Stewardship of privacy, or private capture of a public value? – A Note*

Helen Nissenbaum
Cornell Tech

Last Updated: 28 October 2022

Abstract

In the past two decades, technological developments have created new sociotechnical infrastructures, including social media and mobile platforms. These developments have disrupted ways of life and called into question basic social, ethical, and societal values, which have been insufficiently addressed by law and regulation. Technology companies have moved into this void, defining and operationalizing societal values. Coupled with their role as infrastructure, these platforms have transcended traditional business-to-consumer relationships to affect societal values. Mobile platforms in particular deserve special attention given the central role smartphones play in our everyday lives. Among mobile platforms, Google's Android and Apple's iOS are effectively the only two, and they have declared themselves champions of privacy. We have focused our analysis on Apple because it has emphasized this commitment in its messaging to consumers and to the government. Like other companies, Apple continues to rely on notice and choice as its privacy gatekeeper despite its known flaws. It asserts privileges over wide-ranging, massive data stocks generated by its own holdings as well as those of independent apps operating on its platform. In its defense, Apple cites anonymization and other sophisticated methods, such as differential privacy, but provides insufficient detail to enable independent experts to validate the efficacy of its practices. The lens of contextual integrity highlights the threats these practices pose to privacy when Apple and iOS ignore contextual norms in capturing, merging, and analyzing data from diverse sources. Apple may deserve a place among privacy leaders, but its approach leaves users no more "in control" – meaningfully – of data about themselves. Privacy has become far too important to leave in the hands of stakeholders in the corporate fray to define and unilaterally enforce.

I. INTRODUCTION

1. Technology has developed rapidly in recent years, posing significant challenges to regulators: developments that threaten to undermine societal values and individual well-being often outpace the capacity of existing law and policy to adapt.[1] In the case of digital technologies, one consequence is a regulatory void that private technology firms have taken upon themselves to fill. On the one hand, private firms may be lauded for performing a useful societal role; on the other, as interested parties with much at stake, their proposals deserve and have received critical scrutiny. The role of dominant actors in private industry defining and enforcing public values is the conundrum motivating these

* The author thanks Stephen Chan, Yik Siu Chan, Ali Simsek, Nimo Suleyman, Bartley Tablante, Albert Zhang, and Qinyue Zhou for research assistance. The author would like to acknowledge support from the Match Group. The views expressed in this essay are solely those of the author.

[1] Moses, L. B. (2007). Recurring dilemmas: The law's race to keep up with technological change. U. Ill. JL Tech. & Pol'y, 239.

comments. Although privacy is the central focus of this Note, this Note starts by addressing speech norms which have recently been in the public debate.

2. In past decades, the growing dominance of social media platforms has given them a role in defining and enforcing norms of allowable speech. As social media platforms have increasingly facilitated public discourse[2] in multiple domains, so has expressed anxiety over harmful speech spread on the platforms. Speech can be labeled as harmful if it is considered abusive, aggressive, threatening, misleading, or false ("fake news"). Platforms may have several motivations for regulating speech, including: facilitating positive interactions, preventing abuse in their online communities, or avoiding external regulation and legal action. Platforms have sought to fill a perceived regulatory void by regulating speech on their platforms via content moderation, take-down notices, censorship, etc. Approaches include a range from automated technical blocks and human reviewer moderation to expressed principles and prohibitions.[3] Platforms therefore implicitly and explicitly define allowable speech and forge norms and rules to enforce it. On the one hand, such rules can draw controversy and have been argued to limit the constitutional right to free speech.[4] On the other hand, it is widely agreed that *some* level of moderation is necessary on online forums.[5]

3. Given the complexity of the task and potential societal implications, social media platforms have resorted to increasingly elaborate structures of control, becoming in effect "the government of a new type of community."[6] The Facebook case contains interesting parallels to existing governments. After considering a legislative model in the vein of Congress to adjudicate controversial content moderation decisions,[7] it settled on a quasi-independent "Supreme Court," the Facebook Oversight Board (FOB),

---

[2] Çela, E. (2015). Social Media as a New Form of Public Sphere. *European Journal of Social Science Education and Research*, *2*(3), 195–200. Retrieved from: https://doi.org/10.26417/ejser.v4i1.p195-200

[3] Gillespie, T. (2020). Content moderation, AI, and the question of scale. Big Data & Society, 7(2), 2053951720943234. Retrieved from: https://journals.sagepub.com/doi/full/10.1177/2053951720943234

[4] Brannon, V. C. (2019). Free speech and the regulation of social media content. *Congressional Research Service*, *45650*, 1-43. Retrieved from: https://www.everycrsreport.com/files/20190327_R45650_9f272501744325782e5a706e2aa76781307abb64.pdf

[5] For example, the infamous "Tide Pod Challenge" started as a parody of online challenges popular at the time before teens actually started eating Tide Pods. Even after such phenomena clearly take a negative turn, blanket bans can also stifle positive content like informative social commentary on the matter. Grimmelmann, J. (2018). The Platform is the Message. Geo. L. Tech Rev. Retrieved from: https://georgetownlawtechreview.org/wp-content/uploads/2018/07/2.2-Grimmelmann-pp-217-33.pdf

[6] Grimmelmann, J. (2015). The virtues of moderation. Yale JL & Tech., 17, 42. Retrieved from: https://openyls.law.yale.edu/bitstream/handle/20.500.13051/7798/Grimmelmann_The_Virtues_of_Moderation.pdf?sequence=2

[7] To cite just one example, Facebook content moderation algorithms mistakenly flagged accurate health information about COVID-19 as spam in March 2020. Peters, J. (2020). Facebook was marking legitimate news articles about the coronavirus as spam due to a software bug. The Verge. Retrieved from: https://www.theverge.com/2020/3/17/21184445/facebook-marking-coronavirus-posts-spam-misinformation-covid-19)

to review such decisions.[8] The FOB represents the highest level of appeal for content moderation decisions submitted either by users or Facebook itself for review.[9] In lieu of a constitution, the FOB relies on Facebook's Community Standards to decide whether content moderation decisions will be upheld or be overturned and issues written explanations of decisions that are reminiscent of Supreme Court briefs.[10] [11]

II. BIG TECH AND PUBLIC VALUES

4. It might be argued that the privacy, speech, and content policies set by private, commercial companies are matters of limited concern affecting a closed relationship between these companies and their customers. Facebook/Meta, Apple, and Google, however, given sheer size, have become infrastructure-like platforms, whose decisions and policies spread far beyond closed loops with individual customers. Instead, policies they adopt may spillover into the public sphere and impose constraints on other services built on top of their platforms.[12] Meta alone, through Facebook and Instagram, captures 79% of the social media market share in the US.[13] Around the world, Facebook has almost 3 billion[14] and Instagram has 1.2 billion monthly active users.[15] Platforms themselves acknowledge their critical role, with Mark Zuckerberg as CEO of Meta calling expression through social media "a Fifth Estate alongside the other power structures of society."[16] It is no wonder that the world looks on with hope, frustration, and indignation as platform giants issue policies, guidance, and decisions unaccountable to the public.

