Information Asymmetry Meets Data Security:

The Lemons Market for Smartphone Apps

Margaret W. Smith

This article examines the market for smartphone applications (commonly called "apps") with the goal of assessing current information asymmetry about app security and consumer privacy. It also reviews signaling as a potential policy intervention designed to address information asymmetry. Given the rapid growth of the app market, comparisons can be drawn between the market for smartphone apps and a market for lemons, as commonly found in a developing economy that lacks structured quality-control mechanisms. Despite growing concern over personal data collection and how these data are used, traded, and/or sold, the public remains relatively uneducated about and either ignorant of or apathetic toward privacy concerns when downloading apps to their smartphones. Incorporating simple security cues—similar to the "star" scale used in consumer reviews—is one example of a signaling mechanism that could help address the information asymmetry in the app marketplace.

This article first examines similarities between the smartphone app market and George A. Akerlof's classic lemons market. The goal is to expose the lemons market for app security—to simplify the scenario, an app will either be secure or insecure. Regular consumers do not have full information and therefore make purchases without knowing if an app is secure or insecure. Next, the article investigates how average consumers make decisions about cybersecurity and whether addressing the information asymmetry in the app market will alter decision making. Finally, it suggests incorporating a simple, icon-based security signal to reduce the information asymmetry and discusses the potential impact of such a policy.

DISCLAIMER: The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

THE SMARTPHONE APP MARKET

Smartphones are everywhere. Bright screens display tiny mosaics of multipurpose apps that provide everything from online banking services to entertainment. Similar to the software market, app security is extremely varied and not transparent to shoppers. An information asymmetry exists in the app market with regard to privacy and security: the average consumer does not understand user agreements, privacy permission levels, or how to locate information about an app's security. Further, any customer agreements are often so lengthy and jargon-filled that users ignore them.

A general lack of regulation in this area is also at fault. The Federal Trade Commission (FTC) maintains an online tip sheet for app developers suggesting they take a proactive approach to app development that begins with a thoughtful look at security (FTC 2017a). However, FTC guidelines are not binding, leaving security choices in the hands of developers and insecure apps in the market. The result is a common manifestation of information asymmetry that Akerlof (1970) refers to as a "market for lemons," with sellers that possess greater knowledge about app security, consumers that cannot distinguish between secure and insecure apps, and an industry without a designated party responsible for setting security standards.

To explore the smartphone app market, this article substitutes security for quality, generating two types of apps: secure apps (good ones) and insecure apps (bad ones). The choice to download is therefore a cost-benefit analysis that weighs the benefits (security) with the costs (personal information or data exfiltration). However, both costs and benefits in this situation are relatively unknown to consumers who, as the data subjects, have less information than the developers or data holders regarding the purposes and conditions of future use of their data (Akerlof 1970, as cited in Acquisti et al. 2017). Even large, public companies such as Facebook have obscure features that confuse consumers about how the app uses their personal data. While testifying before Congress in early 2018, Facebook CEO Mark Zuckerberg firmly stated that the company does not access a phone's microphone to listen to private conversations. However, he followed up by explaining how Facebook can access a phone's audio when a person records video content for use on Facebook (Goode 2018). Zuckerberg's statement, intended to be exhaustive and clarifying, reveals how data-gathering technology has become more sophisticated while permissions have remained obscure and confusing for end-users (Goode 2018).

Data ownership confounds the problems further: consumer data can be bought and sold like any other commodity. An extreme—but deeply concerning—example is the recent Cambridge Analytica (CA) scandal that also involved Facebook. CA, a voter-profiling company, harvested data, without users' permission, from millions of Facebook profiles and used it to predict and influence voter patterns in U.S. elections (Rosenberg et al. 2018). The data allowed CA to devise social media targeting tactics for the 2016 presidential election by exploiting private users' social media data on behalf of its clients, most notably the campaign of the Republican nominee Donald

Trump (Rosenberg et al. 2018). The buying and selling of data unbeknownst to the consumer furthers the information asymmetry because individuals do not know who has access to their personal data or how it is being used.

