f i ® s t m ¤ ñ d @ ¥
PEER-REVIEWED JOURNAL ON THE INTERNET

Oversharing the super safe stuff: "Privacy-washing" in Apple iPhone and Google Pixel commercials

by Angela M. Cirucci

Abstract

Inspired by the ever-evolving concerns surrounding data privacy, this study analyzes Apple's and Google's ads for their iPhone and Android devices, respectively, as well as each company's privacy policies. Findings via critical discourse analysis reveal that the ads conflate privacy with security, relying on powerful imageries that depict the phones as safes from which data cannot travel. These depictions, however, do not align with the policies that provide separate sections for privacy and security. With these findings in mind, I propose a widespread adoption of "privacy-washing" to promote a newfound literacy of granular data types.

Contents

Introduction

In late 2019, a Pew study found that more than half of the U.S. population believe they cannot move through life without having their digital data collected and shared, citing a lack of understanding and control (Auxier, *et al.*, 2019). Thus, it is not surprising that two leaders in the production of smartphones in the U.S. — Apple and Google — seized the opportunity to advertise their popular products — iPhone and Pixel — through a privacy and security lens. The goal of this paper is to explore how Apple and Google responded to the growing concerns around digital privacy through the analysis of two recent commercials — Apple's Oversharing ad for iPhone and Google's Super Safe Stuff Securer ad for Pixel — as well as the companies' privacy policies.

Findings indicate that Apple and Google conflate "privacy" and "security" as well as sidestep complete definitions of data, including explicit data but excluding implicit, aggregated, and inferred data. I argue that,

through their ads, the companies rely on socially held expectations of privacy, delivering powerful metaphors of social hacking and phones acting as safes, allegedly letting no data leave the physical devices. In reality, their policies include that data freely flow to and from the phones, both natively and via-third parties, but these processes are deemed not important to discuss because aggregated and inferred data are not considered "personal."

Through this analysis, I suggest a widespread adoption of a term coined herein — "privacy-washing." "Privacy-washing" occurs when companies attempt to promote privacy friendly policies to deflect attention from their less privacy friendly activities as well as to influence customer choice, relying on widely held assumptions about who they are as brands more broadly. The concept of "privacy-washing" includes the explicit discounting of dynamic definitions of privacy (social and institutional) as well as confusing or ignoring one or more types of data (explicit, implicit, inferred, and aggregated). It also works to promote the uncoupling of privacy and security.

Digital privacy

It is no secret that a multitude of studies has attempted to explore, understand, and define digital privacy. Definitions of privacy are intertwined with varying levels of perceived and desired control (*e.g.*, Trepte, 2021). Indeed, a traditional definition of privacy is the right to control personal information (Moore, 2008). But privacy may also be extended to include the managing of others' information as well (Petronio, 2013). Privacy also is often also entangled with debates surrounding anonymity; the two are often taken to be interchangeable. However, while privacy is the right to control who knows what, anonymity is the unlinkability of these bits of information.

It is widely argued that the more that users have the agency to control their data online, the more privacy they will experience. Yet as digital technologies become more advanced, controlling networks and data flows becomes increasingly difficult (Trepte, 2021). Many governments around the world have enacted privacy regulations that rely on "informational self-determination," often implemented via notices or consent statements, like privacy policies or terms of service. These documents are supposed to inform the user about data flows, and then the user can make an informed decision. But much research has shown that current practices of obtaining consent are deeply flawed. Most documents are too long and too complex and do not actually guide users to understanding potential future use or consequences [1]. People either do not read the policies, do not understand the policies, do not have enough background knowledge to make informed decisions, or are not offered a choice beyond take-it-or-leave-it (Gharib, 2012; Solove, 2013).

Another popular area of research regarding digital privacy is that a "privacy paradox" exists — users claim to care about their digital privacy, but then do not seem to follow best guidelines for keeping their information "safe" in online spaces (Barnes, 2006). Scholars have attempted to understand this "paradox," noting that perhaps users do not understand the risks involved (Acquisti and Gross, 2006) or how to protect their data (Hargittai and Litt, 2013). Popular social network sites, from MySpace to TikTok, fuel this hypothesis; users constantly post photos, thoughts, and locations (Hargittai and Marwick, 2016). Of course, other scholars have argued that no such paradox exists (*e.g.*, Solove, 2021).

As Raynes-Goldie (2010) explained, much of the confusion may be attributed to the fact that there are really two types of privacy online — social and institutional. While social privacy refers to all content that can be seen through the end-user interface (*i.e.*, by other end-users), institutional privacy includes stored data that are usually only accessible to those working for the collecting companies or building advertising campaigns. Most socially visible data are explicitly created data (information about an end-user that they have actively input) — profile pictures, tweets, posts, bio information, etc.

While institutional data include this content, algorithmic sorting and recommendations are more reliant on *implicitly* created data — data that end-users are constantly creating, but not knowingly. These include data like location, mobile battery percentage, if WiFi is turned on, what other phones are near an end-user's phone, and so on (Leith, 2021). Algorithmic processes are best at predicting the future, so *inferred* data are

an important third type of data. Some algorithms work to make guesses about end-users, taking in explicit and implicit data and outputting user characteristics (Hinds, *et al.*, 2020), which tend to be surprisingly accurate (*e.g.*, Youyou, *et al.*, 2015).

