2021

The COVID-19 Pandemic and the Technology Trust Gap

Johanna Gunawan

David Choffnes

Woodrow Hartzog
Boston University School of Law

Christo Wilson

The COVID-19 Pandemic and the Technology Trust Gap

Johanna Gunawan,[*] David Choffnes,[**] Woodrow Hartzog[***] & Christo Wilson[****]

Industry and government tried to use information technologies to respond to the COVID-19 pandemic, but using the internet as a tool for disease surveillance, public health messaging, and testing logistics turned out to be a disappointment. Why weren't these efforts more effective? This Essay argues that industry and government efforts to leverage technology were doomed to fail because tech platforms have failed over the past few decades to make their tools trustworthy, and lawmakers have done little to hold these companies accountable. People cannot trust the interfaces they interact with, the devices they use, and the systems that power tech companies' services.

This Essay explores these pre-existing privacy ills that contributed to these problems, including manipulative user interfaces, consent regimes that burden people with all the risks of using technology, and devices that collect far more data than they should. A pandemic response is only as good as its adoption, but pre-existing privacy and technology concerns make it difficult for people seeking lifelines to have confidence in the technologies designed to protect them. We argue that a good way to help close the technology trust gap is through relational duties of loyalty and care, better frameworks regulating the design of information technologies, and substantive rules limiting data collection and use instead of procedural "consent and control" rules. We conclude that the

---

[*]Doctoral Student, M.S., Khoury College of Computer Sciences at Northeastern University.

[**]Associate Professor of Computer Science, Khoury College of Computer Sciences at Northeastern University.

[***]Professor of Law and Computer Science, School of Law and Khoury College of Computer Sciences at Northeastern University.

[****]Associate Professor of Computer Science, Khoury College of Computer Sciences at Northeastern University. The authors would like to thank the editors of the Seton Hall Law Review for their excellent edits and the participants of the Seton Hall Law Review Symposium on Privacy, Healthcare, and Artificial Intelligence for their questions and feedback. This work was partially funded by the Google ASPIRE (Android Security and Privacy Research) award.

pandemic could prove to be an opportunity to leverage motivated lawmakers to improve our privacy frameworks and make information technologies worthy of our trust.

I. INTRODUCTION

One of the factors that has made responding to the COVID-19 pandemic so difficult and frustrating is that industry's current strategy of building an app for every problem was ineffective. Silicon Valley created the world's most powerful surveillance network and tools to influence populations. But few people wanted to use proximity notification apps, and social media was a swamp of disinformation about the virus, treatments, and public health advice. Modern technology allows us to monitor the coronavirus's spread in detail and facilitate public health interventions—but only if people trust the tools they are being asked to use and the companies and governments they are dealing with. There is plenty to critique about the entire institutional and individual response to the pandemic, but the seeds of our collective inability to effectively utilize information technologies as part of our pandemic response were sown long ago. They just bloomed during the pandemic.

The rapid and sometimes heavy-handed implementation of pandemic-response technologies is emblematic of the complicated relationship between individuals and organizations who handle this data. We argue that industry and government efforts to leverage technology were doomed to fail because tech companies have failed over the past twenty years to make their tools trustworthy and

lawmakers have done little to hold these companies accountable. People cannot trust the interfaces they interact with, the devices they use, and the systems that power tech companies' services. Given this historical context, why would people trust their technology to aid them during a life-and-death public health crisis?

In this Essay, we explore the pre-existing ills that contributed to these problems, including manipulative user interfaces, consent regimes that burden people with all the risks of using technology, and devices that collect far more data than they should. A pandemic response is only as good as its adoption, but pre-existing privacy and technology concerns make it difficult for people seeking lifelines to have confidence in the technologies designed to protect them.

Our argument proceeds in three parts. First, in Part II, we outline efforts to use technology to respond to the pandemic and why they were fraught. As an example, we detail Google's Project Baseline, which aimed to help people identify COVID testing centers. We show how questionable requests and broken promises undermined the trustworthiness of the effort. We also describe concerns with other technological interventions, such as proximity notification apps and surveillance technologies. Next, in Part III, we explore one phenomenon that hobbled our technological response to COVID—technology's trust gap. Simply put, when people cannot trust the layout of the screens they interact with, the design of the devices they use, and the background decision-making of the systems they expose themselves to, people are not in a position to use these technologies in a public health crisis. We explore concepts such as dark patterns, insecure Internet of Things (IoT) devices, and algorithms that target the vulnerable and spread public health misinformation. Collectively, these problems give people little reason to feel safe using any digital technology, even if doing so would improve their health prospects.

In Part IV, we propose a way for lawmakers and industry to earn and ensure peoples' trust. We argue that a good way to help close the technology trust gap is through relational duties of loyalty and care, better frameworks regulating the design of information technologies, and substantive rules limiting data collection and use instead of procedural "consent and control" regimes. We conclude that the pandemic could provide an opportunity for motivated lawmakers to improve our privacy frameworks and make information technologies worthy of our trust.

II. DISAPPOINTING TECHNOLOGICAL INTERVENTIONS IN THE PANDEMIC

COVID required government and industry to act with unprecedented speed and scale. Thankfully, our existing technological infrastructure allows companies to implement solutions swiftly and broadly. Unfortunately, companies could not break bad habits developed from decades of information gluttony.[1] Technology presented users with questionable requests for additional information and broken data security promises before the pandemic. When people are desperate for a lifeline, they become ripe for exploitation when governments and corporations make questionable requests for data or misuse information they have collected. Even when companies set out to create a privacy-friendly intervention, such as Apple and Google's respective efforts to leverage their phones for proximity notification apps,[2] they are continuing to draw water from a well that Silicon Valley poisoned years ago. There are complex reasons why institutions had trouble leveraging technologies to respond to the pandemic. Much of this failure is intertwined with governmental shortcomings. But tech companies' questionable requests, broken promises, and techno-solutionism are a significant part of this story.

A. *Questionable Requests*

Data is an asset, and these days, an incredibly valuable one.[3] It powers the data economy,[4] which extracts user data and turns it into insights that can help peddle advertisements and personalization features in the world of digital commerce. To learn more about users, tech companies at all levels of the online experience amass billions of

---

[1] For a more detailed look at the pathologies of information capitalism, see generally JULIE COHEN, BETWEEN TRUTH AND POWER (2020).

[2] *Privacy-Preserving Contact Tracing*, APPLE, https://covid19.apple.com/contact tracing (last visited Apr. 04, 2021); *Exposure Notifications: Using Technology to Help Public Health Authorities Fight COVID-19*, GOOGLE, https://www.google.com/covid19/exposurenotifications/ (last visited Apr. 04, 2021).

[3] ALBERT OPHER ET AL., THE RISE OF THE DATA ECONOMY: DRIVING VALUE THROUGH INTERNET OF THINGS DATA MONETIZATION 16 (2016), https://www.ibm.com/downloads/cas/4JRO LDQ7.

[4] Ludwig Siegele, *A Deluge of Data Is Giving Rise to a New Economy*, ECONOMIST, (Feb. 20, 2020), https://www.economist.com/special-report/2020/02/20/a-deluge-of-data-is-giving-rise-to-a-new-economy; Knowledge@Wharton, *Data as Currency: What Value Are You Getting for It?*, WHARTON SCH. BUS. (Aug. 27, 2019), https://knowledge.wharton.upenn.edu/article/barrett-data-as-currency.

data points from which to mine these insights, but a question remains: is all of that data absolutely necessary to collect?[5]

In the early days of the pandemic in the United States, Alphabet's life sciences arm, Verily, began a program called Project Baseline to help people find COVID-19 testing centers and get screened before receiving a test.[6] The service was initially available in California but has since expanded to include several states across the U.S.[7] By October, however, some California cities shuttered their partnerships with Project Baseline, particularly due to the requirement that people seeking COVID-19 screenings must prove their identity through a Google Account or otherwise register for one—as well as account authentication hurdles for vulnerable populations like the homeless.[8]

Project Baseline's COVID-19 program eligibility requirements cite that an individual must be eighteen years of age or older, able to get to a test site, and willing to sign an authorization and consent form—but do not mention the mandatory Google Account as part of the eligibility criteria.[9] While Project Baseline assures that data used by the COVID-19 program is stored separately and not directly linked to an individual's Google Account,[10] the fact remains that individuals must accept the risk of surveillance or take on the burden of deleting the Google Account after receiving a screening.

While Verily's promises of data separation and limited use may be well and good, it is concerning that people seeking tests in a matter of life and death were required to consent to Google's entire data ecosystem to participate in public health safety guidelines. The homepage for the COVID-19 program describes it as "an effort to expand access to COVID-19 screening and testing," which few would argue against. Beyond this, Verily announced a partnership with Janssen

---

[5] Walter Frick, *Do Tech Companies Really Need All That User Data?*, HARV. BUS. REV. (Sept. 21, 2017), https://hbr.org/2017/09/do-tech-companies-really-need-all-that-user-data.