5. The conundrum is even more acute in the case of mobile devices, including smartphones. 85% of all Americans own a smartphone, with 15% of Americans (and 28% of those aged 18-29) dependent on

[8] Klonick, K. (2021). Inside the Making of Facebook's Supreme Court. The New Yorker. Retrieved from: https://www.newyorker.com/tech/annals-of-technology/inside-the-making-of-facebooks-supreme-court

[9] Oversight Board Charter. (2021). Oversight Board. Retrieved from: https://www.oversightboard.com/governance/

[10] Oversight Board Charter. (2021). Oversight Board. Retrieved from: https://www.oversightboard.com/governance/

[11] Klonick, K. (2020). The Facebook Oversight Board: Creating an Independent Institution to Adjudicate Online Free Expression. Yale Law Journal, V. 129 No. 2418. Retrieved from: https://ssrn.com/abstract=3639234

[12] Pasquale, F. (2017). Democracy Unchained. JOTWELL. (reviewing Rahman, K. S. (2017) Private Power, Public Values: Regulating Social Infrastructure in a Changing Economy. Cardozo Law Review, V. No. 5; Winseck, D. (2017). The Geopolitical Economy of the Global Internet Infrastructure. Journal of Information Policy, V. 7, 228–67.

[13] Social Media Stats United States Of America. (2022). StatCounter Global Stats. Retrieved from: https://gs.statcounter.com/social-media-stats/all/united-states-of-america

[14] Facebook MAU worldwide 2022. (2022). Statista. Retrieved from: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[15] Number of monthly active Facebook users worldwide as of 1st quarter 2022. (2022). Statista. Retrieved from: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/

[16] Romm T. (2019). Zuckerberg: Standing For Voice and Free Expression. The Washington Post. Retrieved from: https://www.washingtonpost.com/technology/2019/10/17/zuckerberg-standing-voice-free-expression/

smartphones for internet access.[17] Apple and Google are effectively the only players in this market, with 99.72% of devices running on iOS or Android, with nearly 60% of the total being iOS devices.[18] This is a significant increase since 2010, when 5 smartphone platforms captured >5% of worldwide sales.[19] App developers also have little choice given that over 90% of mobile apps are sold on the Google Play Store or Apple's App Store.[20]

6. Mobile apps are reshaping industries, with mobile devices accounting for 48% of global gaming revenue at $77.2 billion per year, dwarfing console ($45.3 billion) and PC gaming ($36.9 billion).[21] Further, mobile devices are set to account for 44.2% of retail e-commerce sales in the United States by 2025.[22] These platforms also are major conduits of information for large swathes of society and the medium through which they carry out vital activities.

7. And while Apple and Google have significant control over consumer's mobile lives, both companies also define how Americans browse the Web. 49% of Americans browsing with Google Chrome and 35% using Apple's Safari.[23] And the effects are similarly large in General and Video Search.[24] Accordingly, the infrastructure-like nature of platforms owned by global tech giants belies the suggestion that their policies and practices are a matter of narrow business-to-consumer or business-to-business relationships; rather, their impacts ripple far beyond to impact societal values.

8. Privacy has moved into the spotlight alongside speech. Wave after wave of disturbing revelations about exploitative collection and uses of personal data have elevated privacy into public awareness and as a topic of public anxiety. As a result of the past two decades in which dominant actors effectively had declared open season on personal data, public tolerance has grown thin. As with speech, digital technologies serving dominant business models exposed a void between

[17] Mobile Fact Sheet. (2021). Pew Research Center. Retrieved from: https://www.pewresearch.org/internet/fact-sheet/mobile/

[18] Mobile Operating System Market Share Worldwide. (2022). Statcounter. Retrieved from: https://gs.statcounter.com/os-market-share/mobile/worldwide

[19] Blodget, H. (2010). Android Blows Past iPhone To Capture 17% Of Global Market Share In Q2. Business Insider. Retrieved from: https://www.businessinsider.com/android-iphone-market-share-2010-8

[20] Number of apps available in leading app stores as of 2022. (2022). Statistica. Retrieved from: https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

[21] Wijman, T. (2020). The World's 2.7 Billion Gamers Will Spend $159.3 Billion on Games in 2020; The Market Will Surpass $200 Billion by 2023. Newzoo. Retrieved from: https://newzoo.com/insights/articles/newzoo-games-market-numbers-revenues-and-audience-2020-2023/

[22] Rise of Mcommerce: Mobile Ecommerce Shopping Stats & Trends in 2022. (2022). Insider Intelligence. Retrieved from: https://www.insiderintelligence.com/insights/mobile-commerce-shopping-trends-stats

[23] Browser Market Share United States of America. (2022). Statcounter. Retrieved from: https://gs.statcounter.com/browser-market-share/all/united-states-of-america

[24] For example, Google captures more than 90% of all internet searches through Google Search and YouTube searches (Desjardins, J. (2018). How Google retains more than 90% of market share. Business Insider. Retrieved from: https://www.businessinsider.com/how-google-retains-more-than-90-of-market-share-2018-4)

unprecedented data practices, which had proceeded unabated, and a regime of privacy law and regulation ill-equipped to deal with them. During these two decades, data and information industry incumbents, forming a more-or-less united front, had expressed loud support for a government "hands-off" approach to regulation and, given their economic successes, were more-or-less allowed to steer the course.

9. Leading up to the present time, privacy experts and advocates, who had insistently questioned the prevailing approach[25] have noticed interesting shifts in the data landscape, including a growing disunity among key actors. Although a full account of this progression is beyond the scope of this Note, we provide a brief account of how the infrastructure-like platforms are now pitted against a broad swathe of data services, communications, and media companies in their respective, divergent approaches to filling the void between privacy law and regulation and prevailing data practices. This essay is not interested in declaring favorites or predicting winners and losers. Instead, its immediate concern is the fate of privacy as a meaningful societal value in wake of these conflicts.

10. When the extent of online tracking was exposed, with its teeming populations of specialized data brokers and innumerable layers of marketing and analytics companies, a threshold seemed to have been crossed and the online data ecosystem could no longer be tolerated. In turn, this public exposure also revealed the regulatory void between sociotechnical practice and privacy regulation in the public interest. With the writing on the wall, Apple and Google, two of the dominant infrastructure-like companies, sought to separate from the pack by promoting themselves loudly as "privacy-first." For example, Apple employed slogans such as: "Privacy. That's iPhone,"[26] and Google promised to "strictly uphold responsible data practices so every product we build is private by design."[27] Apple's Tim Cook had already adopted the rhetoric of privacy in 2014, saying "we believe a great customer experience shouldn't come at the expense of your privacy,"[28] while Google had more work on its hands, to distance itself from Eric Schmidt's brash position, "If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."[29]

---

[25] For example, the Electronic Privacy Information Center (EPIC), for example, "was established in 1994 to focus public attention on emerging privacy and civil liberties issues and to protect privacy, freedom of expression, and democratic values in the information age." (About EPIC. (2022). EPIC. Retrieved from: https://archive.epic.org/epic/about.html)

[26] Privacy, That's iPhone Commercial by Apple. (2020). ZacTech Videos. Retrieved from: https://www.youtube.com/watch?v=rEWeA7qDV4k

[27] Security and Privacy. Google. Retrieved from: https://safety.google/intl/en_us/security-privacy/

[28] Cook, T. (2014). A message from Tim Cook about Apple's commitment to your privacy. Apple. Retrieved from: https://web.archive.org/web/20140918102737/http:/www.apple.com/privacy/

[29] Esguerra, R. (2009). Google CEO Eric Schmidt Dismisses the Importance of Privacy. Electronic Frontier Foundation. Retrieved from: https://www.eff.org/deeplinks/2009/12/google-ceo-eric-schmidt-dismisses-privacy