Multiple studies have found that, in practice, end-users are often more concerned with family, friends, teachers, and potential employers seeing certain content than what companies and governments may be collecting about them (Raynes-Goldie, 2010; Young and Quan-Haase, 2013). When privacy issues are trending, users are more likely to alter platform-provided or permitted "privacy tools" (boyd and Hargittai, 2010) including using pseudonyms, providing false information, limiting friends and followers, and reviewing tags and photos (boyd and Hargittai, 2010; Miltgen and Peyrat-Guillard, 2014; Young and Quan-Haase, 2013).

Yet, these methods are almost exclusively situated in social privacy and explicit data. It is rare that these tools touch on institutional privacy, namely implicit and inferred data. Further, platforms that are widely considered "social media" are the companies providing these tools. Services like Apple and Google, as discussed later in this section, rarely provide "privacy" tools because their "social" functionalities are much more limited.

Although users are making decisions about "privacy," these decisions are also often not well-informed. Privacy decisions have been found to be based on incomplete information. And, even if users had all information, research has shown that bounded rationality limits abilities to acquire, memorize, and process all the related information. Instead, users rely on inaccurate representations of companies' handling of data, largely influenced by social preferences and norms (Acquisti and Grossklags, 2005). Indeed, studies report no significant relationship between a concern for privacy and levels of online disclosure (Tufekci, 2008).

Importantly, while most studies about privacy focus on platforms and software, few focus on hardware and devices. Popular smart phone providers like Apple and Google also rely on data flows. In fact, they are privy to everything that happens through the phone, often with less visibility and fewer reminders for users. More broadly, Apple and Google are more than just smartphone companies. To begin with the latter, Google of course includes the popular search engine, as well as services like Gmail, the Chrome browser, and cloud services like Google Photos. Also relevant is Google's acquisition of powerhouse ad firm DoubleClick, approved by the U.S. Federal Trade Commission in late 2007 (Tene, 2008). Apple is more situated in selling hardware like phones and laptops but provides popular services as well including Apple Music and iCloud.

A few studies have explored Apple and Google data practices. For instance, regarding voice-based assistants Siri and Google Assistant, Vimalkumar, *et al.* (2021) found that users are more likely to have privacy concerns when they have apprehensions about the technology itself. But, if these perceived risks are addressed, their privacy concerns also diminish. Overall, users' trust in the company plays an important role.

Recently, Apple and Google launched APIs for developers to build COVID-19 contact tracing apps. These APIs use Bluetooth to access health status as well as user location. Not only are these APIs problematic due to socio-cultural gaps — lower socio-economic groups and older people are less likely to have smartphones with these capabilities but more likely to be most vulnerable to the virus — they also provide Apple, Google, and third parties with these data. Health and location data can then be used to make decisions about who should go back to work or who should have access to public spaces and services as well as make inferences about social relations, hobbies, and interests. Ultimately, it is important to remember that Apple and Google still have control of all the metadata associated with the apps that utilize their APIs (Sharon, 2021).

Specifically related to Apple and Google smartphones, Leith (2021) investigated what information was sent to Apple and Google. Just in the U.S., Apple collects about 5.8GB of data every 12 hours and Google about 1.3TB. The phones connect to the backend, on average, every 4.5 minutes, even when the phones are not

being used. Pre-installed apps and services are actively collecting and sending data, even if users have never opened them. For Apple, these include Siri, Safari, and iCloud. For Google these include YouTube, Chrome, Google Docs, Google Messaging, clock, and the Google Searchbar.

Every time the phones connect with the backends, they also verify IP addresses, and collect telemetry data (mobile carrier details, signal strength, battery level, volume settings, number of reboots, etc.). While seemingly benign alone, these data can be linked with other data Apple and Google have, so easy cross-references can be conducted linking usernames, e-mail messages, credit card information, and so on. An important point here is that all these processes are encrypted, so there is little to no social privacy (*e.g.*, hacking) concern. Instead, these invisible processes are salient institutional privacy concerns (Leith, 2021).

With the above in mind, it is perhaps more productive to argue that, instead of a privacy paradox, there exists a lack of understanding regarding social vs. institutional privacy as well as varying types of data (explicit, implicit, inferred). Previous research has shown that most users are only primed to think about social privacy. This makes sense since social privacy most resembles our expectations for privacy offline. But the confusion is perhaps compounded and exploited by digital conglomerates.

Against this backdrop, the current study analyzes two recent TV ads, one for Apple's iPhone and one for Google's Pixel. The goal is to explore how the two conglomerates depict privacy to the general public including how these depictions align with the companies' actual data policies. Thus, the research questions guiding this study are:

> *RQ1*: How do Apple and Google define "privacy" through their ads?
>
> *RQ2*: How do the companies' definitions compare to actual, exhaustive definitions of privacy?
>
> *RQ3*: How do these definitions compare to what is included in the companies' privacy policies?

Method

To answer these three research questions, I conducted a critical discourse analysis [2] (Fairclough, 1995) of two TV ads — Apple's Oversharing iPhone ad (which I will refer to as "Apple's ad") and Google's Super Safe Stuff Securer Pixel ad (which I will refer to as "Google's ad"). During multiple views, I took special note of themes surrounding social vs. institutional privacy. I then compared the advertisements' themes to Apple's and Google's privacy policies, as well as to overarching app permission norms and expectations.