In his paper, *The Market for Lemons,* Akerlof (1970) presents the conditions required for a lemons market: the presence of an information asymmetry, incentives to present all goods as quality goods, a lack of a credible means to share or disclose information, low-quality average goods, and a lack of quality assurance guarantees. The app market exhibits these conditions in the following manner:

- ***Information asymmetry.*** It is extremely difficult for consumers to compare apps based on security. Currently, online app marketplaces such as Apple's App Store or Google Play do not offer shoppers a comparison tool for privacy or security. Both stores control their own "app ecosystems" but rely heavily on app developers to follow the established guidelines (Goode 2018). In both cases, for an app to work, it is required to meet the current Android operating system and Apple iOS basic functionality requirements (Goode 2018).

- ***An incentive for all sellers to portray their app as secure.*** There is no signaling mechanism for security. Aside from comments regarding security or privacy found in consumer reviews, buyers must search for product information on company websites (if they exist) to identify any concerns. Companies do not market apps for security but incentives do exist to avoid being labeled or reviewed as insecure, since downloads increase with positive consumer feedback. Because it is difficult for the average consumer to "see" how an app uses their personal data or to know what phone features an app has access to, developer or seller incentives are geared more toward functionality than security.

- ***A lack of a credible disclosure technology.*** A permissions model allows a consumer to opt-in or opt-out of privacy levels. The permissions model is further discussed below but, in general, it refers to the process by which consumers control the capabilities or information an app can access on the user's device.

- ***Low app security on average.*** Sellers, or data holders, want consumer information for a variety of reasons and since strong incentives to secure this data do not exist, most apps remain insecure. Personal data can be used for good or bad purposes. For example, researchers at Carnegie Mellon University investigated the top 100 Android apps and found that more than half used device ID, contact lists, and/or location (Carnegie Mellon University 2013). Surprisingly, the team discovered that apps unrelated to mapping or other location-based services collected location information, citing Dictionary.com and Angry Birds as two examples. Some apps use

the collected information for benign purposes (e.g. internal research) but often, unbeknownst to consumers, apps will sell or share their data with online marketers.

- ***A lack of effective quality or security assurance guarantees.*** Once the consumer downloads the app, he or she is stuck with the results and it is extremely difficult to regain control over personal data once it is released. Regulations do not effectively cover personal data security and sellers' responsibilities regarding that data.

In general, consumers should have clear and complete information at the time of purchase for a market to function efficiently and, based on the comparison above, the smartphone app market exhibits a true information asymmetry with regard to information security and privacy.

Interestingly, upfront information is provided in the app market: apps use a permissions model designed to support informed choice and address the information asymmetry (Momenzadeh & Camp 2017). Choices made via the permissions model either permit or prevent an app from accessing user data and phone functions. However, most buyers do not understand the model, so it fails to support security-conscious decision-making. The model relies heavily on an individual's understanding of the costs associated with specific choices and how to compare and contrast the security tradeoffs presented within the model (Momenzadeh & Camp 2017). The average consumer cannot do this without significant time or cognitive effort—which most are unwilling or incapable of spending—leaving buyers and their data at risk (Acquisti et al. 2017).

According to Akerlof (1970), "[t]here is considerable evidence that quality variation is greater in underdeveloped [areas] than in developed areas" (496). The app market is relatively new and unregulated, leading to the wide variation in security one would expect in a lemons market. The FTC, for example, has published privacy guidelines for healthcare apps (discussed in greater detail below) to inform app developers of the federal laws related to users' private health information that might apply to their product (FTC 2016a). Ultimately, however, apps are created to provide a service and consumers rate them on functionality, not security or privacy.

Importantly, app price is not an indicator of security. Price can suggest a more thoughtful and thorough development process, but an expensive app can still pose significant privacy risks to the consumer due to the user-input requirement of the permissions model. Such cases result in lemons problems because superior technology is costlier to produce than inferior technology, but consumers have no way of knowing whether the costlier alternative is also the better and more secure alternative, compared with the cheaper alternative (Cordes 2011; Akerlof 1970). Given that peer reviews sway purchasing decisions, the choice to download an app, on average, is not based on privacy or security considerations but instead on popularity (Kelley et al. 2013).

