitigating the most risks through security and data minimization.[78]

There seem to be three reasons that policy currently focuses on transparency. These are: transparency is perceived as easy to implement, transparency is perceived as a non-technical issue, and transparency shifts the responsibility on the user. We discuss each of these below.

The NTIA MSHP chose to address transparency as the first consumer privacy protection, as it was perceived as "discrete enough to be addressed in a reasonable period of time."[79] This indicates that designing alerts to users about data usage and sharing is perceived as the low-hanging fruit. However, this may also indicate an ongoing lack of awareness of the need for user studies and designing for understanding. Indeed, the NTIA MSHP did create a code of conduct with recommended user messages, but the usability of these messages was shown to be lacking.[80] In 2002 the director of the Bureau

---

[78] For this analysis, we assume that the policy-makers are interested in protecting the consumers, and don't have vested interest in insecure data collection. While this assumption may not hold for some governmental bodies, such as the NSA, we believe this to be true for the branches of administration, such as the FTC, that have been investigating smartphone privacy.

[79] Lawrence E. Strickling, Putting the Consumer Privacy Bill of Rights into Practice (2012), http://www.ntia.doc.gov/blog/2012/putting-consumer-privacy-bill-rights-practice (last visited Dec 15, 2013).

[80] Rebecca Balebako, Richard Shay & Lorrie Cranor, *Is Your Inseam a Biometric? A Case Study on the Role of Usability Studies in Developing Public Policy* WORKSHOP ON USABLE SECURITY (2014)

of Consumer Protection highlighted the need to develop privacy notices that could be understood by users.[81] Eight years later, the Federal Trade Commission still complained about privacy notices being "incomprehensible."[82] Therefore, we are concerned that the perception that transparency is an easy problem to address may be misplaced.

Notice is considered a non-technical issue, in contrast to secure handling of data or data minimization. Stakeholders, including policy makers or lobbyists for technical companies, may be concerned that intervening in technical areas may stifle innovation. Calo describes notice as being an alternative to law, along with code and nudges. He posits that regulators may choose notice as they "do not need to undertake the difficult, costly, and politically challenging task of telling firms exactly how they should run their businesses."[83] We suggest that policy bodies turn to standards-setting bodies or consult with expert consultants for technical expertise.

Transparency puts the responsibility on the consumer to reduce risk through his or her own decisions. Notice is consonant with the principles of autonomy and beneficence, and these principles have guided several policy discussions, such as cigarette or pharmaceutical regulation.[84] However, these principles have also been used to shift liability and responsibility from the industry to end consumers.[85] While this may work for well-known products and services where it is clear what people can do to prevent harm, it does not work well for things like apps in smartphones, as the mitigations available to users are not always clear.[86]

Policy makers should recognize that the "easy" problem of transparency is not easy, and does not mitigate the major risks. Notice by itself does not guarantee user comprehension; notice without comprehension might lead to the habit of acknowledging information that is not even read. This problem is aggravated by the lack of formal training in privacy of most app developers, their lack of awareness of governmental guidelines concerning privacy and security, and their low appreciation of data

---

[81] Remarks by Howard Beales, Dir. of Consumer Protection, on Privacy Notices at the FTC Privacy Agenda, January 2002. Cited on Op. Cit., Cranor, "Necessary but not sufficient", 2012, p. 278.

[82] Op. Cit., Cranor, "Necessary but not sufficient", 2012.

[83] RYAN CALO, CODE, NUDGE, OR NOTICE? (2013).

[84] David Egilman & Susana Rankin Bohme, *A Brief History of Warnings, in* HANDBOOK OF WARNINGS (Michael S. Wogalter ed., 2006).

[85] Susana Rankin Bohme & David Egilman, *Consider the Source: Warnings and Anti-Warnings in the Tobacco, Automobile, Beryllium, and Pharmaceutical Industries*, in HANDBOOK OF WARNINGS (Michael S. Wogalter ed., 2006).

[86] Popescu et al. argue that lock-ins and exit costs in the mobile ecosystem prevent users from making choices (p 279-282) to protect their privacy, and that even when opt-out mechanisms exist, they do not allow users to express their full range of preferences (p 278-279). Mihaela Popescu & Lemi Baruh, *Captive But Mobile: Privacy Concerns and Remedies for the Mobile Environment*, 29 THE INFORMATION SOCIETY 278, 278-282 (2013).

minimization and privacy policies.[87] Good policy on data minimization may require expertise, and will require action by app developers and platforms.