The two ads

In Apple's 60-second ad, eight quick narratives show people awkwardly sharing information with strangers in different public settings. In one vignette, a person stands on a crowded bus and shouts "I browsed eight sites for divorce attorneys today!" In another, a person sits at a table in a crowded restaurant with two others and shares "On March 15th at 9:16 am I purchased prenatal vitamins and four pregnancy tests" (Figure 1). People around them are annoyed and look at the sharing person like something is very wrong. (For a complete transcript see the Appendix.)

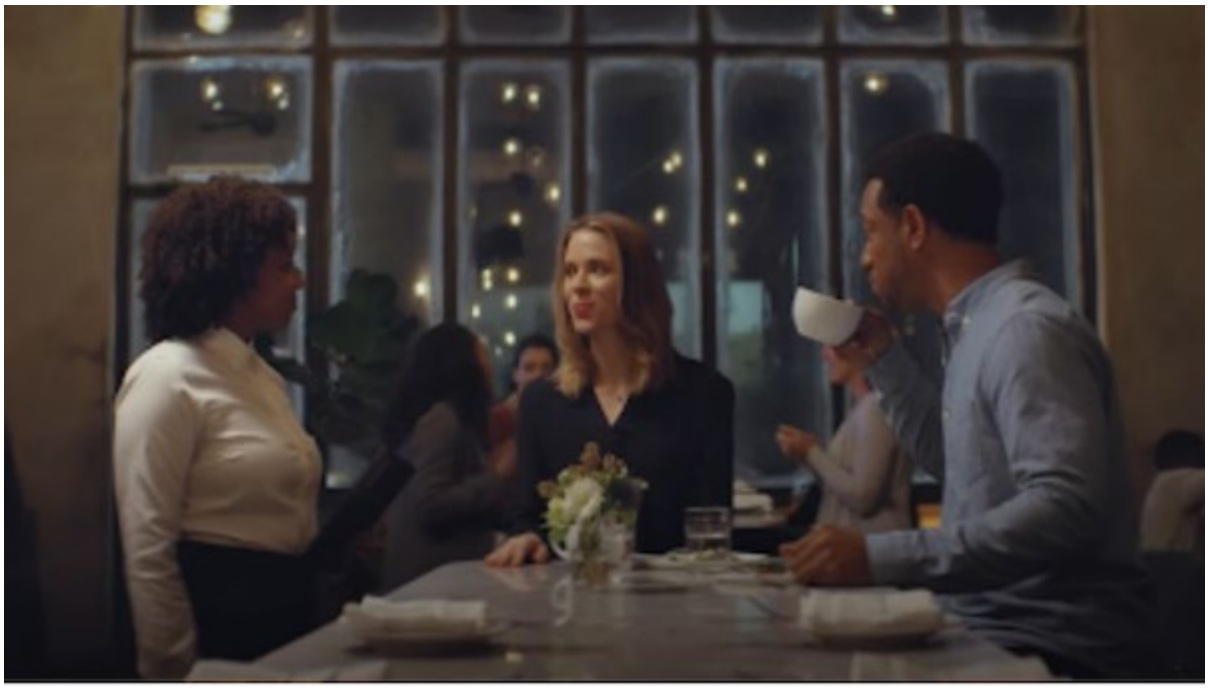

Figure 1: A person shares their online purchase history (0:37).

It is clear that Apple's vignettes are designed to conjure up specific types of data—search histories; login credentials; direct messages; download histories; location data; health data; buying histories; and credit card details. This also implicitly links to popular services including health trackers like Fitbit, shopping apps like Amazon, and messaging apps like Facebook Messenger. The ad attempts to persuade viewers that Apple's new iPhone ensures that private information stays that way.

In Google's 15-second ad, the back of the Pixel 5 is displayed as partially transparent, revealing a glowing green and black microchip attached to the main processing board (Figure 2). Introduced as the "Titan M security chip," the ad then shows a person securing multiple door locks and saying, "I don't mess around." The phone is labeled the "Super Safe Stuff Securer," and no further details are provided.