[6] *Verily, In Collaboration With The California Governor's Office, Federal, State, And Local Public Health Authorities, Will Launch Pilot Intended To Expand Access To COVID-19 Risk Screening And Testing For High Risk Individuals At Bay Area Locations,* PROJECT BASELINE (Mar. 15, 2020), https://blog.projectbaseline.com/2020/03/verily-in-collaboration-with-california.html.

[7] *COVID-19 Testing Program*, PROJECT BASELINE, https://www.projectbaseline.com/covid-19 (last visited Apr. 04, 2021).

[8] Jenny Gold & Pradhan Rachana, *Verily's COVID Testing Program Halted in San Francisco and Oakland*, KAISER HEALTH NEWS (Oct. 26, 2020), https://khn.org/news/verilys-covid-testing-program-halted-in-san-francisco-and-oakland; *COVID-19 FAQ*, PROJECT BASELINE, https://www.projectbaseline.com/covid-support.

[9] *COVID-19 Testing Program*, *supra* note 7.

[10] *COVID-19 FAQ*, *supra* note 8.

Research & Development to launch a new COVID-19-related study as part of Project Baseline, using data from screening users to determine eligible participants.[11] This follows a previous study launched by Verily, which began in May of 2020, to study immune responses to the virus.[12] Verily stated that study participants needed to have previous COVID-19 test results, but that these tests did not have to be conducted by Verily.[13] Considering that the original purpose of Project Baseline was to "make it easier for people to participate in clinical research,"[14] it is still unclear why Google Accounts are the only acceptable form of authentication for COVID-19 screening, when prerequisites to join the Verily studies do not require Verily tests.

A Google account-or-nothing consent regime in such distressing times is worrisome, even if COVID-19 data is kept separate from the greater Google ecosystem. Promises that data will remain siloed are hard to trust. In the early days of the pandemic, few other options for getting tests existed, and individuals should not have had to consent to tertiary services in their efforts to protect their health.

As many have pointed out, industry's values do not always align with the public interest, and this can create issues when trying to fashion technology-driven solutions to public problems.[15] It can be difficult to disentangle tech companies' benevolence in a pandemic with their profit-driven goals.

B. *Broken Promises*

When technology changes faster than individuals can understand and respond, people are put at a steep disadvantage when it comes to protecting their privacy. System designs that do not seriously protect privacy are vulnerable to mission creep and exploitation over time,

---

[11] Frank Vinluan, *Verily Joins with Janssen, Adding Covid-19 to Project Baseline Study*, MEDCITY NEWS (Feb. 9, 2021, 12:00 PM), https://medcitynews.com/2021/02/verily-joins-with-janssen-adding-covid-19-to-project-baseline-study; *Verily Partners with Janssen to Launch COVID-19 Immune Response Study*, VERILY LIFE SCI. (Feb. 8, 2021), https://verily.com/stories/verily-partners-with-janssen-to-launch-covid-19-immune-response-study.

[12] Elise Reuter, *Alphabet's Verily launches Covid-19 antibody study*, MEDCITY NEWS, (May 18, 2020), https://medcitynews.com/2020/05/alphabets-verily-launches-covid-19-antibody-study.

[13] *Id.*

[14] *New Baseline COVID-19 Research Project launches*, VERILY LIFE SCIS. (May 18, 2020), https://verily.com/stories/new-baseline-covid-19-research-project-launches.

[15] *See, e.g.*, Julie Cohen, Woodrow Hartzog, and Laura Moy, *The Dangers of Tech-Driven Solutions to COVID-19*, BROOKINGS INST. (June 17, 2020), https://www.brookings.edu/techstream/the-dangers-of-tech-driven-solutions-to-covid-19. *See generally* COHEN, *supra* note 1; FRANK PASQUALE, THE NEW LAWS OF ROBOTICS (2020).

whether through unprecedented data collection under promises of "temporary" pandemic purposes or through data being repurposed beyond its original goal. The whiplash of failed privacy promises leads to greater doubt and distrust in technologies intended to protect public health.

Singapore, one of the first countries to deploy contact tracing apps to track the spread of COVID-19 among its population, is a good example of how mission creep leads to broken promises and the erosion of trust. The country initially struggled with the adoption of their voluntary TraceTogether smartphone app.[16] First released in March 2020, the app was reportedly adopted by a mere 20% of the population by May,[17] when the app became mandatory for migrant workers.[18] To address the needs of citizens who do not use or prefer not to use a mobile phone, the Singaporean government provided physical proximity devices (called the TraceTogether Token) and made these available to Singaporeans in June.[19]

Both the app and the token use a custom protocol, BlueTrace, that collects information from either a smartphone or the token whenever devices with TraceTogether installed detect each other. This protocol facilitates proximity tracing by keeping records of who has come into proximate contact with one another. By November, nearly half of the country's residents had adopted the application[20] and a digital check-in system, SafeEntry,[21] but by then it seemed that the government would make the app or token mandatory for people visiting public facilities by

---

16 TRACETOGETHER, GOV'T OF SINGAPORE, https://www.tracetogether.gov.sg (last visited Apr. 04, 2021); Sarah Kreps et al., *Contact-tracing apps face serious adoption obstacles*, BROOKINGS INST. (May 20, 2020), https://www.brookings.edu/techstream/contact-tracing-apps-face-serious-adoption-obstacles.

17 Sarah Kreps et al., *supra* note 16.

18 Press Release, Singapore Ministry of Manpower, New Resources to Provide Better Care for Migrant Workers (May 27, 2020), https://www.mom.gov.sg/newsroom/press-releases/2020/0527-new-resources-to-provide-better-care-for-migrant-workers.

19 Press Release, Seniors to Receive First Batch of TraceTogether Tokens, Smart Nation Singapore (Jun. 28, 2020), https://www.sgpc.gov.sg/sgpcmedia/media_releases/sndgo/press_release/P-20200628-2/attachment/Media%20Release%20-%20Seniors%20to%20receive%20first%20batch%20of%20TraceTogether%20Tokens%2028062020.pdf.

20 Bobbie Johnson, *Some Prominent Exposure Apps are Slowly Rolling Back Freedoms*, MIT TECH. REV. (Nov. 23, 2020), https://www.technologyreview.com/2020/11/23/1012491/contact-tracing-mandatory-singapore-covid-pandemic.

21 SAFEENTRY, https://safeentry.gov.sg (last visited Feb. 23, 2021).

December 2020.[22] In mid-December, the target date for mandatory TraceTogether check-in was pushed back to early 2021.[23]

Then, in early January 2021, the Singaporean government announced that the police would be able to access data collected by the TraceTogether/SafeEntry system for use in seven categories of criminal offenses—contradicting claims the government made at launch that the technologies would be used solely for contact tracing, right as nearly 80% of the country's population had adopted the software.[24] A minister who previously touted the TraceTogether software as "purely for contract tracing" revealed that contract tracing data had already been used by the Singaporean police in a murder investigation.[25] TraceTogether's privacy policy was updated to reflect this revelation after the minister's announcement on January 4, 2021—almost a year after the app's initial release without this disclosure.[26]

Governments naturally want to commandeer powerful tools for their own purposes. Google and Apple are creating a playbook for governments on how our phones can be repurposed for all kinds of surveillance. Even large and powerful companies are subject to political pressure. Will tech companies that develop COVID information technologies be able to resist indefinitely governments' attempts to change the design of these tools? The U.S. government vacated its order to compel Apple into building a modified iOS that would allow them to bypass encryption protections, but can we always count on this backtracking?[27] Apple reportedly dropped its plan to allow users to

---

[22] Lester Wong, *Use of TraceTogether App or Token Mandatory By End Dec.*, STRAITS TIMES (Oct. 21, 2020), https://www.straitstimes.com/singapore/use-of-tracetogether-app-or-token-mandatory-by-end-dec; Lester Wong, *Singapore Cinemas to Begin Rolling Out Compulsory TraceTogether-Only Entry From Oct. 26*, STRAITS TIMES (Oct. 19, 2020), https://www.straitstimes.com/tech/singapore-cinemas-to-begin-rolling-out-compulsory-tracetogether-only-entry-from-oct-26.

[23] Press Release, Moving Into Phase Three of Re-Opening, Ministry of Health of Singapore (Dec. 14, 2020), https://www.moh.gov.sg/news-highlights/details/moving-into-phase-three-of-re-opening.

[24] Mia Sato, *Singapore's police now have access to contact tracing data*, MIT TECH. REV. (Jan. 5, 2021), https://www.technologyreview.com/2021/01/05/1015734/singapore-contact-tracing-police-data-covid.

[25] Amir Hussain, *TraceTogether Data Used by Police in One Murder Case: Vivian Balakrishnan*, YAHOO NEWS (Jan. 5, 2021), https://uk.news.yahoo.com/trace-together-data-used-by-police-in-one-murder-case-vivian-084954246.html.