11. These public campaigns were directed at users and consumers of their products (e.g., through lavish billboards and other traditional forms of advertising), to be sure, but, we surmise, also at regulators (lawmakers and government agencies) whom they were assuring "we're on it!" The message? Champions of privacy, we, the infrastructure-like companies are in no need of governmental regulation; instead, we will lead the way in filling the void between law in the books and data practices. Apple and Google were also putting on notice a third audience, namely, the swath of companies who had previously been benefitting from untrammeled access to behavioral, transactional, and demographic data, whose products functioned atop the massive platforms, and were fully dependent on them. In the domain of mobile smartphones, these included apps, a complex advertising domain, libraries of supporting products, and others. This audience was none too happy about restrictions imposed on their activities in the name of privacy.[30] And the result of these restrictions affected the developer ecosystem, including increasing paid apps and moving away from ad-funded apps.[31]

12. Given the role that Apple and Google have assumed as protectors of privacy, it is critical to scrutinize how they conceptualize or define privacy and how they operationalize and enforce it. Unless the conception of privacy they promote corresponds to a societal and ethical value that is meaningful and important to people, these companies' pronouncements carry little weight. Accordingly, we ask: 1) what do Apple and Google mean by privacy and 2) what policies, protocols, and practices are they following in its name?

13. To answer the first question: both firms adopt a high-level conception of privacy as control over information about ourselves. Google in its privacy center states: "we create easy to use privacy and security settings so you're in control."[32] Apple in its privacy materials states: "Whatever you choose is up to you,"[33] among numerous variations of this theme. Both firms interpret control by means of transparency and choice (also, notice and choice, informed consent, etc.). Apple states: "We believe in telling you up front exactly what's going to happen to your personal information and asking for your permission before you share it with us. And if you change your mind later, we make it easy to stop sharing with us. Every Apple product is designed around those principles."[34] We address the second question about policies, protocols, and practices in the next section.

---

[30] For example, Meta accused Apple of harming the ad-supported free app ecosystem by implemented App Tracking Transparency which reduced developers' ability to monetize through ads. (Statt, N. (2022). accuses Apple of 'self-serving tactics' on gaming app restrictions," Protocol. Retrieved from: https://www.protocol.com/bulletins/facebook-gaming-appleapp-store)

[31] Kesler, Reinhold. "The Impact of Apple's App Tracking Transparency on App Monetization," http://dx.doi.org/10.2139/ssrn.4090786

[32] Security & Privacy - Google Safety Center. Google, Accessed 3 Sep 2022 Retrieved from: https://safety.google/intl/en_us/security-privacy/

[33] Privacy | App Tracking Transparency | Apple. (2021). Apple. Retrieved from: https://www.youtube.com/watch?v=Ihw_Al4RNno

[34] Privacy – Control. Apple. Accessed 3 Sep 2022. Retrieved from: https://www.apple.com/privacy/control/

14. At the heels of what we uncover, we pose two further questions: 1) does this interpretation align with a meaningful conception of privacy – a conception that people care about; and 2) even if we accept the conception as sound, are these infrastructure-like companies justified in claiming they are privacy-first. And if they are not justified in claiming they are privacy-first, citing privacy as a reason for imposing blanket constraints on outside companies whose services the platforms mediate does not hold water.

A. Notice and Choice

15. The interpretation of privacy as control that Apple and Google use, operationalized as notice and choice, is deeply entrenched in online transactions. However, there is good reason to be skeptical.[35] For one, control may not be the route to meaningful privacy; second, notice and choice need not ensure control; and third, the ubiquitous approach taken in the tech industry to operationalize notice and choice through privacy policies and assumed consent is deeply flawed. These shortcomings of notice and choice are validated through empirical findings and careful analysis. Several papers have proposed establishing informational norms and privacy expectations as an alternative to notice and choice due to the significant gaps in the model.[36] The point we wish to emphasize is that the approaches to privacy that Apple and Google take in defining and enforcing notice and choice are not particularly problematic, only that they are as flawed as the approaches taken by other good-faith actors. Being as flawed as others, nevertheless, is potentially more damaging to privacy than the practices of others because of the unique role they play as infrastructure-like intermediating platforms.

16. In detailing the shortcomings of a notice and choice approach, we tease apart the two components, starting with choice though arguably "notice" has been more comprehensively studied.

1) Choice

17. To support a claim that users are "in control," it must be clear that users are genuinely choosing, that they are selecting deliberately or freely in accordance with their preferences and values. It's tricky to disentangle choice from notice (or consent from being informed) because it's impossible to say that

---

[35] Adjerid, I., Acquisti, A., & Loewenstein, G. F. (2018). Choice Architecture, Framing, and Cascaded Privacy Choices," Management Science V. 65 No. 5, 1949-2443. Retrieved from: https://doi.org/10.1287/mnsc.2018.3028; Habib, H. & Cranor, L. F. (2022). Evaluating the Usability of Privacy Choice Mechanisms. USENIX Association. Retrieved at https://www.usenix.org/conference/soups2022/presentation/habib; Sloan, R. H. & Warner, R. (2014). Beyond Notice and Choice: Privacy, Norms, and Consent. Journal of High Technology Law. Retrieved at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jhtl14&div=11&id=&page=

[36] Martin K. (2013). Transaction Costs, Privacy, and Trust: The Laughable Goals and Ultimate Failure of Notice and Choice to Respect Privacy Online. First Mondey, V. 18, No. 12-2. Available at SSRN: https://ssrn.com/abstract=2370451; Sloan, R. H. & Warner, R. (2014). Beyond Notice and Choice: Privacy, Norms, and Consent. Journal of High Technology Law. Retrieved at: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jhtl14&div=11&id=&page=

an uninformed person is *choosing*. Yet, the opposite may well hold. Namely, a person may be informed via a privacy notice, for example, and still make a selection against their preferences, a selection that is not freely or willingly made. Although some attention has been paid to opt-in versus opt-out as mechanisms of choice, not enough has been paid to the extent our selections are compelled and not freely chosen. Both GDPR and CPRA have recognized that a selection with significantly degraded service, or a selection where a user is in the dark about what it will do are not genuine choices.[37] In these cases regulators have tried to insist that a user should not be forced to select one or other option in order to use a particular service. Yet, anecdotally, users are presented "accept" boxes to check, with no indication of an alternative.

18. The infrastructure-like role that Apple and Google occupy as smartphone platforms, for example, also increases the costs of non-consent. Few in the United States can earn a livelihood, educate their kids, shop, seek medical care, etc. without a smartphone. How well can we live without performing mobile online searches or browsing the Web? The pretense that people have an alternative to "take it or leave it" privacy policies is easily exposed, particularly with threats such as once issued in Google's privacy policy, "You can decline to submit personal information to any of our services, in which case Google may not be able to provide those services to you." [38] Apple's privacy policy similarly states, "You are not required to provide the personal data that we have requested. However, if you choose not to do so, in many cases we will not be able to provide you with our products or services or respond to requests you may have."[39] Take-it-or-leave-it when leaving a mobile platform has significant cost, and policies that are non-negotiable and inflexible along almost all dimensions of data are a far-cry from any normal understanding of "choice" or control.