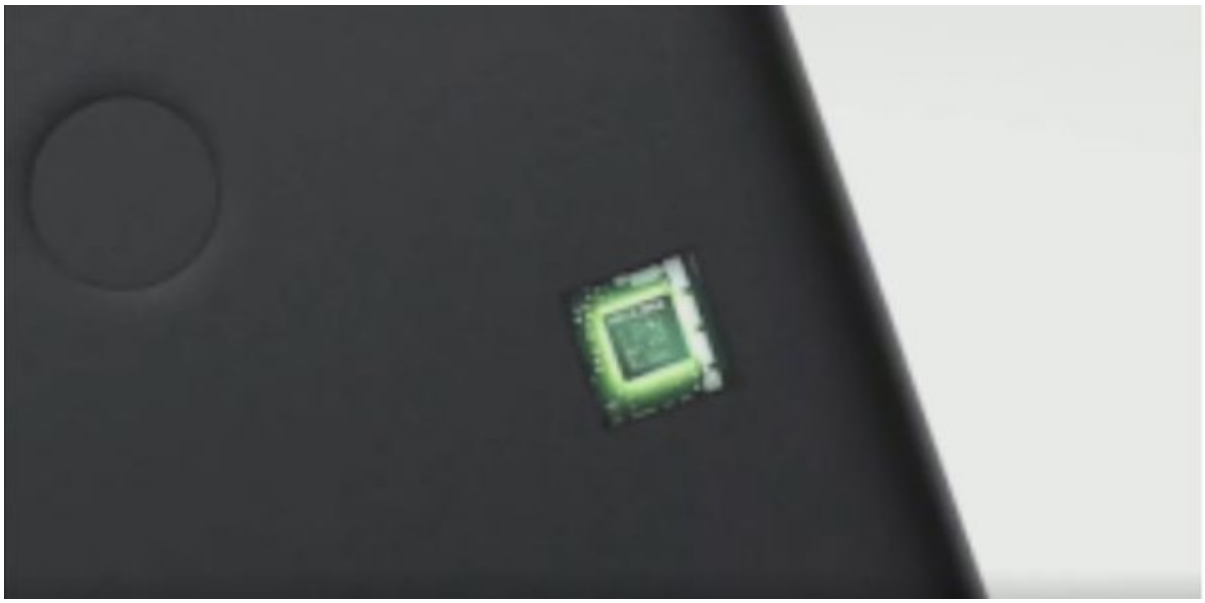

Figure 2: The Titan M chip glows beneath the Pixel's surface (0:03).

The policies

While their commercials attempt to portray a high level of "privacy," directly attributed to the phones themselves, Apple's [3] and Google's [4] data policies tell a different story. To begin, both Apple and Google have specific, more strict privacy policies when it comes to what they label "personal data." Directly identifying data like a user's name as well as indirectly identifying data, like a device ID, are defined as personal data. But aggregated and inferred data are not included under this umbrella. This is likely because the companies, in a sense, create these data on their own and thus feel the right to own and control these data in a different way.

Each policy has a lengthy section on the types of data that they collect. These include identifiers — like names, phone numbers, and device IDS; demographics — including age, gender, and language; commercial information — like payment information and purchase history; biometrics — including fingerprints and face detection; Internet activity information — like search terms and views and interactions with apps; health information — including physical and mental health conditions; fitness information; activity on third-party platforms; geolocation data; and inferences drawn from all the above.

Although the above is fairly exhaustive, how these data are used is much more difficult to decipher. Apple's policy states that it "does not use algorithms or profiling to make any decision that would significantly affect you without the opportunity for human review." Of course, this short statement elicits numerous questions including, how Apple defines "significantly affecting" their users and who is completing the human review. Google is slightly more transparent:

> Figuring out basic stuff like which language you speak to more complex things like which ads you'll find most useful, the people who matter most to you online, or which YouTube video you might like.

They label this as "personalized services" that include things like recommendations, personalized content, and customized search results. Importantly, both policies include that they do not have control over how third parties define, collect, or use data.

Interestingly, each policy has a completely separate section for security. These sections are much shorter and generally discuss encryption, reviewing data storage policies, and so on. Apple provides a separate page labeled “Apple Platform Security” that includes sections on hardware security — including an M1 chip that is very similar to Google’s Titan M; system security — relating to the startup process and software updates; encryption and data protection — to “enable remote wipe in the case of device theft or loss;” and app security — ensuring that apps are free of malware.

Google’s section is labeled “Keeping your Information Secure” and discusses how security is “built in” to “protect” information. They explain, “We work hard to protect you and Google from unauthorized access, alteration, disclosure, or destruction of information.” This includes aspects like using encryption while data are in transit and Safe Browsing and 2 Step Verification. Digging more deeply, Google’s “Safety Center” explains that the Titan M helps to protect users’ “most sensitive data,” handling encryption and verifying the operating system (OS) when the Pixel boots.

Discussion

Apple’s and Google’s ads are clearly meant to tap into the general public’s anxieties regarding *social* privacy. Apple’s quick vignettes display embarrassing social situations wherein users divulge personal information to other end-users with an air of obliviousness that implies they are unaware of their disclosures. Google depicts a person locking a door, implying a type of “keeping out” of other users. This reliance on only portraying the disruption of social privacy aligns with people’s offline privacy expectations and exploits overall illiteracy regarding implicit and inferred data.

Ironically, at least half of the data spoken aloud in the Apple commercial are actually implicit data — geolocation, search history, credit card details — data that rarely, if ever, would be shared socially with other end-users. The only exception is the case of “bad actors,” other end-users who are actively trying to hack these data. Social data included in Apple’s ad, like direct messages, are explicit data, but again would only be disclosed to unwanted parties in the case of a social privacy breach — someone accidently or purposefully sharing those messages with unintended end-users. Obviously left out of the Apple commercial are mentions of institutional privacy and inferred data. In addition, the end graphic of the iconic Apple logo becoming a lock paired with an iPhone literally blocking out the face of a person, suggest that the protected data live on the phone itself and thus the hardware is providing the protection.

Google’s shorter ad does, in fact, include the word “security.” It could be that including the word “security” clears up the notion that privacy and security are separate, or it could further promote that conflation, seemingly using the terms “privacy” and “security” interchangeably. Although the Google ad is more abstract, the physical locking of a door again implies that another person, or end-user, is coming for information that lives on the Pixel itself.

It seems that both companies use their ads to purposefully conflate privacy with *security*. Privacy involves the laws and regulations that require companies to protect user identity, but security refers to the *technical* method of protecting data (Herzog, 2016). Both ads indicate some technical method of protecting user data, specifically, as discussed more thoroughly below, what they would define as “personal data” and what most privacy definitions would denote as explicit and implicit data. This is more evident in Apple’s ad, but also creatively portrayed in Google’s ad — the person locking the door is aware that something needs to be protected in the first place.