[26] TRACETOGETHER, *supra* note 16.

[27] Romain Dillet, *Justice Department Drops Lawsuit Against Apple as FBI has now Unlocked Farook's iPhone*, TECHCRUNCH (Mar. 28, 2016), https://techcrunch.com/2016/03/28/justice-department-drops-lawsuit-against-apple-over-iphone-unlocking-case.

encrypt their backups in the cloud after the FBI complained.[28] This dam will not hold indefinitely.

A pandemic response clearly must escalate in proportion to the intensity of a global health crisis. Governments and private organizations can and should do what is necessary to stop the spread and protect human lives—but they should not overstep boundaries under a blanket excuse of public health. Mission creep violates our expectations of safety and privacy and makes us skeptical of government actions that may be repurposed post-pandemic.

C. *Techno-Solutionism*

One of the most predictable and often misguided trends of the smartphone era is tech companies and governments trying to solve complex social problems with apps.[29] "There's an app for that" is not just a marketing slogan[30]—it is an operating ethos for Silicon Valley. But overreliance on apps and technical solutions is not just a question of efficacy. It represents a massive opportunity cost, as it diverts valuable political capital and dominates public discourse when other more difficult, but more effective and sustainable, options are the wiser path.

One of the most high-profile technological pandemic interventions was Google and Apple's respective modifications of their phones' operating systems to accommodate proximity notification apps.[31] The project modified the iOS and Android operating systems to allow government health agencies to build apps that use a mobile phone's Bluetooth communication capabilities.[32] These apps would enable a person who tests positive for the coronavirus to send out an "exposure" notification to other app users' phones to alert them that their phones had been in the vicinity of the infected person's phone during a given period. People getting this information could decide whether to self-isolate or get tested.

To protect privacy, the system only used Bluetooth, did not collect location data, hid a user's identity, required permission to collect proximity data or upload data from the phones of people who test

---

[28] Joseph Menn, *Exclusive: Apple Dropped Plan for Encrypting Backups After FBI Complained--Sources,* REUTERS (Jan. 21, 2020), https://www.reuters.com/article/us-apple-fbi-icloud-exclusive/exclusive-apple-dropped-plan-for-encrypting-backups-after-fbi-complained-sources-idUSKBN1ZK1CT.

[29] *See, e.g.*, EVGENY MOROZOV, TO SAVE EVERYTHING, CLICK HERE (2013).

[30] Brian Chen, *Apple Registers Trademark for 'There's an App for That'*, WIRED (Sept. 10, 2010), https://www.wired.com/2010/10/app-for-that.

[31] Steph Hannon, *Exposure Notifications: End of Year Update*, GOOGLE (Dec. 11, 2020), https://blog.google/inside-google/covid-19/exposure-notifications-end-year-update.

[32] *See supra* note 2.

positive for COVID-19, and stored all data locally on a user's phone unless the user decided to notify others.[33] Additionally, the companies required users to enter a unique code provided by health authorities to notify nearby users that they have been infected.[34]

Adoption of this contact tracing technology, both by governments and citizens, varied widely. In the United States, efforts to roll out apps with Exposure Notification features must be conducted at the state level, with the app approved only in nineteen U.S. states as of December 2020.[35] For some states, adoption levels among the population were lower than 10% even after months of the apps' availability.[36] In other regions, numbers are more promising[37] but still fall short of ideal.

The public has good reason to view COVID apps with a critical eye. First, tech platforms can only control so much. For example, Google and Apple promised to serve as staunch gatekeepers of the system they created by only allowing government health authorities to use the Exposure Notification tracing capabilities.[38] To protect civil liberties, the companies said they would not allow other government agencies to mandate use of the app (presumably by denying them system access). That does not prevent other parties like employers and schools, who are not bound by the platforms' terms of use for app developers, from requiring app participation as a condition of employment or entrance. It is also unclear how well Apple and Google can police the app operators to ensure that the apps comply with the rules. How can policymakers help guarantee system-wide fidelity when it is so easy for things to fall through the cracks?

But perhaps the biggest reason people are rightfully distrustful of an app-based approach to complex social problems is the concept of path dependency—the idea that norms, history, and technical and organizational structure make diverting from a particular path difficult. Once deployed, information tools, systems, and practices are unlikely to be "rolled back." Governments and tech platforms repeatedly touted

---

[33] APPLE, INC. AND GOOGLE, EXPOSURE NOTIFICATIONS FREQUENTLY ASKED QUESTIONS (2020), https://static.googleusercontent.com/media/www.google.com/en//covid19/exposurenotifications/pdfs/Exposure-Notification-FAQ-v1.2.pdf.

[34] *WI Exposure Notification App Privacy Policy*, WIS. DEP'T OF HEALTH SERVS. (Dec. 23, 2020), https://www.dhs.wisconsin.gov/covid-19/app-privacy.htm.

[35] Asmae Fahmy, *Google and Apple Join Forces to Bolster Contact Tracing*, VERYWELL HEALTH (Dec. 21, 2020), https://www.verywellhealth.com/google-apple-exposure-notification-covid-5092947; Alejandro De La Garza, *People are Finally Downloading COVID-19 Exposure Notification Apps. Will They Make a Difference?*, TIME (Dec. 14, 2020), https://time.com/5921518/covid-exposure-notification-apps.

[36] De La Garza, *supra* note 35.

[37] Hannon, *supra* note 31.

[38] EXPOSURE NOTIFICATIONS FREQUENTLY ASKED QUESTIONS, *supra* note 33.

contact tracing apps and COVID-19-related surveillance as temporary measures for use only until the pandemic passes. That is likely to be a fantasy.

Surveillance inertia is remarkably difficult to resist. Norms get set, and practices and tools become entrenched. And who can say when this will wind down? We are still dealing with the supposedly temporary surveillance authorized almost twenty years ago in the wake of 9/11. Rollbacks are rare and highly unlikely because the tools we build today create a path dependency that will shape our future data and surveillance practices.

There are significant opportunity costs and switching costs for such heavy investments in these contact tracing apps. This tech-first approach was less effective than governments hoped. But industry and government do not often have the resolve and humility to double back and try a different approach. Plus, the time lost to proximity notification, which governments could have used to coordinate better tools for public health messaging and a more effective and equitable public health rollout, is time we cannot get back.

Silicon Valley tries to make all tasks easier. Tech platforms see the costs associated with searching, sharing, and sorting as things to be eliminated. But in the wake of countless privacy lapses on social platforms and an unending wave of data breaches, it is clear that making tasks easier, even important ones, can have the potential to cause great collateral harm. The public is coming around to this. Tech companies' crisis of trust should come as no surprise to anyone.

III. A LACK OF TRUST IN TECHNOLOGIES

It turns out that Silicon Valley's approach of "moving fast and breaking things" does not inspire a lot of confidence. In this Part we will explore how the concerns that plagued pandemic-response technologies were present well before the virus began to spread. We consider three specific untrustworthy contexts: individuals cannot trust the content and interfaces before their eyes, they cannot trust the devices and software they use to keep their data safe, and they cannot trust that their data would not be abused or used against them.

Privacy and trust are intuitively connected. We disclose our secrets only to trusted individuals in real life if we can help it and try to reveal only public or benign information to new acquaintances. In technology, information and computer security rely on myriad authentication methods to verify whether parties in communication with one another, be they computer or device or human, can be trusted to continue with data transfer. In law, privacy takes many interpretations, but trust is

one option that defines privacy within relational contexts—especially for information relationships.[39]

When people cannot trust the tools they use, they will withdraw or be hurt and misguided. Technology's trust gap existed before the pandemic and is likely to continue long after it. Until lawmakers ensure that tech companies will respect peoples' trust, the same problems will exist when lawmakers and industry try to leverage information technologies to respond to the next public health emergency. In this Part, we expand upon the privacy problems we outlined in Part II. We break our analysis down into three areas of user inter interaction: an interface and information level, a device and security level, and a systemic, organizational level.

A. *Interfaces and Information*

The internet has a legitimacy problem, even during a pandemic. As people are encouraged to stay at home and socially distance, the resultant uptick in internet use exacerbates existing problems with interface design elements in software and apps as well as the alarming rate of misinformation across social media.