19. Finally, *expressed choice may not matter*. Even if users do not consent to sharing personal information with platforms, platforms can infer personal information using models drawn from machine learning

[37] GDPR Recital 42, "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment." GDPR Article 4(11): "Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her." (OJ L 119, 4.5.2016, p. 1–88, retrieved from: https://eur-lex.europa.eu/eli/reg/2016/679/oj) Furthermore, the CPRA defines a dark pattern as: "[a] user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation." (California Consumer Privacy Act of 2018 [1798.100 - 1798.199.100], retieved from: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5)

[38] Google Privacy Policy," Google, 11 March 2009. Retrieved from: https://policies.google.com/privacy/archive/20090311?hl=en-US

[39] Apple Privacy Policy. Apple, 27 October 2021, available at Retrieved from: https://www.apple.com/legal/privacy/en-ww/

(ML) algorithms over data from similar users who had consented.[40] For example, Target used the past purchase data of consumers who later set up baby shower registries to predict which consumers were pregnant.[41] Similarly, social network companies, such as Facebook, are able to predict sexual orientation based on friends who have identified as gay.[42] While advanced digital technology has made adequate notice for meaningful choice impossible, advanced analytics, powered by AI and ML have made it irrelevant. Although the power of advanced analytics is not uniquely available to infrastructure-like companies, its potency is far greater for those who have access to massive pools of diverse data.

2) Notice

20. We organize the problems with notice around three themes: *time, comprehension,* and *manipulability.* As above the key takeaway is that providing "notice" to users does not lead to users having control.

21. *Time*: It is practically impossible for ordinary people to read through the privacy policies of all the devices and services they encounter, due to sheer length.[43] One estimate places the annual national opportunity cost of the time required to read (let alone understand) such policies at an aggregate $781 billion.[44] This figure does not account for being able to compare the policies of multiple sites, to make informed decisions about engaging in online activities due not only to length but also to complexity.[45] It is no surprise that privacy policies remain largely unread, with the UK's Competition and Markets Authority (CMA) finding that the average user spends less than a minute reading Google's privacy policy, with 85% of users spending less than ten seconds reviewing the policy.[46] Such practices do not appear to support rational decision making.

[40] Choi, J. P., Jeon, D. S., & Kim, B. C. (2019). Privacy and personal data collection with information externalities. Journal of Public Economics, V. 173, 113-124. Retrieved from: https://www.sciencedirect.com/science/article/abs/pii/S0047272719300131; Acemoglu, D., Makhdoumi, Malekian, A. & Ozdaglar, A. (2019). Too much data: Prices and inefficiencies in data markets. National Bureau of Economic Research, No. w26296. Retrieved from: https://www.nber.org/papers/w26296; Bergemann, D., Bonatti, A. & Gan, T. (2022). The economics of social data. The RAND Journal of Economics. Retrieved from: https://onlinelibrary.wiley.com/doi/abs/10.1111/1756-2171.12407

[41] Duhigg, C. How Companies Learn Your Secrets. (2012). New York Times. Retrieved from: https://www.nytimes.com/2012/02/19/magazine/shopping-habits.html

[42] Jernigan, C. & Mistree, B. F. (2009). Gaydar: Facebook friendships expose sexual orientation. First Monday. Retrieved from: https://firstmonday.org/ojs/index.php/fm/article/view/2611

[43] McDonald, A. M. & Cranor, L. F. (2008). The cost of reading privacy policies. Isjlp, 4, 543. Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc4&div=27&id=&page=

[44] McDonald, A. M. & Cranor, L. F. (2008). The cost of reading privacy policies. Isjlp, 4, 543. Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc4&div=27&id=&page=

[45] Acquisti, A. & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE security & privacy, 3(1), 26-33. http://infosecon.net/workshop/downloads/2004/pdf/acquisti.pdf

[46] Online Platforms and Digital Advertising – Market Study Final Report. (2020). UK Competition and Markets Authority. Retrieved from:

22. *Comprehension*: Even if time were not an issue, ordinary users would not be not able to grasp the meaning of privacy policies. Studies show that even experts are not able to grasp most privacy policies or retain what they have read.[47] Even beyond grasping the immediate semantics of a notice, its practical meaning requires an understanding of the current data ecosystem and future trajectories.[48] In Apple's case, users given a choice to opt out of targeted advertising do not know whether this stops Apple from tracking and profiling, which is more relevant from a privacy perspective, or merely the presentation of ads that have been derived from these practices. Apple is being deliberately obscure. It is no surprise that most individuals concur out of a sense of helplessness,[49] not because they believe they are making an informed trade-off.[50]

23. There is no easy way out of this conundrum, according to Nissenbaum's "transparency paradox:" a privacy policy simple enough for the layperson to understand is unable to capture the full extent of data practices necessary to describe, and a policy that comprehensively describes practices of any degree of complexity is infeasible for the layperson to understand. [51] Finally, there is evidence to show that even after reading a policy, people recall the policy saying what they expect it to say and not what it actually says.[52]

24. *Manipulability*: Acceptance of privacy policies has shown to be easily manipulated. The Associated Press reported in 2018 that Google was storing user location information even after pausing a

---

https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf

[47] Reidenberg, J. R. et al. (2014). Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding. 2014 TPRC Conference Paper. Berkeley Technology Law Journal, V. 30, 2015, Fordham Law Legal Studies Research Paper, No. 2418297. http://dx.doi.org/10.2139/ssrn.2418297

[48] Turow, J., Hennessy, M., & Draper, N. (2015). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Available at SSRN 2820060. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060

[49] A 2019 Pew survey reveals that 81% of U.S. adults feel that "they have very little/no control over the data companies collect," and that "potential risks of companies collecting data about them outweighs the benefits." 79% of respondents stated that they "are very/somewhat concerned about how companies use the data collected." See Auxier, B., et al. (2019). Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research Center. Retrieved from: https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

[50] Nissenbaum, H. (2011). A contextual approach to privacy online. Daedalus, V. 140 No. 4, 32-48. Retrieved from: https://www.amacad.org/sites/default/files/daedalus/downloads/Fa2011_Protecting-the-Internet-as-Public-Commons.pdf

[51] Nissenbaum, H. (2011). A contextual approach to privacy online. Daedalus, V. 140 No. 4, 32-48. Retrieved from: https://www.amacad.org/sites/default/files/daedalus/downloads/Fa2011_Protecting-the-Internet-as-Public-Commons.pdf

[52] Turow, J., Hennessy, M., & Draper, N. (2015). The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation. Available at SSRN 2820060. Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2820060

"Location History" setting.[53] In internal emails, unsealed as part of a lawsuit filed by the Arizona Attorney General against Google, Google engineers described labyrinthine privacy settings that could elicit consent for any data collection convenient to Google: "the current UI feels like it is designed to make things possible, yet difficult enough that people won't figure it out."[54] The result that individual judgements and preferences can be readily manipulated has also been demonstrated empirically. Alessandro Acquisti and his collaborators, leading experts in studying privacy through the lens of behavioral economics, have found this result in several studies.[55]

B. Anonymity

25. Defending ubiquitous collection and use of personal data, companies often explain that the data at issue is anonymized, or deidentified, implying that such data lies outside privacy's remit entirely.[56] Sure, we have a say over data about identifiable individuals but once identities are scrapped, all bets are off. By now, a large body of literature – outside the scope of this Note – has revealed that effective anonymization is difficult to achieve.[57]

26. Recognizing some of the failings of simplistic anonymization techniques (e.g. deleting the "Name" field) other approaches have been devised, including k-anonymity.[58] At the time of writing this Note,

---

[53] Nakashima, R. (2018). AP Exclusive: Google tracks your movements, like it or not. Associated Press. Retrieved from: https://apnews.com/article/north-america-science-technology-business-ap-top-news-828aefab64d4411bac257a07c1af0ecb

[54] Loppato, E. (2020). Even Google engineers are confused about Google's privacy settings. The Verge. Retrieved from: https://www.theverge.com/2020/8/26/21403202/google-engineers-privacy-settings-lawsuit-arizona-doubleclick

[55] See, e.g., Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. IEEE security & privacy, V. 3 No. 1, 26-33.; Adjerid, I., Acquisti A., and George Loewenstein. (2019). Choice architecture, framing, and cascaded privacy choices. Management Science, V. 65.5, 2267-2290.