This conflation can also be seen when the ads’ promoted definitions of privacy are compared to their privacy policies. The bulk of both policies discuss their definitions of data and how these data are used. However, they each have *separate* security sections that more closely align with the technologies presented in the ads. It is salient to question, then, why the delineation of privacy and security is so important that

they receive separate sections within the policies but are treated as interchangeable in the commercials.

The likely answer is twofold. First, while extremely sophisticated, the technologies that enable security are more objective and easier to maintain and upgrade than the everchanging privacy expectations and related legal discussions. Second, building large data repositories and using these to infer future user behaviors are critical to Apple's and Google's profit models. Thus, the two ads work to build trust around a more understood topic — security — and the policies work to focus on the slightly more protected "personal data" but not on topics like inferred data, aggregated data, and the flow of these data to third-parties.

Indeed, not considering inferred and aggregated data as sensitive ignores the full truth of data privacy. While much of the discussion is around "personal" privacy, aggregating and inferring data are the processes that are most likely to affect others (Bernal, 2020). Once "profiles" are created and matched to other users who are likely to behave in a similar way, ads, news content, political campaigns, and so on can be targeted to users with specific vulnerabilities and tendencies. This is exactly what we saw happen with the Cambridge Analytica scandal. The ability to target political messaging to users with specific fears was not due to collecting a lot of data about all those people. But, instead, the process was possible through, first, the collection of a lot of other data that were used to train a powerful algorithm. This algorithm could then identify the "types" of people that groups like Trump's 2016 presidential campaign team and the Brexit team were hoping to reach (Hinds, *et al.*, 2020).

The security sections of both ads discuss keeping apps within their respective stores free from malware, but this language also conveniently sidesteps the allowed, and numerous, flows of data to and from the phones at any moment. The blame here can of course be put on the user — every app includes its own data policy that users agree to upon download and installation [5]. However, because both the Apple ad and the Google ad focus on the phone itself as being a sort of safe, it is easy to incorrectly assume that *all* data on the promoted phones stay in the phone itself. By each of the ads putting so much emphasis on the physical phones, Apple and Google artfully circumvent true data flows to and from the phones, both natively and via third parties.

In both ads the work of keeping personal data private is put on the user. In Apple's ad, we see that the people shouting their personal information seem to not know how to control their privacy. Purchasing an iPhone is portrayed as fixing this control issue. In Google's ad we see a person heavily securing a door, actively working to control who can pass. Purchasing a Pixel is portrayed as synonymous with the control over door locks. Tapping into notions of control is powerful because research has shown that if users feel like they can control their data then they feel like it is private. However, as revealed through the data policy analyses, purchasing these phones has little to do with actual control of data flows, especially institutional data that move to and from the phone via Apple and Google themselves as well as multiple third-party apps.

Privacy-washing

As with data privacy issues, the public awareness of environmental issues is increasing. This leads to stakeholders taking some of these issues into consideration. In the U.S., and around the world, we have seen increased pressure for companies to disclose environmental performance and to provide environment-friendly products and services. Of course, what is disclosed is not always what it seems (Netto, *et al.*, 2020).

The term "greenwashing" was first coined by Westervelt due to hotels telling customers that if they did not ask for their towels to be washed, they would be helping conserve water (Netto, *et al.*, 2020). Today greenwashing is defined as the "practice of promoting environmentally friendly programs to deflect attention from an organization's environmentally unfriendly or less savory activities" (Netto, *et al.*, 2020). Companies are interested in both influencing consumer choices as well as perfecting their political strategies, but greenwashing can show up in many forms. Companies may selectively disclose environmental practices, deflect to minor issues to avoid concrete actions, and rely on largely held assumptions about their morals (Cislak, *et al.*, 2021; Netto, *et al.*, 2020).

Apple's and Google's lack of discussion around data flows and aggregated and inferred data paired with their seemingly purposeful conflation of privacy and security within their ads can be labeled as "privacy-washing." The companies are attempting to promote privacy friendly policies to deflect attention from their less privacy friendly activities. They are clearly attempting to influence customer choice as well as relying on widely held assumptions about who they are as brands more broadly.

Interestingly, Cislak, *et al.* (2021) found that national narcissism predicted the support of greenwashing campaigns. Large American companies like Apple and Google likely benefit from the same correlation. Users are not often primed to see, or want to see, Apple and Google themselves as bad actors, but instead perhaps imagine foreign countries or shady characters with illegal intentions as the ones collecting data. These perceptions are perfectly supported and validated through Apple's and Google's ads — we will protect you from people passing by on the street or attempting to break down your "door."

Although the term privacy-washing has shown up briefly in some Californian and Canadian law documents (*e.g.*, Jiminez, 2022), it has yet to make its way to academic analysis. They define privacy-washing as

> when a company advertises that it prioritizes data protection with its customer-facing products and services but neglects to actually implement best privacy practices to secure and minimize the processing of customers' personal information.

In 2020, the *Washington Post* published an article about Apple, Facebook, and Amazon "preaching privacy," describing privacy-washing techniques at the popular CES (Consumer Electronics Show) hosted each year by the Consumer Technology Association (Fowler, 2020). It is clear these trends exist across multifarious digital companies, but the widespread use of the term privacy-washing to both understand and investigate practices would prove helpful in not only research but explaining these tactics to everyday consumers.