SECURITY AND PRIVACY DECISIONS ARE NOT SIMPLE

Modern technologies are constantly evolving, leaving everyday users in a state of incomplete information despite their best efforts to remain informed (Acquisti et al. 2017). Constant evolution means new apps are being developed and introduced into the market regularly. A May 2015 report by Google found the top factors influencing users' choice to download a new app to their phone were "price" (82 percent), "ratings and reviews" (60 percent), and "recommended by others" (33 percent) (Google 2015). However, Google did not include factors related to security or personal data protection as options for survey participants to select in describing what influences their download choices. Interestingly, in the Google study, "familiarity with company/brand" garnered a 24 percent response rate suggesting that brand signaling is also a factor. Another earlier study also showed that "people make privacy judgments … based on a company's name, but not necessarily based on its privacy practices" (Ur et al. 2012 as cited in Acquisti et al. 2017, 6).

Ultimately, it is difficult for app buyers to determine how much of their personal data will be collected upon purchase and how the seller might use that data—the vulnerabilities for the consumer remain unclear. The challenge for consumers is that the tradeoff associated with privacy decisions in the permissions model is multifaceted and highly nuanced (Acquisti et al. 2017). These problems, according to Acquisti et al. (2017), "are exacerbated by the inherent uncertainty, and sometimes ambiguity, associated with the tradeoffs involved in privacy and security choices, where laxer settings may be key to unlocking additional functionalities and to deriving (seemingly) more value from a given system" (2).

Why do the majority of people ignore permissions when making decisions about app purchases? Research has tried to understand how people make online security decisions in an effort to make privacy interfaces more accessible and usable for regular consumers (Sasse et al. 2001; Cranor & Garfinkel 2005; Garfinkel & Lipford 2014 as cited in Acquisti et al. 2017). In one study (Felt et al. 2012), only 17 percent of participants reported having paid attention to permissions and only 3 percent answered the three permission comprehension questions correctly. Felt et al.'s findings suggest that Android permissions warnings do not actually help users make security decisions. Other studies found as few as 7 percent or 8 percent of people looked at permissions before making the decision to download an app (Momenzadeh & Camp 2017; Rajivan & Camp 2016). In contrast, a separate study found that 74 percent of people, when asked, claimed to be comfortable with their level of understanding of the app permissions model (Harris et al. 2015 as cited in Momenzadeh & Camp 2017).

People overlook app security for a number of reasons. Kelley et al. (2013) discuss how app download counters in app marketplaces act as the major decision factor for consumers. Morton (2014) also investigated this social cue in his article, "All My Mates Have Got It, so It Must Be Okay," and found that despite an overall concern

for privacy, people believe widespread downloading of an app indicates that it has an acceptable level of security (Morton 2014 qtd. in Momenzadeh & Camp 2017). Additionally, people are cognitive misers and will not engage with a security solution or permissions model unless it is simple, concise, and easy to use (Acquisti et al. 2017; Forget et al. 2016). However, other research finds the average person remains relatively unconcerned about security and is willing to accept risk if it means they can get the desired service (Harris et al. 2015 as cited in Momenzadeh & Camp 2017).

An alternative view, one that acknowledges the information asymmetry in the market, is that people *do* care about security, but lack the necessary information to make informed decisions. Studies found that providing consumers with upfront information about security levels or privacy permissions improves their decision making (Milne & Culnine 2004; Wechsung & Möller 2014). Finally, Tsai et al. (2011) found that consumers are willing to pay a premium for privacy and respond to cues on websites that indicate the site's security level. These studies show support for the idea that, given simple visual cues or information nudges, people will change their behavior.

INFORMATION NUDGES CAN INFLUENCE BEHAVIOR

One possible intervention in the apps market that could improve security outcomes for consumers is the nudge. Nudges are policy approaches that maintain freedom of choice while simultaneously steering individuals in a particular direction. Often considered paternalistic, Sunstein (2014) emphasizes that the real point of nudges is to make life easier by simplifying tough choices. For example, Sunstein uses the example of global positioning system (GPS) navigation to describe nudging, explaining that a GPS device will instruct a driver to take the shortest and most direct route to their destination but the driver remains free to choose their own course.

Default rules are considered one of the most effective forms of nudging and hold potential for app security (Sunstein 2014). Establishing a baseline app security requirement or default security posture to ensure some level of data protection removes the time consuming and burdensome task from the consumer. However, as the FTC notes, an alarm clock app has different security needs than a social media app. As a result, there is no standardized baseline level of security for apps; they vary in purpose and as a result, the security features vary as well (FTC 2017a).