[56] For example, once Apple has applied privacy preserving techniques to anonymize and aggregate user data, then it is "considered non-personal data for the purposes of this Privacy Policy." Apple Privacy Policy. Apple. 27 October 2021. Retrieved from: https://www.apple.com/legal/privacy/en-ww/)

[57] An early example of such a failure is the case of the AOL search dataset. The company released a large dataset of anonymized search queries for research purposes. This seemingly benevolent act created significant privacy harms when reporters from the New York Times were able to re-identify the anonymized individuals based on the content of their search queries (Barbaro, M. & Zeller, T. Jr. (2006). A Face Is Exposed for AOL Searcher No. 4417749. New York Times. Retrieved from: https://www.nytimes.com/2006/08/09/technology/09aol.html). In another famous case, researchers were able to easily re-identify anonymized Netflix members by employing IMDb as a source (Narayanan, A. & Shmatikov, V. (2006). How to break anonymity of the netflix prize dataset. arXiv preprint cs/0610105. Retrieved from: https://arxiv.org/abs/cs/0610105).

[58] Sweeney, L. (2002). k-anonymity: A model for protecting privacy. International journal of uncertainty, fuzziness and knowledge-based systems, 10(05), 557-570. Retrieved from: https://www.worldscientific.com/doi/abs/10.1142/S0218488502001648; Ohm, P. (2009). Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. UCLA Law Review, V. 57, p. 1701, U of Colorado Law Legal Studies Research Paper No. 9-12, Available at SSRN: https://ssrn.com/abstract=1450006

however, the state-of-art is believed to be differential privacy,[59] an ingenious method for supplying aggregate statistics about a dataset while reducing the statistical likelihood that individuals inside the dataset can be reidentified.

27. Tactics abound for returning to anonymized data some of the utility of PII even without traditional markers of identity, such as names or social security numbers. Example tactics include: assigning artificially generated persistent identifiers to individuals, such as ad IDs (e.g. cookies),[60] or fixing individuals through unique patterns of movement, which can be achieved through location tracking. The impact of persistent, non-traditional identifiers allows companies to perform an end-run around some of the barriers of anonymity.[61] The GDPR has tried to undermine some of these workarounds by expanding privacy rights over data that can single out individuals, that is, make them reachable, even absent traditional identifiers.

28. Rendering individuals difficult to identify through sophisticated anonymization techniques such as differential privacy (DP), is not a panacea. Apple has committed to using differential privacy when drawing data to its central servers from distributed devices. The guarantee of deidentification that differential privacy affords depends on the choice of epsilon, which affects the degree to which data is obfuscated by the DP system. Yet, despite the fact that Apple's Machine Learning Research team regularly publishes research on privacy techniques, the last time Apple disclosed the epsilon values it actually deployed for their algorithm was in 2017,[62] and critics argued that this disclosure was insufficient to provide easy testing of Apple's claims.[63] This prevents external experts from either understanding or validating Apple's anonymization claims.

[59] Dwork, C. (2008). Differential privacy: A survey of results. In International conference on theory and applications of models of computation. Springer, 1-19. Retrieved from: https://link.springer.com/chapter/10.1007/978-3-540-79228-4_1

[60] How Google Marketing Platform advertising products and Google Ad Manager use cookies. Google, Accessed 3 Sep 2022, available at Retrieved from: https://support.google.com/campaignmanager/answer/2839090?hl=en

[61] Barocas S. & Nissenbaum H. (2014). Big Data's End Run Around Consent and Anonymity. In Privacy, Big Data and the Public Good. Eds. Lane J., Stodden V., Bender S., Nissenbaum H., Cambridge University Press. Retrieved from: https://nissenbaum.tech.cornell.edu/papers/Big%20Datas%20End%20Run%20Around%20Consent%20and%20Anonymity.pdf

[62] Differential Privacy Team (2017). Learning with Privacy at Scale. Apple. Retrieved from: https://docs-assets.developer.apple.com/ml-research/papers/learning-with-privacy-at-scale.pdf

[63] Tang, J., Korolova, A., Bai, X., Wang, X., & Wang, X. (2017). Privacy loss in Apple's implementation of Differential Privacy on macOS 10.12. arXiv preprint arXiv:1709.02753. Retrieved from: https://arxiv.org/pdf/1709.02753.pdf

29. The technical details of this argument are not as important as the high-level conclusion. Apple has potential access to a tremendous amount of highly detailed data about individuals.[64] The promises Apple makes are that extraction of information about individuals will be made in a "privacy preserving" way;[65] this is part of their claim to be privacy-first company. Yet differential privacy promises nothing without guarantees like an epsilon of the right level and algorithms whose quality is assured, validated – in our view – by impartial, external parties. All the billboards in the world are insufficient without these assurances.

30. Furthermore, as we have argued elsewhere, sophisticated inference techniques applied to increasingly massive datasets allow individuals to be clustered with others like them and treated differently – so-to-speak – together.[66] What is the good of being anonymous as long attributes about you can be gleaned through methods such as these? When massive platform companies have enough data points to assign individuals into meaningful clusters in service of the company's interests, individuals are rendered accessible to them even if these companies utilize techniques that remove obvious identifiers.

31. *Taking stock*. Many of the points we have made about the failures of informed consent and deidentification to assure privacy as control over information apply across almost all companies who have adopted them in data intensive transactions. Nevertheless, it is important to review these points in relation to dominant, multifarious platforms, such as Google, and particularly Apple, which are the focus of this Note. First, because Apple, specifically, presenting itself as "privacy first," has earned trust of unsuspecting users while it draws on this self-presentation to keep other companies at arms' length. As such, we expect Apple's practices not only to be no worse than but also to surpass those of others. Second, in depending on Notice and Choice as a means of assuring control, these companies are no better than others and potentially worse, because size or scale matters by far outstrips the cognitive ability of individuals to make a choice based on understanding of relevant practices. How that affords control we do not know. Finally, companies with ready access to massive and diverse stocks of data have greater power to work around allegedly failsafe techniques of deidentification (as discussed above), allowing a company to single out individuals for distinctive treatment (e.g., personalized marketing), whether individually, or in clusters of similar individuals. In sum, privacy as

[64] For example, the US Supreme Court unanimously decided in Riley v. California (2014) that police cannot search cellphones cannot without a warrant. Supreme Court of the United States. (2013). Riley v. California. Retrieved from: https://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf)

[65] A prompt asking users to consent to data collection for analytics purposes, for example, says, "All data is collected using privacy preserving techniques such as differential privacy and is not associated with your account." (iPhone Analytics. Apple, iOS 15.5. Accessed 16 May 2022)

[66] McGuigan, L. & Nissenbaum, H. (2021). On Google's Sandbox/FLoC Proposal: Comments Submitted to UK-CMA. Retrieved from: https://www.dli.tech.cornell.edu/post/comments-on-proposed-privacy-sandbox-commitments-regarding-user-welfare-case-reference-50972

control is ill-served by Notice and Choice. Deidentification through promises of differential privacy does not legitimize no-holds-barred access to data about individuals.