Indeed, privacy-washing extends beyond the iPhone and Pixel. Recent news has revealed that Google is again being sued for promoting its "incognito mode" even though it does not protect users' data as advertised (De Vynck and Schaffer, 2022). Even beyond Apple and Google, privacy-washing can be seen on popular social media sites — Facebook, for instance, promotes socially facing privacy tools like the setting "only me." Users assume that a post or image is visible solely to them, but explicit and implicit data are still being collected from the post and flow to the relevant native and third-party repositories (Cirucci, 2017).

The term privacy-washing should be refined to include the explicit discounting of dynamic definitions of privacy (social and institutional) as well as confusing or ignoring one or more types of data (explicit, implicit, inferred, and aggregated). It should work to promote the uncoupling of privacy and security. "Privacy-washing" should also include the notion that controlling privacy should not be completely up to the user, especially when data policies are difficult to understand or companies provide only binary, take-it-or-leave-it, options. The term would then prove helpful in data literacy efforts as well as legal disputes and political campaign promises.

Conclusion

As increasing data privacy issues are brought to light, digital companies feel the strain to promote that they keep their users' data private. In the U.S., most users' conceptions of privacy only focus on social privacy, aligning with offline possibilities and expectations. However, online information is shared both socially (with other end-users) and institutionally (with the native platform as well as third parties). These data also come in varying forms — explicit, implicit, aggregated, and inferred. Although largely outlined in data

privacy policies that users "agree" to when downloading and installing apps, there is little understanding of how data flow and are then analyzed and repurposed to support profit models, target ads, and build political campaigns.

Through an analysis of Apple's and Google's commercials for their iPhone and Pixel, respectively, this study found that the companies purposefully conflate the concept of privacy with security. While privacy involves the laws and regulations that require companies to protect user identity, security refers to the technical method of protecting data (Herzog, 2016). Both ads argue that the phone itself acts as a sort of safe that keeps user data from leaving. But, upon analyzing their data policies, how they define security is separate from their definitions of privacy including lengthy definitions of "personal data." In addition, the ads and policies completely sidestep the multitude of data that flow to and from the phone, both natively and via third parties. Aggregated and inferred data are not considered "personal data," and are thus not included in the policies. However, these are the types of data that are most useful for training algorithms and targeting specific groups of people, techniques perhaps most famously employed by Cambridge Analytica.

Like the phenomenon of "greenwashing," I label this phenomenon "privacy-washing" — companies' intentional focus on specific "privacy" and security methods that belie their true, not-so-privacy-friendly practices. A complete definition of "privacy-washing" includes the purposeful conflation of security with privacy, the disregarding of more granular definitions of privacy (social vs. institutional privacy as well as data types including explicit, implicit, aggregated, and inferred), and a general reliance on offline privacy expectations that are no longer applicable to online spaces.

The practice of privacy-washing ensures users are less likely to realize the ways that targeted content has real implications for everyday life (*e.g.*, Noble, 2018). Indeed, the ways in which targeted ads and recommended content draw from tens of thousands of data points play an integral role in our views of the world. Issues around misinformation, "fake" news, and biased content depend on aggregated and inferred data to make guesses about people — who they are and what their vulnerabilities and fears are. The more that companies exploit users' lack of knowledge surrounding actual privacy and data infrastructures, the more prevalent are things like positive feedback loops/echo chambers and the more people get pushed to the margins and socially lose even a semblance of a middle ground.

Although only an analysis of two commercials and two privacy policies, this study highlights the many misconceptions surrounding privacy and security and the ways in which two powerful U.S. companies exploit this ignorance to their advantage. These themes are clearly present within other companies, including Meta and Amazon, and more analyses should be completed to further explore definitions of privacy and to hone "privacy-washing." Future studies should also test these findings by conducting user experiments that investigate if watching these ads, and others like them, do in fact lead users to believe the promoted privacy and security ideals.

About the author

Angela M. Cirucci is an associate professor of communication studies at Rowan University in Glassboro, N.J.
E-mail: ciruccia [at] rowan [dot] edu

Notes

1. Gharib, 2021, p. 2.

2. While critical discourse analysis is most fitting for the goals of this paper, it is important to note that it is

reliant upon my subjective, but informed, reading.

3. https://www.apple.com/legal/privacy/en-ww/.

4. https://policies.google.com/privacy?hl=en-US.

5. Of course, this is further exploited via the widespread knowledge that end-users are extremely unlikely to read these policies in the first place (*e.g.*, Obar and Oeldorf-Hirsch, 2020).

References

A. Acquisti and R. Gross, 2006. "Imagined communities: Awareness, information sharing, and privacy on the Facebook," *PET'06: Proceedings of the Sixth International Conference on Privacy Enhancing Technologies*. Berlin: Springer, pp. 36–58.
doi: https://doi.org/10.1007/11957454_3, accessed 3 May 2024.

A. Acquisti and J. Grossklags, 2005. "Privacy and rationality in individual decision making," *IEEE Security and Privacy*, volume 3, number 1, pp. 26–33.
doi: https://doi.org/10.1109/MSP.2005.22, accessed 3 May 2024.

B. Auxier, L. Rainie, M. Anderson, A. Perrin, M. Kumar, and E. Turner, 2019. "Americans and privacy: Concerned, confused, and feeling lack of control over their personal information," *Pew Research Center* (15 November), at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/, accessed 3 May 2024.