Due to the expansive nature of online services, technology users make security tradeoffs every day—even accepting a friend request on Facebook is a basic security choice. Providing upfront and clear information to consumers about these choices can arm them to make better purchasing decisions, bridging the information asymmetry in the market (Acquisti et al. 2017). Bhargava and Lowenstein (2015) discuss "Privacy and Information Disclosure" in their paper, *Behavioral Economics and Public Policy 102: Beyond Nudging,* and suggest that any informational nudging approach to online security should be expressed in a simple, standardized fashion designed to raise consumer awareness and understanding. There is evidence that displaying security

and privacy information can influence purchasing behavior: in one study, Kelley et al. (2013) created a simulated app marketplace and displayed app security information on the site, which led participants to alter their download selections.

However, Bhargava and Lowenstein (2015) also warn that a stronger approach to security might be required—such as regulations on how companies can use consumer data—and that educational nudging should be used in conjunction with other policy mechanisms aimed at security and not as a stand-alone solution. Regulating how companies use personal data protects consumers by taking the onus off them and their selected privacy settings—companies are instead regulated by law. Educating buyers and augmenting the permissions model with a visual security cue is a desirable goal. However, increasing awareness and information does not guarantee that consumers will achieve their stated preferences or maximize their welfare when making privacy choices (Acquisti et al. 2017). Ultimately, no matter how useful or salient information is, consumers can easily ignore it without changing behavior.

Consumers with hyperbolic preferences—i.e. those who prioritize immediate benefits or rewards over future benefits or rewards—are particularly unlikely to trade instant functionality for security and privacy. If a buyer with hyperbolic preferences wants to download an app, the future risk of data exposure is unlikely to sway their decision; they are more likely to choose to play the game today despite the risks of privacy concerns tomorrow. Additionally, the context of online privacy and security presents a unique challenge because the benefits of making "smart" security decisions are often intangible or difficult to measure in the near term. Therefore, nudges or any soft paternalism approaches could simply be ignored because immediate behavioral feedback is lacking.

IMPLEMENTATION AND POTENTIAL IMPACTS

Using the coercive powers of government to discourage or interfere with private action requires justification (Weimer & Vining 2011). In the case of mobile app security, public decision-makers should be willing to give up some market efficiencies to protect consumer privacy and to promote fairness in the market by minimizing information asymmetry with regard to mobile app privacy and security (Weimer & Vining 2011). Inadequate security also has implications for the economy. Makridis and Dean (2018) found a negative association between data breaches and firm outcomes; however, they also caution that because the United States does not have mandatory breach notification rules, the "requisite evidence is not available for econometric analysis" to make causal claims (21). The list of press releases related to mobile technology on the FTC's website (FTC 2017b) suggests that app security is a problem and that consumers are targeted for lax permissions settings that allow access to their personal data—security lapses that could be prevented by informing consumers or implementing a universal standard. The addition of a visual cue to inform potential buyers about an app's security is an example of a "nudge" or "soft paternalism" since the act does not impose a decision on the consumer but rather attempts to bridge

information asymmetry in the market to "guide users' decisions towards safer, better choices" (Acquisti et al. 2017, 11). The goal is to prompt the consumer to think about the security risks associated with the app before downloading it without requiring the buyer to actually *do* anything.

To address the information asymmetry, the FTC must propose industry standards for app security. For this to be effective, apps would be required to include a simple, visual cue—for example, a red star indicating an insecure app; a green star indicating a secure app; a yellow star indicating the app, previously rated green, is undergoing recertification after an update or patch—in their marketing description to let potential buyers know *by sight* if the app meets FTC standards. Naming the FTC as the organization to designate, update, and maintain the standards is consistent with the agency's current role in consumer protection and mobile technology. In April 2016, the FTC released a new, web-based tool for developers of health-related mobile apps (FTC 2016a). The purpose of the online tool is to make developers aware of any federal laws and regulations that might apply to their apps—specifically, the data their apps could generate, store, or share (FTC 2016a). As this example illustrates, the FTC is already capable of creating and maintaining app security recommendations.