C. Privacy as Contextual Integrity

32. Until now, we have accepted the account of privacy as control over personal information, which has informed most commercial digital services, including major infrastructure-like platforms. In recent years an alternative, the theory of privacy as contextual integrity (CI), has gained traction. CI defines privacy as the *appropriate flow of information*. It adopts a conception of society comprised of multiple social domains (or "contexts"), which is elucidated in a social theory and entrenched by legal and political systems. Each of these domains, such as health care, finance, and education, is oriented around distinctive purposes, values and a distinct set of roles, practices, and guiding norms, including norms governing information flows. Information flows are *appropriate* if they conform with *contextual informational norms*. Informational norms are characterized by five parameters: data subject, sender, and recipient (collectively referred to as the actors), information type (or attribute), and transmission principles (the conditions that constrain data flow from senders to recipients).

33. The parameters of CI serve as precise instruments to determine the appropriateness of an information flow. Through CI's lens, the conception of privacy as control reduces privacy to only one parameter, the transmission principle, and only one value for that parameter, control.[67] By contrast, when evaluating whether privacy has been respected or violated, one must ascertain whether data flows are appropriate, which, in turn, involves mapping it against all five parameters.[68] When ascertaining how robust CI is, we note the connection between appropriateness as conformance with informational norms and a central idea of "reasonable expectation of privacy."

34. It is important to mention that informational norms themselves may be evaluated in terms of how well they serve respective contextual ends and purposes. For example, a norm governing confidentiality of patient information that prevents physicians from sharing that information broadly serves healthcare in a variety of ways, such as engendering patient trust to share key health data with the physician in service of the provision of quality healthcare. (More about the theory of contextual

[67] Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

[68] Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press.

integrity may be found in numerous other publications.)[69] Through CI's lens, HIPAA[70] is an interesting case, on the one hand validating the relevance of the five parameters in the structure of its privacy rules. Yet, on the other hand, covering only healthcare providers (and business associates) and omitting from its purview a host of health apps serving mental health, fertility, and menstrual tracking.[71] An evaluation of HIPAA, which draws on CI, would suggest evaluating flows of health-related data in terms of purposes and values of healthcare. To pursue this evaluation lies outside the scope of this Note.

35. Before returning to the practices of infrastructure-like intermediaries, such as Google and Apple in light of contextual integrity (CI), it is important to mention that a growing body of empirical work demonstrates that CI captures the ways people think about privacy and how they respond to questions about personal data collection, sharing, and use.[72] Key takeaways from recent empirical studies are that people's judgements on whether data practices described to them are acceptable or not is not based solely on whether data subjects control information about themselves. Neither can every piece of data be classified solely as "private" or "public." Instead, the judgement for data flow must be attuned to whether privacy expectations are met and, in turn, are sensitive to specific values for all five parameters. In other words, people may agree that a given data flow is acceptable even if the data in question is judged "sensitive," as long as the recipient is acceptable. As an example, mental health factors are expected to flow to a patient's psychiatrist.

D. The Il-logic of First Party vs. Third Party

[69] Nissenbaum, H. (2009). Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford University Press. Nissenbaum, H. (2019). Contextual Integrity Up and Down the Data Food Chain. Theoretical Inquiries in Law, 20:1, 221-256; Nissenbaum, H. & Patterson, H. (2016). Biosensing in Context: Health Privacy in a Connected World. In Quantified: Biosensing Technologies in Everyday Life. The MIT Press, 79-100. Ed. Nafus D.; Nissenbaum, H. (2015). Respect for Context as a Benchmark for Privacy Online: What it is and isn'. In Social Dimensions of Privacy. Cambridge University Press. Eds. Roessler B. & Mokrosinska D. (Reprinted in Privacy, Security and Accountability: Ethics, Law and Policy. (2016). Rowman & Littlefield International, 39-62. Ed. Moore, A.)

[70] The Health Insurance Portability and Accountability Act of 1996. (1996). GPO. Retrieved from: https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf

[71] See, for example: Federal Trade Commission. (2021). FTC Finalizes Order with Flo Health, a Fertility-Tracking App that Shared Sensitive Health Data with Facebook, Google, and Others [Press Release]. Retrieved from: https://www.ftc.gov/news-events/news/press-releases/2021/06/ftc-finalizes-order-flo-health-fertility-tracking-app-shared-sensitive-health-data-facebook-google

[72] Shvartzshnaider, Y. et al. (2018). Analyzing Privacy Policies Using Contextual Integrity Annotations. Available at SSRN: http://dx.doi.org/10.2139/ssrn.3244876; Shvartzschnaider, Y. ,Sanfilippo M. R., & Apthorpe, N. (2021). Contextual Integrity as a Gauge for Governing Knowledge Commons. Cambridge University Press. Governing Privacy in Knowledge Commons (Cambridge Studies on Governing Knowledge Commons). Eds. Sanfilippo, M., Frischmann, B., & Strandburg, K. ; Wijesekera, P. et al. (2015). Android permissions remystified: A field study on contextual integrity. 24th USENIX Security Symposium (USENIX Security 15).

36. Fueling the growing outrage over online tracking, was the negative sentiment against a morass of actors labeled "third parties," who were to be contrasted from "first parties." A convenient murkiness surrounds this distinction, which, originated in the development of Web standards surrounding cookies. First parties are any parties with the same top-level domain as the site that a user has intentionally visited. Third parties were all others who had been admitted to that site for a variety of secondary purposes, such as analytics or advertising. These concepts were developed at a time far simpler than the one we currently inhabit, including the ascendance of massive infrastructure-like services and massive walled gardens, such as Facebook/Meta. In the fallout of public deliberation and outrage over tracking the labels, first-party and third-party assumed a different meaning, roughly, acceptable and unacceptable. Adding more flesh to these, first parties might be described as, actors with whom individuals would expect to be sharing relevant data because they understand themselves to be engaged in a relationship (fleeting or continuous) with these actors, who would have a legitimate right to this data (e.g., street address to a delivery company). And third parties would be all others who may want or profit from this data but do not have a legitimate right to it.

37. It has been possible to exploit the elision of the technical distinction with the normative distinction because many ordinary, non-expert individuals (including lawmakers) conclude that the two distinctions are but one and the same. The entitlement of first parties is not challenged while a presumption exists against third-party access.

38. This elision of the technical with the normative has been quietly entrenched with results that are unexpected and unintuitive. Because, at this point in time, users almost always engage commercially or socially via dominant platforms, including browsers, search engines, social media sites, and iOS or Android, these intermediaries have eagerly assumed themselves to be "first parties," presumptively entitled to the data flowing between the commercial and social parties with whom the users are intentionally engaging. In other words, Google and Apple, as default, have assumed the mantle, "first party," which both permits untrammeled receipt of data generated in the transaction, at the same time empowering them to constrain access to others, whom they characterize as third parties. The irony is twofold. First, although the top-level domains of companies like Google and Apple cover a vast array of highly diverse services, the elision of technical and normative interpretations of first and third parties means they assume a green light to merging data from all these services.[73] As noted above, merging this data undermines the dominant approach to privacy through Notice and Choice. Second, in our view, most people would intuitively agree that the parties with whom they are interacting, e.g., websites they have clicked from search results, or services provided via mobile apps – to be first parties. This intuition is not ill-founded: who among us would believe that Verizon is first-

[73] Zimmer, M. (2008). Privacy on Planet Google: Using the Theory of "Contextual Integrity" to Clarify the Privacy Threats of Google's Quest for the Perfect Search Engine. Journal of Business & Technology Law, V. 3. Retrieved from: https://digitalcommons.law.umaryland.edu/cgi/viewcontent.cgi?article=1094&context=jbtl

party to the call with our friend, or that Federal Express is first-party to the contents of a package it is delivering?