S.B. Barnes, 2006. "A privacy paradox: Social networking in the United States," *First Monday*, volume 11, number 9.
doi: https://doi.org/10.5210/fm.v11i9.1394, accessed 3 May 2024.

P. Bernal, 2020. *What do we know and what should we do about Internet privacy?* London: Sage.
doi: https://doi.org/10.4135/9781529712841, accessed 3 May 2024.

d. boyd and E. Hargittai, 2010. "Facebook privacy settings: Who cares?" *First Monday*, volume 15, number 8.
doi: https://doi.org/10.5210/fm.v15i8.3086, accessed 3 May 2024.

A.M. Cirucci, 2017. "Normative interfaces: Affordances, gender, and race in Facebook," *Social Media + Society* (28 June).
doi: https://doi.org/10.1177/2056305117717905, accessed 3 May 2024.

A. Cislak, A. Cichocka, A. Wójcik, and T.L. Milfont, 2021. "Words not deeds: National narcissism, national identification, and support for greenwashing versus genuine proenvironmental campaign," *Journal of Environmental Psychology*, volume 74, number 3, 101576.
doi: https://doi.org/10.1016/j.jenvp.2021.101576, accessed 3 May 2024.

G. De Vynck and A. Schaffer, 2022. "Lawsuit claims Google knew its 'incognito mode' doesn't protect users' privacy." *Washington Post* (25 October), at https://www.washingtonpost.com/politics/2022/10/25/lawsuit-claims-google-knew-its-incognito-mode-doesnt-protect-users-privacy/, accessed 3 May 2024.

N. Fairclough, 1995. *Critical discourse analysis: The critical study of language*. London: Longman.

G.A. Fowler, 2020. "At CES, Apple, Facebook, and Amazon are preaching privacy. Don't believe the

hype," *Washington Post* (8 January), at https://www.washingtonpost.com/technology/2020/01/08/ces-apple-facebook-amazon-are-preaching-privacy-dont-believe-hype/, accessed 3 May 2024.

M. Gharib, 2021. "Privacy and informational self-determination through informed consent: The way forward," *Computer Security — ESORICS 2021*. Cham, Switzerland: Springer, pp. 171–184.
doi: https://doi.org/10.1007/978-3-030-95484-0_11, accessed 3 May 2024.

E. Hargittai and A. Marwick, 2016. "'What can I really do?' Explaining the privacy paradox with online apathy," *International Journal of Communication*, volume 10, pp. 3,737–3,757, and at https://ijoc.org/index.php/ijoc/article/view/4655, accessed 3 May 2024.

E. Hargittai and E. Litt, 2013. "New strategies for employment? Internet skills and online privacy practices during people's job search," *IEEE Security and Privacy*, volume 11, number 3, pp. 38–45.
doi: https://doi.org/10.1109/MSP.2013.64, accessed 3 May 2024.

C. Herzog, 2016. "You can't have privacy without security," *National Cybersecurity Alliance* (13 October), at https://staysafeonline.org/blog/you-cant-have-privacy-without-security/, accessed 3 May 2024.

J. Hinds, E.J. Williams, and A.N. Joinson, 2020. "It wouldn't happen to me': Privacy concerns and perspectives following the Cambridge Analytica scandal," *International Journal of Human-Computer Studies*, volume 143, 102498.
doi: https://doi.org/10.1016/j.ijhcs.2020.102498, accessed 3 May 2024.

K. Jiminez, 2022. "Privacy-washing: What is it and how to stop it from happening to your company," *California Lawyers Association*, at https://calawyers.org/business-law/privacy-washing-what-is-it-and-how-to-stop-it-from-happening-to-your-company/, accessed 3 May 2024.

D.J. Leith, 2021. "Mobile handset privacy: Measuring the data iOS and Android send to Apple and Google," In: Joaquin Garcia-Alfaro, Shujun Li, Radha Poovendran, Hervé Debar, and Moti Yung (editors). *Security and privacy in communications networks (SecureComm 2021)*. Cham, Switzerland: Springer, pp. 231–251.
doi: https://doi.org/10.1007/978-3-030-90022-9_12, accessed 3 May 2024.

C.L. Miltgen and D. Peyrat-Guillard, 2014. "Cultural and generational influences on privacy concerns: A qualitative study in seven European countries," *European Journal of Information Systems*, volume 23, number 2, pp. 103–125.
doi: https://doi.org/10.1057/ejis.2013.17, accessed 3 May 2024.

A. Moore, 2008. "Defining privacy," *Journal of Social Philosophy*, volume 39, number 3, pp. 411–428.
doi: https://doi.org/10.1111/j.1467-9833.2008.00433.x, accessed 3 May 2024.

S.V. de F. Netto, M.F.F. Sobral, A.R.B. Ribeiro, and G.R. de L. Soares, 2020. "Concepts and forms of greenwashing: a systematic review," *Environmental Sciences Europe*, volume 32, article number 19.
doi: https://doi.org/10.1186/s12302-020-0300-3, accessed 3 May 2024.

S.U. Noble, 2018. *Algorithms of oppression: How search engines reinforce racism*. New York: NYU Press.

J.A. Obar and A. Oeldorf-Hirsch, 2020. "The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services," *Information, Communication & Society*, volume 23, number 1, pp. 128–147.
doi: https://doi.org/10.1080/1369118X.2018.1486870, accessed 3 May 2024.