The process also requires a certification agency to grant apps a red, green, or yellow star rating and to manage the recertification process when an update or patch is released. The U.S. Department of Agriculture's (USDA) "Certified Organic" food labeling requirements can be used as a model for this process. To be granted "Certified Organic" status and permission to use the USDA organic logo on food products, a farmer must apply for certification from a USDA certifying agency (typically a trade union). Due to the lack of a software developer trade union, *Consumer Reports* is an example of an independent body with the ability to test apps against FTC standards, recommend ratings, and distribute labels in a uniform, consistent manner for a fee. Since this is an informational issue, using a third party concerned with consumer safety for certification is acceptable and will minimize any delays associated with waiting for a government body to take action.

Adding security-related cues to the app marketplace is a mitigating effort and not a full solution to the lemons problem. Eliminating the entire information asymmetry to create fully informed customers is difficult because information security is complex, nuanced, dynamic, and favors the developer. The biggest challenge is that technology changes rapidly and requires consumers, even professionals in the field, to mimic a medical field-like thirst for current best practices. For a consumer to remain current on information and data security, they would have to proactively access, absorb, and adopt new information, procedures, and techniques as the field develops—similar to how a medical doctor remains current on procedural techniques. For the average consumer, this level of interaction or research is impractical and unlikely. The red, green, or yellow star method is a simple, consumer-agnostic cue to prompt better choices—it is a quick, digestible piece of information about a product that alerts consumers to a potential security risk without requiring any action from that consumer.

To be effective, security cues need to be simple, easy to use, and noninvasive, or a customer is likely be overwhelmed by the information and ignore it (Acquisti et al. 2017; Forget et al. 2016). The signaling method proposed is a small but necessary step toward creating a more transparent app marketplace that influences the consumer side of the market and is better than taking no action to correct the current information asymmetry.

However, requiring developers to submit apps for review could also prompt a change in developer or production-side behavior. Currently, developing security into a program—as an organic process—is rare. Security is often an afterthought, laid on top of an app or program's functionality after ensuring basic Android or Apple iOS interoperability. The proposed security certification process could prompt developers to keep apps out of the market until FTC standards are met and prompt an industry shift toward "baking in" security rather than continuing the retroactive process. Both actions will further mitigate the app market's information asymmetry.

At the same time, apps, because they are software, require updating or patching on an ad hoc basis. Creating a security certification generates a major market inefficiency: What happens when an app publishes a patch? Does the app restart the certification process? Ideally, the answer is yes, an app requires recertification whenever an upgrade or patch is released to maintain certification integrity. However, allotting certification expiration dates to create a time-based recertification requirement (annually, biannually, or monthly) is likely more feasible. The yellow star rating, proposed by this paper, is only granted to apps that initially maintained a green star rating but require recertification due to a new edition, upgrade, patch, or expiration. Without a recertification requirement, a developer could easily release an app with a green star security rating and then release a malicious update. To maintain integrity in the process and the FTC standards, this type of activity must be prevented. However, recertification may also prompt developers to delay and clump updates to avoid paying multiple recertification fees. Patch delays are concerning since vulnerabilities present opportunities for exploitation. Delays of any sort are against industry best practices because they put consumers at risk.

Another concern associated with this approach is the impact a new, FTC-guided rating scheme will have on the smartphone app market as a whole. To fund the effort, *Consumer Reports*, or the named certifying body, must charge a certification fee. To enter the marketplace, an app would be evaluated against FTC standards and the developers would pay a fee for the app's security rating prior to offering their product for sale in the marketplace. This process will have several impacts on the app market. First, the certification requirement will slow the app development process thereby slowing down an entire market that is characterized by fast-paced new offerings. This could prompt a greater investment in development, as discussed above, or it could discourage potential developers from generating new products to avoid paying additional certification fees. Also, raising the average consumer's security awareness could change the composition of the entire marketplace by pushing unsecure insecure apps out of the market and curbing the spontaneous creativity that defines it.

CONCLUSION

This article analyzed the information asymmetry in the market for smartphone apps and discussed implementing a visual cue to bridge the knowledge gap with regard to security and privacy concerns. Much of this paper reviewed how average consumers make online security choices and how signaling, as a potential policy intervention, with standards set by the FTC and managed by an independent third party, could positively influence consumer behavior in the app market. Much of the literature discussed the factors that go into security and privacy choices, methods to positively influence buyers' decisions, and how information nudges can drive choices for greater security.