'Dark patterns,' which are software interfaces crafted to trick users into activities they did not otherwise intend to perform, plagued the screens of people looking to their tools for help during the pandemic.[40] Some dark patterns can lead to financial consequences, such as patterns employed to get users to purchase additional services in online

---

[39] *See generally* DANIEL SOLOVE, THE DIGITAL PERSON 42–45 (2006); ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE 7 (2018); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1187 (2016); Jack Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 14 (2020); Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611, 612 (2015); Lauren Scholz, *Fiduciary Boilerplate*, 46 J. CORP. L. 143 (2020); Ian Kerr, *The Legal Relationship Between Online Service Providers and Users*, 35 CAN. BUS. L.J. 419, 446 (2001); Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431 (2016); Neil Richards & Woodrow Hartzog, *Privacy's Trust Gap: A Review*, 126 YALE L.J. 1180, 1185 (2017); Neil Richards & Woodrow Hartzog, *Trusting Big Data Research*, 66 DEPAUL L. REV. 579 (2017); Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 4 EUROPEAN DATA PROT. L. REV. 1, 3 (2020); Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law* (forthcoming 2021); Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in A Networked World*, 69 U. MIAMI L. REV. 559, 560 (2015); Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 CASE W. RES. L. REV. 193 (2016). *But see* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 498 (2019).

[40] Harry Brignull, *Dark Patterns: Deception vs. Honesty in UI Design*, A LIST APART (Nov. 1, 2011), https://alistapart.com/article/dark-patterns-deception-vs-honesty-in-ui-design; Colin M. Gray, et al., *The Dark (Patterns) Side of UX Design*, *in* PROCEEDINGS OF THE 2018 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS, 1, 1–14 (2018), http://dl.acm.org/citation.cfm?doid=3173574.3174108.

shopping contexts.[41] Others may have privacy consequences, such as "Bad Defaults,"[42] which are default settings that are set to the options that benefit user privacy least. Dark patterns are the dark underbelly of persuasive technologies[43] or nudges—designs that facilitate an individual's decision-making toward a specific outcome.[44] Both dark patterns, or "sludges,"[45] and nudges exploit cognitive biases.[46] The difference lies in who benefits from the outcomes of an individual's nudged choices. Research on dark patterns spans several disciplines, including behavioral economics, psychology, computer science, human-computer interaction, and law.

All interface designs influence people one way or another. Choice architecture cannot be avoided or "wish[ed] [] away."[47] People are inundated with daily choices, and even more so when using digital technologies—the number of choices is overwhelming.[48] Choices must be constrained within the services we use.[49] When it comes to privacy, however, individuals' autonomy and control over their data must be improved, rather than eroded, through the use of dark patterns.[50]

---

41 Arunesh Mathur, et al., *Dark Patterns at Scale: Findings from a Crawl of 11K Shopping Websites*, 3 PROC. ACM HUM-COMPUT. INTERACTIONS 1, 2 (2019) [hereinafter *Dark Patterns at a Scale*]; Arunesh Mathur, et al., *What Makes a Dark Pattern... Dark? Design Attributes, Normative Considerations, and Measurement Methods*, *in* PROCEEDINGS OF THE 2021 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1, 13 (forthcoming 2021) [hereinafter *What Makes a Dark Pattern...Dark?*], http://arxiv.org/abs/2101.04843.

42 Christoph Bosch et al., *Tales from the Dark Side: Privacy Dark Strategies and Privacy Dark Patterns*, 2016(4) PROC. ON PRIV. ENHANCING TECHS. 237, 248 (2016); Ari Ezra Waldman, *Cognitive Biases, Dark Patterns, and the "Privacy Paradox"*, 31 CURRENT ISSUES IN PSYCH. 105, 105, 107–09 (2020).

43 B. J. FOGG, PERSUASIVE TECHNOLOGY: USING COMPUTERS TO CHANGE WHAT WE THINK AND DO 213 (1st ed. 2002).

44 RICHARD H. THALER & CASS SUNSTEIN, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS (2009).

45 Richard H. Thaler, *Nudge, Not Sludge*, 361 SCI. MAG. 431 (Aug. 3, 2018), https://science.sciencemag.org/content/361/6401/431; Stuart Mills, *Nudge/Sludge Symmetry: On the Relationship Between Nudge and Sludge and the Resulting Ontological, Normative and Transparency Implications*, BEHAVIOURAL PUB. POL. 1, 12 (2020); Olivia Goldhill, *Politicians Love Nudge Theory. But Beware its Doppelgänger "Sludge"*, QUARTZ (July 31, 2019), https://qz.com/1679102/sludge-takes-nudge-theory-to-new-manipulative-levels.

46 *See generally* Waldman, *supra* note 42, at 2; *see also Dark Patterns at a Scale*, *supra* note 41; *What Makes a Dark Pattern...Dark?*, *supra* note 41.

47 Cass R. Sunstein, *The Ethics of Nudging*, 32 YALE J. REGUL. 413, 449 (2015), https://digitalcommons.law.yale.edu/yjreg/vol32/iss2/6.

48 Woodrow Hartzog, *The Case Against Idealising Control*, 4 EUROPEAN DATA PROT. L. REV. 423, 429 (2018).

49 *Id.* at 426.

50 *See generally* Bosch, et al., *supra* note 42.

In a pandemic, people flock not only to government-recommended applications or health-related applications like Project Baseline[51] but also to social software and platforms. Strict lockdown measures and severe adjustments to quotidian living led to sharp increases in the usership of several applications, many of which offered free or discounted versions of their service at the beginning of the pandemic.[52] The cognitive bias of framing, however, intensifies in severity during a pandemic. Framing selectively chooses aspects of a given reality and amplifies them, typically resulting in different interpretations of the item being described.[53] It adds different weight to an object and influences how a person might perceive it, often to encourage certain conclusions over others—for better or worse, depending on how the framing is applied. When it comes to privacy, how an application frames a feature will impact whether people consider it to be privacy-protective or secure, regardless of how secure a feature truly is. Framing, then, contains the potential to obfuscate problems regardless of intent, sometimes in manipulative ways. In pandemic times, people are juggling additional stressors, from health and safety to adjusted living situations, and the available mental energy for carefully screening each decision for potential manipulation is low in supply.

The urgency of a global health crisis changes the way people perceive lifelines like contact tracing apps or other digital socialization software. When apps offer free services under a banner of altruism or helpfulness but fail to inform new, tentative users of the ad or third-party tracking software already built into their service, they exploit individuals' limited mental resources during an already difficult time. Compounded with dark patterns, like requiring account creation or providing credit card information for free trials, these 'altruistic' offers only add to a person's burdens.[54] Some communication and remote socialization apps exploded in popularity during the early months of the pandemic, when people sought ways to interact under social distancing guidelines. But one such app, HouseParty, was rife with dark patterns that prodded users into providing the app with their contact lists,

---

[51] PROJECT BASELINE, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.google.android.apps.baselinestudy&hl=en_US.

[52] Chance Miller, *These Apps and Services are Responding to Coronavirus Pandemic with Free Information*, 9TO5MAC (Apr. 2, 2020), https://9to5mac.com/2020/04/02/apps-and-services-coronavirus.

[53] Robert M. Entman, *Framing: Toward Clarification of a Fractured Paradigm*, 43 J. COMMC'N 51, 51–58 (1993).

[54] Woodrow Hartzog et al., *Beware of Apps Bearing Gifts in a Pandemic*, BERKMAN KLEIN CTR. COLLECTION (Aug. 18, 2020), https://medium.com/berkman-klein-center/beware-of-apps-bearing-gifts-in-a-pandemic-490fabaade01.

Facebook friend lists, and unnecessary smartphone permissions—and HouseParty's privacy policy indicates that individuals' information may be used by third parties, other vendors, and their parent organization.[55] Positive framing manipulates users' cognitive resources and glosses over the negatives or existing problematic data collection policies of such services.[56]

Governments have attempted to address dark patterns through legislation, though such changes have yet to be enacted. The Deceptive Experiences to Online Users Reduction (DETOUR) Act of 2019 aims to prohibit deceptive user interfaces. The Act considers dark patterns as interfaces with the effect of "obscuring, subverting, or impairing user autonomy, design-making, or choice to obtain consent or user data."[57] The California Privacy Rights Act of 2020 (CPRA) amended the California Consumer Privacy Act (CCPA) and explicitly mentions dark patterns specific to consent regimes, stating that "agreement obtained through use of dark patterns does not constitute consent."[58] Yet there is no federal law that prohibits companies from leveraging peoples' limited resources and abilities against them in an adversarial way that benefits the company at the expense of the person.

Misinformation is also a scourge online. There is some reason to believe that the copious amount of misinformation that social media companies amplify is not as consistently effective at duping people as some headlines might suggest.[59] There is plenty of reason, however, to be concerned about the fact that misinformation takes up so much real estate in our information diets and headspace, crowding out important truths and vital public health messaging. Giving people the choice to pick which information is "true" leads to people choosing false information as their guiding light or leads to people disengaging from information altogether out of decision fatigue. In both cases, failing to prevent the proliferation of false information amplifies the risk of encountering bad outcomes. Additionally, there is evidence that algorithmic filtering might facilitate or strengthen echo chambers where people are connected to ideas that they are prone to agree with.[60]

---

55 HOUSEPARTY PRIVACY POLICY, https://houseparty.com/privacy-policy.

56 Waldman, *supra* note 42, at 106.

57 Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/1084/text.