S. Petronio, 2013. "Brief status report on communication privacy management theory," *Journal of Family Communication*, volume 13, number 1, pp. 6–14.
doi: https://doi.org/10.1080/15267431.2013.743426, accessed 3 May 2024.

K. Raynes-Goldie, 2010. “Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook,” *First Monday*, volume 15, number 1.
doi: https://doi.org/10.5210/fm.v15i1.2775, accessed 3 May 2024.

T. Sharon, 2021. “Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech’s newfound role as global health policy makers,” *Ethics and Information Technology*, volume 23, supplement 1, pp. 45–57.
doi: https://doi.org/10.1007/s10676-020-09547-x, accessed 3 May 2024.

D.J. Solove, 2021. “The myth of the privacy paradox,” *George Washington Law Review*, volume 89, number 1, pp. 1–51, and at https://scholarship.law.gwu.edu/faculty_publications/1482/, accessed 3 May 2024.

D.J. Solove, 2013. “Introduction: Privacy self-management and the consent dilemma,” *Harvard Law Review*, volume 126, number 7, pp. 1,880–1,903, and at https://harvardlawreview.org/print/vol-126/introduction-privacy-self-management-and-the-consent-dilemma/, accessed 3 May 2024.

O. Tene, 2008. “What Google knows: Privacy and Internet search engines,” *Utah Law Review*, volume 2008, number 4, pp. 1,433–1,492.

S. Trepte, 2021. “The social media privacy model: Privacy and communication in the light of social media affordances,” *Communication Theory*, volume 31, number 4, pp. 549–570.
doi: https://doi.org/10.1093/ct/qtz035, accessed 3 May 2024.

Z. Tufekci, 2008. “Can you see me now? Audience and disclosure regulation in online social network sites,” *Bulletin of Science, Technology & Society*, volume 28, number 1, pp. 20–36.
doi: https://doi.org/10.1177/0270467607311484, accessed 3 May 2024.

M. Vimalkumar, S.K. Sharma, J.B. Singh, and Y.K. Dwivedi, 2021. “‘Okay Google, what about my privacy?’: User’s privacy perceptions and acceptance of voice based digital assistants,” *Computers in Human Behavior*, volume 120, 106763.
doi: https://doi.org/10.1016/j.chb.2021.106763, accessed 3 May 2024.

A.L. Young and A. Quan-Haase, 2013. “Privacy protection strategies on Facebook: The internet privacy paradox revisited,” *Information, Communication & Society*, volume 16, number 4, pp. 479–500.
doi: https://doi.org/10.1080/1369118X.2013.777757, accessed 3 May 2024.

W. Youyou, M. Kosinski, and D. Stillwell, 2015. “Computer-based personality judgments are more accurate than those made by humans,” *Proceedings of the National Academy of Sciences*, volume 112, number 4, pp. 1,036–1,040.
doi: https://doi.org/10.1073/pnas.1418680112, accessed 3 May 2024.

Appendix

Transcript of Apple’s ad

Person standing on bus: “I browsed eight sites for divorce attorneys today!”

Person speaking to another person in dark movie theater (then they move on to a couple a few seats down, it is clear they are about to tell them next): “My log in for everything is pauline@paulinephu.com”

Person at work, in front of computer, surrounded by others at desks: “I love working with you!”
Another person yelling: “Me too!”

First person: “Red heart emoji!”
Second person: “Pink heart emoji!”
First person: “Yellow heart emoji!”
Second person: “Blue heart emoji!”
First person: “I hate Lee though.”
Second person: “Me too!”
First person: “Puke emoji!”
Second person: “Puke emoji!”
Third person who is probably Lee, sitting behind first person turns around to look at them, surprised.

Person is washing their hands and hears another person in bathroom stall.
Person in stall: “I am currently reading an article titled Ten Ways to Keep Sweaty Hands from Holding You Back.” The camera turns to show their feet under the stall, clearly sitting on the toilet.

Person walking down sitting street: “My home is in one thousand feet.”

Person in sweatshirt and sweatband, walking down a path: “My heart rate is currently 150, 151, 152, and back down to 150!” They pass another person on the trail and a couple sitting on the grass.

Person sitting at table in restaurant with two others: “On March 15th at 9:16 am I purchased prenatal vitamins and four pregnancy tests.”
One of the other people at the table spits out coffee and the other looks at them in shock.

Person standing in busy square in city with bullhorn: “The number on my credit card is 0, 2, 3, 7, 1, 2, 2, 1, 0, 7, 2, 5, 0, 2, 1, 1. That’s 0, 2 ...”
People walk by and look at them or each other with confusion.

Black background, white letters, middle of screen: “Some things shouldn’t be shared. iPhone keeps it that way.”

Person walking through the city, holds up a white iPhone so it blocks their face. Their hand is positioned just under the apple icon so that it is clearly an iPhone. White letters, middle of screen: “Privacy. That’s iPhone.”

At the end Apple icon but instead of leaf, u-lock, locks into apple, clicking sound. Then becomes a leaf.

Editorial history

Received 12 January 2024; revised 8 February 2024; accepted 4 May 2024.

Oversharing the super safe stuff: “Privacy-washing” in Apple iPhone and Google Pixel commercials
by Angela M. Cirucci.
First Monday, volume 29, number 5 (May 2004).
doi: https://dx.doi.org/10.5210/fm.v29i5.13321