VII. CONCLUSIONS

By interviewing experts from many stakeholder groups, we were able to get a holistic perspective of the harms and concerns to users from smartphone data sharing, and how they can be mitigated. The experts identified a number of harms from smartphone data sharing. These harms included tangible and direct harms such as financial harm and physical harms. They also included less direct harms such as behavioral advertising and embarrassment. In order for users to continue enjoying the benefits of smartphones, it is best to mitigate the risks of the harms.

Experts identified a number of mitigations that users, platform developers, app developers, and regulators could implement. We classified these mitigations as providing notice, control, security, or data minimization, and provided evidence as to how some of the most harmful problems cannot be addressed by notice alone. The interventions that improve security and minimize data collection mitigate the most harmful risks, such as financial, physical, and social harms.

By focusing only on Notice and Choice, existing policies fall short at addressing the problems identified by experts in our study. Most experts mentioned transparency as the main intervention for both app and platform developers; however, this is a necessary but not sufficient condition to protect users' privacy.[88] While notice may help to address social problems and those risks that are most readily identified as privacy-related, most harmful problems cannot be addressed by notice alone. This is due partly to the flaws of notice (requiring user attention). In other cases, increased control is needed for users to act on the notice. Finally, some harms stem from malicious parties who will deliberately circumvent user notice and control. While notice and user education is a precondition for better control and better decisions by the user, the focus of future policy and efforts should include security, control and reduced access. We encourage app developers, platforms, and policy-makers to enlarge their efforts to include best security practices and data minimization.

---

87 Balebako et al., Op. Cit., "The Privacy and Security of Smartphone App Developers".

88 Cranor, Op. Cit., "Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice".

VIII. Appendix

A. Interview Script

Thank you for agreeing to participate in this interview. As you have read in the consent form, your participation is voluntary. All your responses will be kept anonymous. You may stop the interview at any time. We will be recording the audio of the interview for transcription.

Do you have any questions about the process before we begin?

I have turned on the audio recording. Please confirm you are ok with being recorded.

- What is your professional title and industry?
- Tell me a bit about your background and expertise.

I'm doing research on the risks of data flowing from smartphones, with the end goal of designing better user interfaces so users can make informed decisions. In particular, I'm interested in the harms, risks, and privacy concerns that could occur from smartphone data sharing. I'd like your thoughts on how harms can occur and what the smartphone user can do to prevent them. I am also interested in privacy concerns, which may not involve physical or financial harm, but that a smartphone user would find uncomfortable or undesirable. I will be asking about what users can do or need to know to prevent harms and risks. If there is information they need but don't currently have access to, please include that in your response.

- How would you define data sharing from smartphones, in terms of what the data is and where it goes?
- What harms could come to smartphone users from data sharing? [Expert should brainstorm list of harms]
- To recap, you've mentioned the following harms [interviewer repeats harms mentioned]:

I have some other harms that have been mentioned in research and by smartphone users. I'm mentioning these to help with brainstorming.

Please feel free to add to this list or object to any items on the list.

- Malicious apps stealing financial information
- Apps sharing location information leading to stalking
- Business sharing their data sets that then becomes de-anonymized
- Data breach leading to financial harm or identity theft
- Apps sharing behavioral information with social circles, leading to embarrassment or problems with friends and family
- Un-encrypted data sent over a public network, leading to stealing of financial or sensitive information
- Premium texting or downloading unwanted software

Do you have any more to add?

I'm interested in categorizing the harms into two lists: the most harmful and the most likely. Of all the harms we discussed, which are the most likely.

- Which ones could cause the most damage or harm?
- My mother just got a smartphone. What should she do and what does she need to know to prevent this harm?
- How should the smartphone interface or OS change to protect her?
- What should an app developer do to prevent the harms or concerns?
- What should regulators or public policy be doing to mitigate the risks? [Question only asked explicitly of government stakeholder]
- Are any of these harms or concerns different if children are involved?
- Are there any other vulnerable populations?
- Looking forward 5-10 years, what will change when it comes to privacy and security?
- That concludes my interview questions. What questions do you think I should have asked, or should ask future experts?
- Is there anything else you would like to add