Despite growing concern over personal data collection and how it is used, the public remains relatively uneducated on privacy concerns when downloading apps to their smartphones. Incorporating simple security cues, as suggested in this paper, is a positive step, but an incomplete solution to the information asymmetry in the app marketplace. Future work should focus on the possibility of regulating how companies use consumer data and on creating educational programs embedded into school curriculums that emphasize the importance of security to grow a generation of online consumers that understand the risks associated with app use and developers that consider security an essential part of the production process.

REFERENCES

Acquisti, Alessandro, Idris Adjerid, Rebecca Balebako, Laura Brandimarte, Lorrie Faith Cranor, Saranga Komanduri, Pedro Giovanni Leon, Norman Sadeh, Florian Schaub, Yang Wang, and Shomir Wilson. 2017. "Nudges for Privacy and Security." *ACM Computing Surveys (CSUR)*, 5 (3): 1-41.

Akerlof, George A. 1970. "The Market for 'Lemon'": Quality Uncertainty and the Market Mechanism." *The Quarterly Journal of Economics* 84 (3): 488-500.

Bhargava, Saurabh, George Loewenstein. 2015. "Behavioral Economics and Public Policy 102: Beyond Nudging." *American Economic Review* 105 (5): 396-401.

Carnegie Mellon University (CMU). 2013 "Are Apps Ratting You Out?" Carnegie Mellon University. Accessed March 11, 2019. https://www.cmu.edu/homepage/society/2013/spring/apps-ratting-you-out.shtml.

Cordes, Joseph J. 2011. *An Overview of the Economics of Cybersecurity and Cybersecurity Policy.* Washington, DC: George Washington University. https://cspri.seas.gwu.edu/sites/g/files/zaxdzs1446/f/downloads/2011-6_economics_and_cybersecurity_cordes_0.pdf.

Federal Trade Commission (FTC). 2016a. "FTC Releases New Guidance for Developers of Mobile Health Apps." FTC, April 5, 2016. https://www.ftc.gov/news-events/press-releases/2016/04/ftc-releases-new-guidance-developers-mobile-health-apps.

---. 2016b. "Mobile Advertising Network InMobi Settles FTC Charges It Tracked Hundreds of Millions of Consumers' Locations without Permission." FTC, June 22, 2016. https://www.ftc.gov/news-events/press-releases/2016/06/mobile-advertising-network-inmobi-settles-ftc-charges-it-tracked.

---. 2017a. "App Developers: Start with Security." FTC. Accessed March 11, 2019. https://www.ftc.gov/tips-advice/business-center/guidance/app-developers-start-security.

---. 2017b. "Mobile Technology Issues." FTC. Accessed March 11, 2019. https://www.ftc.gov/news-events/media-resources/mobile-technology.

Felt, Adrienne P., Elizabeth Ha, Serge Edelman, Ariel Haney, Erika Chin, and David Wagner. 2012. "Android Permissions: User Attention, Comprehension, and Behavior." Proceedings of the Eighth Symposium on Usable Privacy and Security, Washington, DC.

Forget, Alain, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, and Lorrie F. Cranor. 2016. "Do or Do Not, There Is No Try: User Engagement May Not Improve Security Outcomes." Paper presented at the Twelfth Symposium on Usable Privacy and Security, Denver, CO.

Garfinkel, Simson and Heather R. Lipford. 2014. *Usable Security.* San Rafael, CA: Morgan & Claypool Publishers.

Garfinkel, Simson and Lorrie F. Cranor. 2005. *Security and Usability.* Sebastopol, CA: O'Reilly.

Goode, Lauren. 2018. "App Permissions Don't Tell Us Nearly Enough about Our Apps." Wired, April 14, 2018. https://www.wired.com/story/app-permissions/.

Google. 2015. "Mobile App Marketing Insights: How Consumers Really Find and Use Your Apps." Google. Accessed March 11, 2019. https://think.storage.googleapis.com/docs/mobile-app-marketing-insights.pdf.