58 CALIFORNIA PRIVACY RIGHTS AND ENFORCEMENT ACT OF 2020 (CCPA), CAL. CIV. CODE § 1798.100-1798.199 (2020).

59 *See generally* Miriam J. Metzger et al., *From Dark to Light: The Many Shades of Sharing Misinformation Online*, 9 MEDIA AND COMMN'C 134, 134–43 (2021).

60 Uthsav Chitra & Christopher Musco, *Analyzing the Impact of Filter Bubbles on Social Network Polarization*, *in* PROCEEDINGS OF THE 13TH INTERNATIONAL CONFERENCE ON WEB

Misinformation can negatively affect public health, racial justice, democracy, and the strength of our commitment to public institutions. During the pandemic, misinformation messaging is associated to public health concerns like vaccine hesitancy and misperceptions of mask-wearing efficacy,[61] as well as racial rumormongering.[62] Even if the majority of netizens disbelieves online misinformation, the consequences of misinformation accepted as truth by some individuals risk lives and safety.

The interfaces and information passing before netizens' eyes were already untrustworthy before the pandemic. But the stakes were raised when severe illness and risk of death were added to the list of potential consequences of manipulative content.

B. *Applications and Devices*

Both smartphone apps and IoT devices can host security vulnerabilities and privacy problems. Frequent discoveries of data leaks and breaches make it difficult to trust the devices we use, and even more difficult at a time when this trust is most crucial.[63]

While a 'bulletproof' app or smart device is a thing of fantasy, the constant discovery of leaks and security issues in computer science research leads to frayed trust in the promises made by application markets or platforms like Android and iOS. Some apps exfiltrate audio, videos, and screenshots from an individual's device to third parties;[64] some apps' privacy risk varies from version to version.[65] Sometimes the

---

SEARCH AND DATA MINING 115, 115–23 (2020), https://doi.org/10.1145/3336191.3371825; John Kelly & Camille Francois, *This Is What Filter Bubbles Actually Look Like*, MIT TECH. REV. (Aug. 22, 2018), https://www.technologyreview.com/2018/08/22/140661/this-is-what-filter-bubbles-actually-look-like; Zoe Schiffer, *'Filter Bubble' Author Eli Pariser on why we need Publicly Owned Social Networks*, VERGE (Nov. 12, 2019), https://www.theverge.com/interface/2019/11/12/20959479/eli-pariser-civic-signals-filter-bubble-q-a.

[61] Robert Hornik, Ava Kikut, Emma Jesch, Chioma Woko, Leean Siegel & Kwanho Kim, *Association of COVID-19 Misinformation with Face Mask Wearing and Social Distancing in a Nationally Representative US Sample*, HEALTH COMMUN. (Nov. 22, 2020), https://pubmed.ncbi.nlm.nih.gov/33225745.

[62] *Misinformation on Novel Coronavirus Impacting Asian American Businesses*, PBS NEWSHOUR (Feb. 18, 2020), https://www.pbs.org/newshour/health/misguided-virus-fears-hitting-asian-american-businesses.

[63] *See* DANIEL J. SOLOVE & WOODROW HARTZOG, BREACHED! WHY DATA SECURITY FAILS AND HOW TO IMPROVE IT (forthcoming 2021) (on file with author).

[64] Elleen Pan et al., *Panoptispy: Characterizing Audio and Video Exfiltration from Android Applications*, 2018 PROC. ON PRIV. ENHANCING TECHS. 33, 33–50 (2018).

[65] Jingjing Ren et al., *Bug Fixes, Improvements,...and Privacy Leaks--A Longitudinal Study of PII Leaks Across Android App Versions*, *in* PROCEEDINGS OF THE 2018 NETWORK AND DISTRIBUTED SYSTEMS SECURITY SYMPOSIUM (2018), https://www.ndss-symposium.org/wp-content/uploads/2018/02/ndss2018_05B-2_Ren_paper.pdf.

same online service leaks different information in app form versus desktop browser form.[66]

Problems with leaky devices make it difficult to trust IoT solutions to the pandemic. Smart devices encompass a wide range of functionality enabled by rich sensors like microphones, cameras, and thermostats, and recent work finds that they not only exfiltrate potentially sensitive data like private conversations[67] but also send data to third parties and exhibit behavior that allows eavesdroppers to infer user activity.[68] Encryption, while necessary and useful, in some cases cannot hide the types of device interactions that create network traffic, which may allow an "eavesdropper to infer [the] devices in [a] consumer's network and how they are used."[69] Leaks aside, IoT data may be used against consumers even when they are aware of the data collection; health organizations like insurance providers have used smart toothbrushes and in-car trackers to adjust customers' rates.[70] This information is not comforting in the scope of COVID-19, when surveillance technologies have been deployed to inspect individuals' temperatures, movements, and compliance with government orders.

In the rush to find better treatments and a cure, the medical field can turn to technology for solutions. Some consider IoT a potentially helpful tool in the arsenal against the virus,[71] but discussions of IoT's

---

66 Christophe Leung et al., *Should You Use the App for That? Comparing the Privacy Implications of App- and Web-Based Online Services*, *in* IMC '16: PROCEEDINGS OF THE INTERNET MEASUREMENT CONFERENCE 365, 365–72 (2016), https://doi.org/10.1145/2987443.2987456.

67 Daniel J. Dubois et al., *When Speakers Are All Ears: Characterizing Misactivations of IoT Smart Speakers*, 2020 PROC. ON PRIV. ENHANCING TECHS. 255, 255–76 (2020).

68 Jingjing Ren et al, *Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach*, *in* IMC '19: PROCEEDINGS OF THE INTERNET MEASUREMENT CONFERENCE 267, 267–79 (2019), https://doi.org/10.1145/3355369.3355577; Said Jawad Saidi et al., *A Haystack Full of Needles: Scalable Detection of IoT Devices in the Wild*, *in* IMC '20: PROCEEDINGS OF THE INTERNET MEASUREMENT CONFERENCE 87 (2020), https://arxiv.org/abs/2009.01880.

69 *Id.*

70 Christina Farr, *This Start-Up Made Connected Toothbrushes--Now it Aims to Overthrow the 'Primitive' Dental Insurance Industry*, CNBC (May 15, 2018), https://www.cnbc.com/2018/05/15/beam-dental-raises-22-million-from-kleiner-to-change-dental-insurance.html; Lee Rainie & Maeve Duggan, *Auto Trackers Not Worth Car Insurance Discounts, Most Say*, PEW RSCH. CTR. (Jan. 14, 2016), https://www.pewresearch.org/internet/2016/01/14/scenario-auto-insurance-discounts-and-monitoring; Tracy Vence, *Why We Don't Recommend Smart Toothbrushes*, N.Y. TIMES (2020), https://www.nytimes.com/wirecutter/blog/smart-toothbrushes-dont-recommend.

71 Ravi Pratap Singh et al., *Internet of Things (IoT) Applications to Fight Against COVID-19 Pandemic*, 14 DIABETES & METABOLIC SYNDROME: CLINICAL RSCH. & REVS. 521, 521–24 (2020).

merits in a pandemic response cannot take place without accounting for the problems with IoT. Technologies proposed for battling COVID-19 include small tokens like TraceTogether's but can also take more alarming forms, like unmanned aerial vehicles (UAVs)[72] and thermal facial recognition devices.[73] Additional software has improved facial recognition capabilities and accounts for mask-wearing,[74] adding to a slew of prior concerns over facial recognition.[75] IoT's virus-fighting benefits cannot be uncoupled from serious ethical concerns, yet some researchers scrambling for a solution have omitted the latter while focusing only on the efficiency of such tools.[76] While the severity of COVID-19 calls for some forms of compromise, the additional risks of strategies like using GPS data for exposure tracing or passive temperature monitoring are still unknown and require stricter scrutiny.[77]

Coupled with the unprecedented levels of data collection that IoT and smartphone sensors are capable of (especially at a global pandemic scale), it is difficult to view the benefits of such tracking technologies as outweighing the risks.

C. *Systems and Intentions*

A third area of distrust is at an organizational, systemic level. Not only is it difficult to trust the algorithms and technical systems underlying the tools we use but it is additionally difficult to trust those who produce these tools. A technology cannot be decoupled from the organization that builds it when considering trust; a well-meaning technology company may have biased algorithms, and even hypothetically just, fair, and accountable technology may be deployed by a company that means to sell it to information-greedy organizations. Both the tool and the organization must be trustworthy for people to feel comfortable sharing their data.

---

[72] *See generally* V. Chamola et al., *A Comprehensive Review of the COVID-19 Pandemic and the Role of IoT, Drones, AI, Blockchain, and 5G in Managing its Impact*, 8 IEEE ACCESS 90225 (2020).

[73] Meredith Van Natta et al., *The Rise and Regulation of Thermal Facial Recognition Technology During the COVID-19 Pandemic*, 7 J.L. BIOSCIENCES (forthcoming 2021), https://doi.org/10.1093/jlb/lsaa038.