39. Although dominant intermediaries, such as, Google and Apple have wholeheartedly embraced a "first-party" versus "third-party" distinction, which permits them first-party privileges while constraining access by alleged third parties they do not fully embrace the underlying technical definition. In particular, certain actors are deemed to have legitimate access to data flowing between individuals and a so-called third party even though these actors do not share top-level domains (e.g., sites that store user information in different domains for security reasons). To remedy this, Google, for example, has proposed grouping websites into First-Party Sets[74] based on ownership, common privacy policy, and "common group identity that is easily observable by users." The third would not be based on the actual feedback of users but determined by an "independent entity."

40. We see no problem with a more thoughtful approach to who is, and isn't entitled to data, based not solely on top-level domains. Common ownership, however, as a necessary criterion also makes little sense as an alternative. Instead, contextual integrity directs us to ask about the implications of data flows for data subjects and for achieving purpose and values of relevant contexts (i.e., "social integrity.")[75] Top-level domain and common ownership may be reasonable proxies but not necessarily the ideal grounds for untrammeled flow in a world of global companies extending across diverse data holdings. Privacy is not about respecting corporate ownership but about appropriate flow; drawing a line on the basis of the former may be arbitrary from the perspective of the latter.

41. In Google's case, remedying the ills of third-party tracking while aware of the irony of its own claims to first-party access, Google has proffered a series of ideas in their Privacy Sandbox, such as FLoCs and Topics.[76] These would allow Google to process (extract patterns) from massive datasets of individual data drawn across innumerable contexts in order to target individuals based on aggregate profiles. Although a discussion about these developments lies outside the scope of this Note, we remind readers of a point made above, namely, that differential treatment of a cluster of individuals may be as harmful as differential treatment based on individual attributes.

III. THE MOBILE "SMARTPHONE" LANDSCAPE

[74] Govind, K. & Sidhana, H. First-Party Sets. WICG. Accessed 21 April 2022. Retrieved from: https://github.com/WICG/first-party-sets

[75] Kim N. (2014). Three's a Crowd: Towards Contextual Integrity in Third-Party Data Sharing. Harvard Journal of Law & Technology, V. 28 No. 1. Retrieved from: http://jolt.law.harvard.edu/articles/pdf/v28/28HarvJLTech325.pdf

[76] Dutton, S. (2022) "The Topics API," Google. Retrieved from: https://developer.chrome.com/en/docs/privacy-sandbox/topics/

42. The walled-garden of mobile platforms is different from the mostly open Internet and Web in some ways.[77] There are, however, structural similarities between major platforms operating on the Web, such as browsers and social media companies and mobile platforms. In this section, we use Apple's iOS to illustrate the problem of private companies, in particular, privately owned infrastructure-like companies unilaterally filling the void left by technical developments that have outpaced privacy law and regulation.

43. Apple keeps a tight rein on the apps on iOS, restricting where they can be downloaded from (only Apple's App Store) and the data an app can access. Citing privacy as one of its justifications, Apple announces that it "puts privacy first by putting control in your hands,"[78] with measures like App Tracking Transparency (ATT), Privacy Nutrition Labels for apps in the App Store, and various consent prompts around information generated by the iPhone. The ATT consent prompt, in fact, nudges users to disable third-party tracking in apps by highlighting how such information is distributed: "We believe you should have a choice in how apps track and share your data with other companies for advertising or with data brokers."[79]

44. It seems fair to mention that Apple is not quite as fierce when alerting users to cross-app tracking by its own ad network. Instead of "Ask App Not to Track" in ATT,[80] for Apple's ad network, it offers "Turn off Personalized Ads" as an option, prefaced by a statement that includes "We protect your privacy" and the option to "Turn on Personalized Ads" prioritized and prominently highlighted.[81] It is *crucial* to emphasize that users who choose the option of turning off personalized ads are not necessarily freed from tracking; they may only be spared ads that are personalized, while tracking, which is a far more important factor from the perspective of privacy, continues in the background. Users are encouraged to allow Apple's ad network to utilize information about all of a user's app downloads and purchases (not merely Apple's own)[82] as well as location information, information about users' interactions with Apple News and Apple Stocks. Yet, at the same time assures users they are not being "tracked."[83]

---

[77] Zittrain, J. (2008). The Future of the Internet – And How to Stop It. Yale University Press & Penguin UK.

[78] Privacy | App Tracking Transparency | Apple. (2021). Apple. Retrieved from: https://www.youtube.com/watch?v=Ihw_Al4RNno

[79] Privacy | App Tracking Transparency | Apple. (2021). Apple. Retrieved from: https://www.apple.com/privacy/control/

[80] Clark, M. (2021). Apple's app tracking transparency feature isn't an instant privacy button. The Verge. Retrieved from: https://www.theverge.com/2021/12/11/22828713/apple-app-tracking-transparancy-psa-privacy-ads-cohorts

[81] Campbell, I.C. (2021). Apple will ask you before it targets you with its ads in iOS 15. The Verge. Retrieved from: https://www.theverge.com/2021/9/2/22654121/apple-personalized-ads-ios-15-prompt-app-tracking

[82] Competition and Markets Authority. (2021). Mobile ecosystems: market study interim report. Retrieved from: https://www.gov.uk/government/publications/mobile-ecosystems-market-study-interim-report

[83] Apple Advertising & Privacy. (2022). Apple. Retrieved from: https://www.apple.com/legal/privacy/data/en/apple-advertising/

45. Another privacy device on iOS is the Privacy Nutrition Label,[84] which requires apps to disclose details of data collection: uses (third-party advertising, app developer's advertising, etc.), data categories (e.g., location, health, and payment information), and whether data is individually identifiable. These privacy nutrition labels have limited efficacy as most users don't know about them and, as discussed earlier, are none the wiser about what data practices are relevant to privacy.[85] Any on-device processing, which is a significant aspect of Apple's strategy to extract knowledge from data, is not included as a field in these labels.[86] Finally, although Apple provides labels for its own apps, no such label exists for components of its operating system.