Harris, Mark A., Amita G. Chin, and Robert Brookshire. 2015. "Mobile Application Installation Influences: Have Mobile Device Users Become Desensitized to Excessive Permission Requests?" *Proceedings of the Twentieth Americas Conference on Information Systems* (AMCIS 2015): 13-15.

Kelley, Patrick G., Lorrie F. Cranor, and Norman Sadeh. 2013. "Privacy as Part of the App Decision-Making Process." *SIGCHI Conference on Human Factors in Computing Systems*: 3393-3402.

Makridis, Christos A. and Benjamin Dean. 2018. *Measuring the Economic Effects of Data Breaches on Firm Outcomes: Challenges and Opportunities.* Stanford University Working Paper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3044726.

Milne, George R. and Mary J. Culnan. 2004. "Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don't Read) Online Privacy Notices." *Journal of Interactive Marketing* 18 (3): 15-29. http://www.sciencedirect.com/science/article/pii/S1094996804701085.

Momenzadeh, Behnood and Jean Camp. 2017. *Technical Report TR736: Peeling the Lemons Problem with Risk Communication for Mobile Apps.* Bloomington, IN: Indiana University. https://www.cs.indiana.edu/cgi-bin/techreports/TRNNN.cgi?trnum=TR736.

Morton, Anthony. 2014. "'All My Mates Have Got It, so It Must Be Okay': Constructing a Richer Understanding of Privacy Concerns, an Exploratory Focus Group Study." I*n Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges,* eds. Serge Gutwirth, Ronald Leenes, and Paul de Hert. Berlin: Springer Verlag.

Rajivan, Prashanth and Jean Camp. 2016. "Influence of Privacy Attitude and Privacy Cue Framing on Android App Choices." Paper presented at the Twelfth Symposium on Usable Privacy and Security, Denver, CO.

Rosenberg, Matthew, Nicholas Confessore, and Carole Cadwalladr. 2018. "How Trump Consultants Exploited the Facebook Data of Millions." *The New York Times*, March 17, 2018. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?module=inline.

Sasse, Martina A., Sacha Brostoff, and Dirk Weirich. 2001. "Transforming the 'Weakest Link' — a Human/Computer Interaction Approach to Usable and Effective Security." *BT Technology Journal* 19 (3): 122-131. https://search.proquest.com/docview/215204902.

Sunstein, Cass R. 2014. "Nudging: A Very Short Guide." *Journal of Consumer Policy* 37 (4): 583-588. http://nrs.harvard.edu/urn-3:HUL.InstRepos:16205305.

Tsai, Janice Y., Serge Egelman, Lorrie F. Cranor, and Alessandro Acquisti. 2011. "The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study." I*nformation Systems Research* 22(2): 254-268. http://www.guanotronic.com/~serge/papers/isr10.pdf.

Ur, Blase, Pedro G. Leon, Lorrie F. Cranor, Richard Shay, and Yang Wang. 2012. "Smart, Useful, Scary, Creepy: Perceptions of Online Behavioral Advertising." *Proceedings of the 8th Symposium on Usable Privacy and Security*: 1-15.

Weimer, David L. and Aiden R. Vining. 2011. *Policy Analysis*. Boston, MA: Longman.

MARGARET SMITH is a second-year PhD student in the public management field. Maggie is an active duty U.S. Army Cyber Officer with over 14 years of experience as both an enlisted Soldier and commissioned Officer. She earned her commission and Master of Public Policy with a focus in Homeland Security and Intelligence Policy at Georgetown University's McCourt School of Public Policy. She is a trained senior watch officer, cyberspace operations planner, offensive cyberspace operations mission commander, and will take a position at the United States Military Academy's Army Cyber Institute following Trachtenberg. Maggie is currently investigating how technology is changing women's contributions to violent extremism and women's connectivity to violent networks.

ACKNOWLEDGEMENTS

The author would like to thank Dr. Gerald Brock, for whose course she wrote this paper. For their thoughtful feedback and guidance, she thanks Editor-in-Chief Marissa Esthimer, Associate Editor Andrew Miller, and her faculty reviewer, Dr. Joseph Cordes. She also thanks her spouse, Patrick, and her daughter, Emily, for their support of her academic pursuits. Lastly, she thanks the Trachtenberg School for their confidence in her abilities.