[74] *Face Recognition Software Shows Improvement in Recognizing Masked Faces*, NAT'L INST. STANDARDS AND TECH. (Dec. 1, 2020), https://www.nist.gov/news-events/news/2020/12/face-recognition-software-shows-improvement-recognizing-masked-faces.

[75] Antoaneta Roussi, *Resisting the Rise of Facial Recognition*, 587 NATURE 350, 350–53 (2020).

[76] Chamola et al., *supra* note 72.

[77] Van Natta et al., *supra* note 73.

Misinformation's filter bubble theory, in which personalization algorithms may isolate users into information 'bubbles' or echo chambers,[78] is concerning as-is, especially when considering the radicalized that susceptible individuals are exposed to online. The danger of filter bubbles, however, is not only in the content but also in the logic that determines how people receive content. Algorithms facilitate at-scale automation and improved efficiency when operating with many users' data, but they are not immune from severe flaws like bias and discrimination either from faulty training sets or the algorithm design itself. It is not only content delivery algorithms that are in question, but advertising delivery ones as well—studies have found that platform advertising algorithms may deliver ads that skew along race and gender lines, even when the advertiser did not so intend.[79] The potential for discrimination through advertising is pervasive, even when platforms provision rules and categories intended to protect against it.[80] Biased outcomes from ad delivery networks can arise across both demographic[81] and political lines,[82] eroding trust in the content placed before individuals and the platforms that service them.

For a pandemic-specific case, Facebook updated their advertising policies specifically for COVID-19 in reaction[83] to findings that their ad delivery system approved and accepted highly dangerous, misinformed advertisements, like those citing bleach as a cure for the virus.[84] A reactionary response is better than no response. Such advertisements could have real damage even within short timeframes for

---

[78] Eli Parisoer, *The Filter Bubble: What the Internet is Hiding From You,* Penguin (2011).

[79] Ailsa Chang, *How Facebook Wants to Handle Misinformation Around the Coronavirus Epidemic,* NPR (March 25, 2020), https://www.npr.org/2020/03/25/821591134/how-facebook-wants-to-handle-misinformation-around-the-coronavirus-epidemic; Kaveh Waddell, *Facebook Approved Ads with Coronavirus Misinformation,* CONSUMER REPS. (April 27, 2020), https://www.consumerreports.org/social-media/facebook-approved-ads-with-coronavirus-misinformation.

[80] Giridhari Venkatadri & Alan Mislove, *On the Potential for Discrimination via Composition, in* PROCEEDINGS OF THE 2020 ACM INTERNET MEASUREMENT CONFERENCE 333, 333–44 (2020), https://dl.acm.org/doi/10.1145/3419394.3423641.

[81] Muhammad Ali et al., *Discrimination Through Optimization: How Facebook's Ad Delivery Can Lead to Biased Outcomes,* 3 PROC. ACM HUM.-COMPUT. INTERACTIONS 1–30 (2019); Venkatadri & Mislove, *supra* note 80.

[82] Muhammad Ali et al., *Ad Delivery Algorithms: The Hidden Arbiters of Political Messaging* (Mar. 2021), *in* PROCEEDINGS OF THE 14TH ACM INTERNATIONAL CONFERENCE ON WEB SEARCH AND DATA MINING, https://dl.acm.org/doi/10.1145/3437963.3441801.

[83] *Information on Advertising Policies about COVID-19,* FACEBOOK, https://www.facebook.com/business/help/1123969894625935, (last visited Feb. 11, 2021).

[84] Waddell, *supra* note 79.

exposure—and it is still difficult to be sure that all dangerous advertisements are effectively filtered from the platform.

Trusting or mistrusting an algorithm, however, is different from being able to trust the organization handling your data. Already concerned about abuses of their data in technology they use, people are especially worried when the incentives of the companies processing their data are murky—or outright controversial. Kashmir Hill's groundbreaking piece on Clearview AI in January 2020[85] shocked the world—how could laypeople have known that a secretive facial recognition start-up was scraping the internet for their photographs, let alone selling this data to law enforcement?[86] The slew of reactions that followed included cease-and-desists from the companies from whom Clearview scraped public data,[87] several class action lawsuits over Clearview's data collection,[88] and considerable discourse over the statutory immunity given to Internet service providers regarding liability for hosting the content of third parties.[89] Companies using Clearview's dataset were under fire as well, with class action lawsuits filed against them for their patronage.[90]

---

[85] Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES (Jan. 18, 2020) https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

[86] Elizabeth Lopatto, *Clearview AI CEO Says 'Over 2,400 Police Agencies' are Using its Facial Recognition Software*, VERGE (Aug. 26, 2020), https://www.theverge.com/2020/8/26/21402978/clearview-ai-ceo-interview-2400-police-agencies-facial-recognition.

[87] *Clearview AI Responds to Cease-and-Desist Letters by Claiming First Amendment Right to Publicly Available Data*, HARV. J.L. & TECH., https://jolt.law.harvard.edu/digest/clearview-ai-responds-to-cease-and-desist-letters-by-claiming-first-amendment-right-to-publicly-available-data; *Google, Youtube, Venmo and LinkedIn Send Cease-and-Desist Letters to Facial Recognition App That Helps Law Enforcement*, CBS NEWS (Feb. 5, 2020, 6:25 AM), https://www.cbsnews.com/news/clearview-ai-google-youtube-send-cease-and-desist-letter-to-facial-recognition-app.

[88] Amanda Bronstad, *NY-Based Facial Recognition Tech Company Wrangles With Judges in Two States Over Privacy Class Actions*, N.Y.L.J. (Sept. 10, 2020), https://www.law.com/newyorklawjournal/2020/09/10/ny-based-facial-recognition-tech-company-wrangles-with-judges-in-two-states-over-privacy-class-actions; Erin Shaak, *Clearview AI Hit with Class Action Lawsuit Over Controversial Data Collection Practices*, CLASS ACTION BLOG, https://www.classaction.org/blog/clearview-ai-hit-with-class-action-lawsuit-over-controversial-data-collection-practices.

[89] Eric Goldman, *Facial Recognition Database Vendor May Not Qualify for Section 230*-Vermont v. Clearview, TECH. & MARKETING L. BLOG (Sept. 18, 2020), https://blog.ericgoldman.org/archives/2020/09/facial-recognition-database-vendor-may-not-qualify-for-section-230-vermont-v-clearview.htm; Naomi Owen, *#Privacy: Clearview Refers to Section 230 in Vermont Lawsuit to Avoid Alleged Privacy Violations*, PRIVSEC REPORT (June 4, 2020).

[90] Sara Morrison, *The World's Scariest Facial Recognition Company is now Linked to Everybody from ICE to Macy's*, VOX (Feb. 26, 2020), https://www.vox.com/recode/2020/2/26/21154606/clearview-ai-data-breach; *Macy's Hit with BIPA Lawsuit for Using*

The scale of Clearview's collection coupled with its law enforcement partnerships and undetected operation serves as an example of why we cannot easily trust industry actors and governments with our sensitive data. In pandemic times, heightened intensity in the types of data collected, where from, how much, and who uses this data exacerbates these fears. In countries like China and Israel, pandemic technologies were married to the government from the outset and directly linked to existing surveillance technologies.[91] In the previously discussed Singapore example, the government stated that the dataset was for COVID-19 purposes only, but revealed law enforcement uses that reneged on original promises.[92] Some increased monitoring is necessary to track the spread of the coronavirus, but not all such monitoring. Added surveillance measures like facial recognition with thermal scans, telecom and cellular data used for location tracking, and QR code check-in apps tied to real identification are dangerous pretexts for "accelerating the mass collection of personal data to track citizens," and this mission creep[93] makes us wary.[94]

The task of determining what level of data collection is appropriate for such extraordinary times is extremely difficult. For a solution to work, it must be widely adopted and provide governments with enough information to stay ahead of the virus' spread. If people cannot trust that this information will not be over-collected or later abused, necessary levels of adoption will be difficult to reach.

Clearview Biometric Surveillance, FINDBIOMETRICS, https://findbiometrics.com/macys-hit-bipa-lawsuit-using-clearview-biometric-surveillance-080701.

[91] Anat Ben-David, *Israel is Following China on Surveillance. Here's Why that Should Worry You*, HAARETZ (Dec. 2, 2020), https://www.haaretz.com/israel-news/tech-news/.premium-israel-is-following-china-on-surveillance-that-should-worry-you-1.9343225; Tehilla Shwartz Altshuler & Rachel Aridor Hershkowitz, *How Israel's COVID-19 Mass Surveillance Operation Works*, BROOKINGS INST. (July 6, 2020), https://www.brookings.edu/techstream/how-israels-covid-19-mass-surveillance-operation-works; Lily Kuo, *"The New Normal": China's Excessive Coronavirus Public Monitoring Could be Here to Stay*, GUARDIAN (Mar. 9, 2020), http://www.theguardian.com/world/2020/mar/09/the-new-normal-chinas-excessive-coronavirus-public-monitoring-could-be-here-to-stay.