A. A special carveout for Apple?

46. Smartphone devices carry, on board, a vast array of sensors. Besides more familiar sensors, such as cameras, touchscreens, microphones, GPS receivers, and heart rate monitors, iPhones,[87] iPads, and Apple Watches[88] also include those less familiar, such as, lidars, magnetometers, barometers, and proximity sensors. To ordinary users, it is not entirely obvious that apps are receiving this sensorium from iOS and that the iOS is generating this data from a user's device. Stringent rules, which apps must follow, prescribe different permissions an app must seek from Apple and from users in order gain access to various types of sensor data. Location, one such type that has garnered significant attention, is regularly the subject of app consent-request pop-ups because it is deemed highly sensitive. Although users are becoming accustomed to apps popping location consent requests (e.g., Tinder or Google Maps) they may be unaware that acquiescing to these requests also opts them into granting Apple's iOS numerous "Systems Services" location data including "Significant Locations" (i.e., iOS tracks where users visit and when to determine which locations are "significant") and "Product Improvement" categories, e.g., "iPhone Analytics," "Routing & Traffic," and "Improve Maps."[89] The last three allow a device to transmit a spectrum of user location information to Apple, including Significant Location GPS coordinates,[90] speed of travel, barometric pressure, trip data, and times and

[84] App Privacy Details. (2022). Apple. Retrieved from: https://developer.apple.com/app-store/app-privacy-details/

[85] App Privacy Details. (2022). Apple. Retrieved from: https://developer.apple.com/app-store/app-privacy-details/

[86] App Privacy Details. (2022). Apple. Retrieved from: https://developer.apple.com/app-store/app-privacy-details/

[87] iPhone 13 Pro and 13 Pro Max - Technical Specifications. (2022). Apple. Retrieved from: https://www.apple.com/iphone-13-pro/specs/

[88] Which Apple Watch is right for you? (2022). Apple. Retrieved from: https://www.apple.com/watch/compare/

[89] Location Services & Privacy. (2022). Apple. Retrieved from: https://www.apple.com/legal/privacy/data/en/location-services/; Location Services Privacy Overview. (2019). Apple. Retrieved from: https://www.apple.com/privacy/docs/Location_Services_White_Paper_Nov_2019.pdf

[90] A user's list of Significant Locations is end-to-end encrypted and not readable by Apple (Location Services & Privacy. (2022). Apple. Retrieved from: https://www.apple.com/legal/privacy/data/en/location-services/),

locations of app usage for Apple product improvement, even when users do not use any of these services.[91] Even if users choose to opt out of all available options, using any location services still enlists their devices into improving Apple's database of Wi-Fi hotspot and cell tower locations.[92]

47. A review of Apple's privacy policy presents no clear picture of Apple's general collection and usage of the vast array of sensor data generated by devices like the iPhone.[93] Apple may justify its silence on grounds that, except where users have given expressed consent, any such data is "anonymized" and delinked from respective individual users before reaching Apple and as such lies outside the purview of the privacy policy. Apple's silence leaves important questions unanswered about how sensor data is handled, which may be relevant to privacy. For example, as long as location traces over time are maintained, stark demonstrations have shown that these persistent traces are almost impossible to deidentify.[94] It is unclear that anonymization techniques that retain linkages among sensor traces, besides location, of the same individual will succeed. We simply do not know enough about how Apple is handling these other streams of sensor data, whether or not these data are maintained as connected traces associated with individual users (even deidentified) or, for example, whether or not traces from multiple sensors from a single phone are linked together. Such aggregates might, for example provide insight into gait, which is a known biometric identifier.[95]

IV. PRIVATE ENFORCEMENT OF SOCIETAL VALUES – CONCLUSION

48. We have suggested that global platforms, including infrastructure-like companies, such as Apple and Google, have stepped into a void in privacy law and regulation, created by dramatic developments in digital technologies and data science. We do not question the early motivations of leaders, such as Tim Cook, who, in 2014, in the wake of the iPhoto scandal, made an explicit commitment to privacy.[96] In the short years since then, however, radical changes in the technical and economic ecosystem have

---

but anonymized correlations between GPS coordinates and street addresses of Significant Locations on a user's device are sent to Apple to improve Maps (Improve Maps & Privacy. (2022). Apple. Retrieved from: https://www.apple.com/legal/privacy/data/en/improve-maps/).

[91] Location Services & Privacy. (2022). Apple. Retrieved from: https://www.apple.com/legal/privacy/data/en/location-services/; Improve Maps & Privacy. (2022). Apple. Retrieved from: https://www.apple.com/legal/privacy/data/en/improve-maps/

[92] Location Services & Privacy. (2022). Apple. Retrieved from: https://www.apple.com/legal/privacy/data/en/location-services/

[93] It does include a section on "Research Sensor & Usage Data" feature in iOS, which governs the flow of "sensitive research data" (iOS 15.5. (2022). Apple.) for iPhone users who choose to enroll in research studies, for example, in health and wellness studies.

[94] Valentino-DeVries, J. et al. (2018). Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. New York Times. Retrieved from: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html

[95] Chellappa R., Veeraraghavan A., Ramanathan N. (2009). Gait Biometrics, Overview. Encyclopedia of Biometrics. Springer. Eds. Li, S.Z., Jain, A. Retrieved from: https://doi.org/10.1007/978-0-387-73003-5_33

[96] Cook, T. (2014). A message from Tim Cook about Apple's commitment to your privacy. Apple. Retrieved from: https://web.archive.org/web/20140918102737/http:/www.apple.com/privacy/

prompted urgent questions. In this Note, we have argued that the definition and enforcement of privacy should not remain in the hands of powerful, commercial interests.

49. We have obtained glimpses into the practices and policies of companies like Google and Apple through our study of published privacy policies, public statements, accounts in expert and public media, and our own grasp of smartphone app ecosystems. From these, we have not been convinced that the interpretations of privacy that these companies give, and lopsided enforcement, fit privacy as a public, societal value. Along the way, our scrutiny has rested most heavily on Apple because of its extravagant public claims of exceptional privacy standards, which (anecdotally) have seemed to hold sway with a largely trusting public, possibly also persuading lawmakers to hold back on regulatory intervention.

50. Furthermore, Apple has used these public pronouncements to justify a closed ecosystem of iOS apps, tightly under its control. In one instance, reacting to a legislative proposal which would compel Apple to allow "sideloading" of apps from stores other than its own App Store, Tim Cook warned in a speech at IAPP Summit 2022, "if we are forced to let unvetted apps onto iPhone, the unintended consequences will be profound."[97]

51. Based on our analysis, Apple may justly take its place among privacy leaders, like them, hobbled by privacy policies that are necessarily complex. We have argued that this approach leaves users no more "in control" of data about themselves in Apple's ecosystem than they are with any other good-faith company. In contrast, unlike the relationships that smaller, contextually bounded companies have with their customers, the potential privacy impacts and harms that companies with vast diverse holdings, such as Apple, Google, and Meta, are far greater and far more dire.

52. The lens of contextual integrity highlights sources of some of these problems. Platform intermediaries claim entitlement to data generated by a diverse array of independently owned apps, extension, etc. functioning atop their servers, with no apparent regard for context specific norms that govern the interactions between these independent businesses and their respective customers. In the case of Apple and specifically iOS, we did not detect sensitivity to contextual norms that arguably govern the data it captures, merges, and analyzes in its sweep of app transactions and sensors. For example, we detected no consideration to whether these data are drawn from contexts of health, religion, commerce, politics, education, or any others. Although massive, infrastructure-like companies may justify the exercise of power afforded through technology on grounds of privacy, we have greater faith in the potential of single service companies acting in good faith as stewards of contextual integrity. Blanket prohibitions on such companies, lacking evidence of data malpractice, may be

[97] Cook, T. (2022). Keynote: Tim Cook, Apple CEO (IAPP Global Privacy Summit 2022. IAPP. Retrieved from: https://iapp.org/news/video/keynote-tim-cook-apple-ceo-iapp-global-privacy-summit-2022/

unwarranted and it also may undermine efforts of app providers to serve and nurture their own ongoing relationship with clients.

53. Ferocious competition for access to data among firms in digital societies places individuals, institutions, and social integrity at great risk. Privacy has become far too important to leave it in the hands of stakeholders in the corporate fray to define and unilaterally enforce. Nor can we fall back on definitions and protocols that no longer are effective.