[92] Sato, *supra* note 24.

[93] Daniel Ryan Koslosky & Fletcher N. Baldwin, *Mission Creep in National Security Law*, 114 W. VA. L. REV. (2011); Wendy K. Mariner, *Mission Creep: Public Health Surveillance and Medical Privacy*, 87 B.U. L. REV. 347 (2007).

[94] Kuo, *supra* note 91.

IV. CLOSING THE TRUST GAP

Even though information technologies are not worthy of our trust now, lawmakers could change that fact before the next public health emergency. To close the trust gap between the organizations that build or leverage data-intensive technologies and the people that use them, especially in global health emergencies, lawmakers and organizations should move beyond individualistic "consent and control over" approaches to privacy to include relationships of trust, radically overhaul design frameworks for information technologies, and embrace substantive rules instead of procedures that ignore power dynamics and justify practices that might be fair to the individual, but result in net harm to society. Relational models of privacy are more sensitive to the power disparities between people and tech companies. Strengthened design frameworks help provide structure to relational norms of loyalty and care, and they give people evidence that a system or company is worth trusting. Substantive rules draw hard lines in the sand to keep people protected whenever improved norms or frameworks are still not enough.

A. *Relational Duties of Trust*

The trust gap exists in part due to the breakneck speed of development for privacy-violating technologies. Pandemic response requires thorough and deep collaboration between the public and private sectors, but when people cannot comfortably put aside their worries regarding the technologies intended to help them, trust in government and well-meaning private organizations wanes.

When adoption at-scale is not only desired but a matter of life and death for many, all actors implementing technological solutions or strategies should operate from a place of duty. A few options have been proposed, from building off relational obligations of trust, with specific obligations of loyalty, care, forthrightness, confidentiality, and more.[95]

---

[95] *See* SOLOVE, *supra* note 39; WALDMAN, PRIVACY AS TRUST, *supra* note 39; Balkin, *Information Fiduciaries*, *supra* note 39, at 186; https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346; Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057 (2019); Brennan-Marquez, *supra* note 39; Ariel Dobkin, *Information Fiduciaries in Practice: Data Privacy and User Expectations*, 33 BERKELEY TECH. L.J. 1, 1 (2018); Kerr, *supra* note 39; Paul Ohm, *Forthright Code*, 56 HOUS. L. REV. 471 (2018); Richards & Hartzog, *Taking Trust Seriously*, *supra* note 39; Richards & Hartzog, *Privacy's Trust Gap*, *supra* note 39, at 1188; Richards & Hartzog, *Trusting Big Data Research*, *supra* note 39; Christopher W. Savage, *Managing the Ambient Trust Commons: The Economics of Online Consumer Information Privacy*, 22 STAN. TECH. L. REV. 95 (2019); Scholz, *supra* note 39; Waldman, *Privacy As Trust*, *supra* note 39; Waldman, *Privacy, Sharing, and Trust*, *supra* note 39; Richard S. Whitt, *Old School Goes Online: Exploring Fiduciary Obligations*

The ideas outlined in these proposals argue that technology organizations should be seen as agents or stewards to those who trust them: their users. People are inherently vulnerable both to poor outcomes from decisions tech companies intentionally make, and to attacks on these companies' security by external threats. This leaves people vulnerable in their information relationships, and mandated trust keeps these relationships afloat.[96] For example, a properly implemented duty of loyalty would prohibit companies from taking any actions regarding their technologies' design or from processing of users' personal information that conflicted with their best interests, to the extent of their exposure.[97] This would prohibit dark patterns that turned people's limitations against themselves and algorithmic decision-making that was opaque, wrongfully biased, and harmful, or which deprived people of significant opportunities. Alleviating the burden of this vulnerability from the end-user requires considerable faith in the controlling organization—namely, that technology companies and government organizations responsibly handle and communicate the risks of data disclosure to people. Improving trust improves the technologically-mediated relationship between people and companies. During a pandemic, improving this relationship might additionally improve the adoption of tools used to control the coronavirus.

B. *Consent, Liability, and Design Frameworks*

When understandings of trust and loyalty mend information relationships, new standards in design and consent regimes that reflect changing norms should follow. Frameworks facilitate these relationships and help people feel safe with technologies that hold themselves to these structures. Even when an individual information relationship fails, industry standards can help keep people protected at a systemic level and let the consumer control what information relationships to cultivate.

---

of Loyalty and Care in the Digital Platforms Era, 36 SANTA CLARA COMP. & HIGH TECH L.J. 75 (2019); Jonathan Zittrain, *Engineering an Election*, 127 HARV. L. REV. F. 335, 340 (2014); Jack Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, ATLANTIC (Oct. 3, 2016), Cameron F. Kerry, *Why Protecting Privacy Is a Losing Game Today—and How to Change the Game*, BROOKINGS INST. (July 12, 2018), https://www.brookings.edu/research/why-protecting-privacy-is-a-losing-game-today-and-how-to-change-the-game. *But see* Khan & Pozen, *supra* note 39.

[96] Richards & Hartzog, *supra* note 39.

[97] *See, e.g.*, Richards & Hartzog, *A Duty of Loyalty*, *supra* note 39.

Digital consent regimes are ultimately broken and insufficient to address the ways individuals interact with online technologies. When people use a device or application, they subject themselves to the provisions outlined in the technology's Terms of Use, Terms and Conditions, and privacy policies. These technologies enjoy carte blanche when they shift the burden of liability onto the user, while individuals are left to deal with the fallout of privacy violations and other misuses of their data. Users need not read these terms to be bound by them,[98] as with the shrink-wrap licenses[99] in the late 1900s. Individuals should not, however, be expected to read these terms and policies—not when the burden and cost of doing so are incredibly high.[100] When consent is provided in this fashion, people are unwittingly trapped into contracts they do not truly understand. In pandemic times, consent can feel more coercive,[101] as with Project Baseline's Google Account requirement[102]—it can feel like the choices are between making an account and getting a test, on which one's life may depend. This can hardly be called an "agreement," nor can it stand up to new standards of consent, like those desired by regulations like the General Data Protection Regulation (GDPR).[103]

To fix broken consent regimes, we can consider ideal circumstances for providing consent and create frameworks that guide organizations as they handle consent statements and registration flows. Beyond the requirements outlined in privacy laws like the GDPR,[104] meaningful consent requests should be infrequent, with easily envisioned risks, and the reasons for consenting should be accompanied by incentives for data subjects to seriously examine the request.[105] Consider the trust relationship in vaccinations, which provides an example of what an ideal consent regime might include. People do not frequently receive vaccines: this satisfies the first precondition. The next two preconditions allow people to conduct an effective risk-benefit analysis. Before vaccination, people are provided with relevant

---

98 Mark A. Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. PA. L. REV. 1051, 1116 (2017).

99 NANCY S. KIM, WRAP CONTRACTS: FOUNDATIONS AND RAMIFICATIONS 36 (2013); Mark A. Lemley, *Terms of Use*, 91 MINN. L. REV. 459, 467 (2006);.

100 *See generally* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. POL. INFO. SOC. 543 (2019).

101 Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1461–1503.

102 *COVID-19 Testing Program*, *supra* note 7.

103 Council Regulation 2016/679, 2016 O.J. (L 119) 1, 6.

104 *See generally* Council Regulation 2016/679, 2016 O.J. (L 119).

105 Richards & Hartzog, *supra* note 101.

information as to potential side effects and the risks of forgoing vaccination. For COVID-19, the risk of going unvaccinated may include severe and life-threatening complications, while the benefits include virus prevention and improved safety for people in contact with a vaccinated person.[106] The risk is vivid and easily imagined; the benefits provide a real incentive for a person consenting to vaccination.

This framework for understanding consent is applicable to data collection. People are inundated with fallible consent requests everywhere, in pop-ups,[107] app permission requests, websites' cookie banners,[108] account registration, and myriad other 'agreements' that may not provide people with real avenues for providing consent. These requests are not infrequent—too many consent requests will begin to lose meaning and can be annoying and deceptive.[109] The risk of consenting to these notices is not vivid or clear—the risks are hidden in time-consuming legal documents. Fixing these consent regimes to be more empowering, meaningful, and transparent for users is necessary for restoring trust and for giving control over data back to the people who provide it. How this would occur is beyond the scope of this Essay, but we imagine stronger guidance around when to provide notice and how as well as formal design structures that delegate more control to the end-user.

Privacy-forward design frameworks must accompany improved consent solutions. Problems with consent are exacerbated when interface tricks are employed to obfuscate the contents of a technology's terms. Research into why designs like dark patterns are so problematic[110] and suggestions for improved privacy interfaces[111] help

---

106 CENTERS FOR DISEASE CONTROL AND PREVENTION, COVID-19 AND YOUR HEALTH, https://www.cdc.gov/coronavirus/2019-ncov/vaccines/vaccine-benefits.html (last updated Jan. 5, 2021, last visited Feb. 14, 2021)

107 Midas Nouwens et al., *Dark Patterns After the GDPR: Scraping Consent Pop-ups and Demonstrating Their Influence*, *in* PROCEEDINGS OF THE 2020 CHI CONFERENCE HUMAN FACTORS COMPUTING SYSTEMS 1, 1–13 (2020), http://doi.org/10.1145/3313831.3376321.

108 Célestin Matte et al., *Do Cookie Banners Respect my Choice?: Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework*, *in* 2020 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (SP) 791, 791–809 (2020).

109 *Most Cookie Banners are Annoying and Deceptive. This is not Consent.*, PRIVACY INT'L (2019), http://privacyinternational.org/explainer/2975/most-cookie-banners-are-annoying-and-deceptive-not-consent.

110 *See generally Dark Patterns at a Scale*, *supra* note 41; *What Makes a Dark Pattern...Dark?*, *supra* note 41.

111 *See generally* LORRIE FAITH CRANOR ET AL., CYLAB SEC. AND PRIV. INST., DESIGN AND EVALUATION OF A USABLE ICON AND TAGLINE TO SIGNAL AN OPT-OUT OF THE SALE OF PERSONAL INFORMATION AS REQUIRED BY CCPA, (2020); Patrick Gage Kelley et al., *A "Nutrition Label" for Privacy*, *in* PROCEEDINGS OF THE 5TH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 1, 1–12 (2009), http://doi.org/10.1145/1572532.1572538.

articulate why design-level regulation is so imperative. While the DETOUR Act would require that online operators frequently present disclosures on data use and that these disclosures not be "deceptively obscured,"[112] robust design standards that clarify when an interface element becomes "dark" could provide better guidance for user experience designers. While there are various aspects of the DETOUR Act that might create implementation problems, the bill outlines the need for a professional standards body that would help define acceptable conduct and build design frameworks driven by ethics and value sensitivity.[113]

In addition to bolstering privacy design frameworks, we should work to improve Fair Information Practice Principles (FIPPs)-based protections (normative guidance for information practices),[114] which often fail in practice.[115] Efforts to improve privacy by design that rely on expounding the importance of FIPPs should also seek to amend the FIPPs themselves, expanding them from vague principles to actionable guidance for practitioners. GDPR's guidance on "data protection by design and default"[116] is an excellent start, but effective approaches like the GDPR's should strive to provide stricter, more specific parameters regarding what design choices to make.

C. *Substantive Rules Limiting Data Collection and Use*

Changes in information relationship norms and interface design can be incredibly powerful for protecting a user's individual welfare, but substantive legal rules can help prevent privacy problems when the previous two recommendations fail to be enough. Consent regimes are practically unscalable, overly individualistic, and function to justify all manner of harmful actions so long as companies that control people's medium of expression can extract a perfunctory acquiescence.[117] What is needed are un-waivable rules, beyond flexible purposes stated by companies and governments themselves, that limit when companies

---

[112] Deceptive Experiences to Online Users Reduction Act, S. 1084, 116th Cong. (2019), https://www.congress.gov/bill/116th-congress/senate-bill/1084/text.

[113] *Id.*

[114] MARTHA K. LANDESBERG ET AL., U.S. FED. TRADE COMM'N, PRIVACY ONLINE: A REPORT TO CONGRESS, at 71 (2009), https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf.

[115] Fred H. Cate, *The Failure of Fair Information Practice Principles*, *in* CONSUMER PROTECTION IN THE AGE OF THE INFORMATION ECONOMY 343, 343 (Jane K. Winn ed., 2006), https://www.ftc.gov/system/files/documents/public_comments/2018/12/ftc-2018-0098-d-0036-163372.pdf.

[116] Council Regulation 2016/679, 2016 O.J. (L 119) 1, 45.

[117] Richards & Hartzog, *supra* note 101; Evan Selinger & Woodrow Hartzog, *The Inconsentability of Facial Surveillance*, 66 LOY. L. REV. 33 (2020);.

and governments can collect information, what kinds of information they can collect, how they can use it, and with whom they can share it.

Concerns over law enforcement's use of COVID-19 tracing data are well-founded, as indicated by Singapore's case. One way to prevent further violations of privacy at the hands of the government is to disallow law enforcement use of tracking data from the outset, whether that be pandemic-specific datasets or privately collected datasets like Clearview's facial database. Australia's pandemic response provides an example of trust-building through substantive rules, particularly regarding their COVIDSafe contact tracing app,[118] released in April 2020. At launch, the app was accompanied by an emergency Determination under Australia's Biosecurity Act of 2015 that would allow the collection, use, and disclosure of COVIDSafe data for prosecuting citizens for offenses under the Act.[119] Researchers quickly responded with concerns over potential law enforcement use of the COVIDSafe data, describing the COVIDSafe provisions as "an experiment in surveillance and trust," and pointed out flaws in the Determination as well as other issues with data use and minimization.[120] This Determination was quickly repealed on May 15, 2020, with the Privacy Amendment (Public Health Contact Information) Act 2020.[121] The Privacy Amendment Act not only disallowed law enforcement use of COVIDSafe data but also created new offenses for using this dataset for purposes other than contact tracing. The government addressed other concerns regarding the technical security of the application or in-the-background data collection by making the source code for both Android and iOS versions of COVIDSafe publicly available on Github.[122] Updates to the source code are pushed to Github and are available for review by the technical community.

Australia's rapid and preemptive measures to alleviate fears of data abuse reflect desired traits for a pandemic response: as transparent as possible, swiftly deployed, and carefully articulated. These traits are also necessary for any technical solutions for the pandemic, especially

---

118 *COVIDSafe App*, AUSTRALIAN GOV. DEP'T OF HEALTH (2020), https://www.health.gov.au/resources/apps-and-tools/covidsafe-app.

119 Biosecurity (Human Biosecurity Emergency) (Human Coronavirus with Pandemic Potential) (Emergency Requirements—Public Health Contact Information) Determination 2020, pt. 2 paras 6–9 (Austl.) (no longer in force).

120 Graham Greenleaf & Katharine Kemp, Australia's 'COVIDSafe App': An Experiment in Surveillance, Trust and Law 2 (April 30, 2020) (unpublished manuscript) (available as part of the University of New South Wales Law Research Series, 2021), http://classic.austlii.edu.au/au/journals/UNSWLRS/2021/7.html.

121 Privacy Amendment (Public Health Contact Information) Act, sch. 1 div. 2 s 94D (Austl.).

122 *COVIDSafe*, GITHUB, https://github.com/AU-COVIDSafe.

where risk of surveillance is high. Conversely, Singapore's delayed responses to privacy concerns and later exposure of law enforcement uses of TraceTogether data provide an example of retroactive measures. To keep citizens' data protected and retain their trust, substantive rules and prohibitions must be outlined well in advance. To maintain trust and inspire it, these substantive rules should be accompanied by auditing and enforcement; such rules will only be useful if they are followed.

Beyond the pandemic, industry and governments will continue to find future uses for large-scale data collection and analysis. To prepare for these developments, governments should preemptively outline explicit limits for the protection of individuals' data. One path forward that may help build substantive lines in the sand for data collection is to use frameworks for understanding data disclosure by weighing the data's utility against an individual's disclosure risk.[123]

V. CONCLUSION

Before the pandemic, we were living with technologies that disrespected or mishandled our privacy, our choices, and our online safety. These problems led to a trust gap between individuals, technology companies, and governments—a trust gap that has only widened as a reaction to concerning COVID-19 practices like contact tracing and mission creep.

While the world races toward a solution to the pandemic, privacy and digital health must not become afterthoughts or sacrificial lambs. The trust gap must be closed, not only to improve adoption of pandemic-response technologies but also to protect people well after the threat of the virus subsides. Adopting relational duties of loyalty and care can help allay some of these concerns, especially when combined with structured design frameworks that improve or outright eliminate consent regimes and reduce interface trickery. These adjustments are potential starts toward mending the broken trust between people and data organizations—but they are not enough. Substantive rules prohibiting misuse of data, particularly COVID-19 data, are necessary to protect individuals' privacy rights and prevent future invasions of privacy from occurring.

---

[123] GEORGE T. DUNCAN ET AL., *Disclosure Risk vs. Data Utility: The R-U Confidentiality Map*, NAT'L INST. STAT. SCIS., at 31 (2001).

The urgency of the pandemic must not be used as an excuse to deprioritize user privacy or undermine trust—it must be seen as an opportunity to rebuild confidence and create better digital experiences that outlast the global health crisis.


SETON HALL UNIVERSITY
1856
HAZARD YET FORWARD