Matt Maloney  
IST 618  
Reflection on privacy and security

*Introduction*

Since the rapid and persistent spread of coronavirus began earlier this year, governments across the world have been seeking, with the assistance of corporate partners, methods of containing the infectious disease. Among the many initiatives are numerous attempts to utilize cell phone data to aid in tracking and contact tracing, with the Centers for Disease Control (CDC) and various state and local governments in the United States utilizing GPS and other data points. Similarly, Google has been collecting information and displaying it on the web interface, Verily Life Sciences, a sister company within the Alphabet company. While the upside of these types of geolocation and biometric tracking programs include a reduction in the number of worldwide cases, they bring with them a massive opportunity for future corporations to exploit these data points for profit even after the virus has subsided. Proposals to rein in these types of data collection and usage range from regulating big technology firms as a type of public utility, to establishing the types of oversight boards that currently observe police use of surveillance in their communities. Regardless of the regulatory approach, these conversations will likely continue as the public health crisis rages on.

*CDC and government data collection*

Under US privacy laws, data about mobile phone users can be collected on a granular level, including GPS data that can track a user’s movement within their own house, let alone throughout their community. Since the outset of the pandemic, the CDC has acquired large swaths of user data, which they have then anonymized, but not aggregated, so that they can track a single user’s movements during a specific block of time (Hern, 2020). In North and South Dakota, state governments have issued a mobile application for their residents that track the users’ location. The application relies on cell towers, GPS, and Wi-Fi information. Again, this information is purportedly pseudonymized once obtained and securely stored (Ram & Gray, 2020). However, “knowing where someone was is enough to reidentify them 95% of the time,” according to one privacy expert, Yves-Alexandre de Montjoye (Hern, 2020).

*Google*

In the private sector, Google has aggressively deployed its vast cache of consumer data during the coronavirus. Much of this information has been funneled into website created by Verily Life Sciences, a subsidiary of Alphabet (Google’s parent company). The firm is also providing COVID-19 screening throughout some of the western US. However, individuals utilizing Verily’s services are required to log in with their Google credentials in order to receive screening services, and there is no indication that Verily is subject to the same HIPAA laws that govern insurance companies, hospitals, and physicians (Cohen, 2020). There are credible fears that information uncovered in the course of the screening will be linked back to the user’s Google account and incorporated into the pre-existing customer profile.

*Advantages, concerns, ethical dilemmas*

The advantages of granting the state unfettered and universal access to private data are immensely alluring. Through a combination of biometric and location data, the possibility of a pandemic looming this large would be slim to none. In fact, it is easy to imagine this type of a data collection providing long term solutions to other diseases and chronic illnesses: intervening when someone who is alcohol dependent parks in front of a bar or liquor store, issuing a sunblock reminder when a user seeks directions to the beach, or, if biometric inputs are included, detecting early symptoms of other maladies.

Although there are certain ethical arguments around the collection of mobile phone data that can be made in abstract, there are also very concrete protections afforded to Americans in the US Constitution. The Fourth Amendment guarantees that “the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures shall not be violated” (U.S. Const. art. IV). While the framers could never have imagined the technological advances that enable the types privacy infringement that are now possible, it is a reasonable expectation that this right to privacy also applies to protect one’s digital footprint from government surveillance (Ram & Gray, 2020).

On the subject of private enterprises’ collection of citizens’ data, the discussion may necessarily devolve into the moralistic realm of ethical considerations. When thinking about responses to the coronavirus outbreak, it is important to recognize that the permissioning out of our private data is unlikely to be undone at the conclusion of the crisis. As Yuval Harari, historian and ethicist at Hebrew University, notes:

Many short-term emergency measures will become a fixture of life. That is the nature of emergencies. They fast-forward historical processes. Decisions that in normal times could take years of deliberation are passed in a matter of hours (Harari, 2020).

While some members of Congress have publicly stressed the importance of a return to the current state of privacy once the virus has subsided, their colleagues and corporate partners may have other motivations (Brough & Martin, 2020). The expansion of the surveillance state in the wake of the September 11, 2001 terrorist attacks, and its persistence in the nineteen years since, demonstrate this phenomenon. When the permanent implications of changes to privacy policy are considered, the decision to enable government bodies with cellular data becomes more challenging. While we know that companies like Google are already tracking and storing this type of information, and that it can be obtained by government actors through the proper legal measures, the prospect of localization data being commodified and permanently incorporated into a marketing campaign might be off-putting to many. Equally alarming is the prospect of these surveillance measures being incorporated into the ever-expanding arsenal of law enforcement tools. In New York City, its police department has already issued fines of $500 for breaking social distancing measures (Durkin, 2020). Armed with geolocation capabilities, punitive actions could be doled out automatically.

*Policy recommendations*

To bulwark against privacy intrusions that last beyond this crisis, it is important for concerned citizens and lawmakers to band together. Matthew Guarigilia and Adam Schwartz from the Electronic Frontiers Foundation have set forth a framework for public health data collection, that includes key concepts like expiration (insisting that data collected during the crisis not outlast it), transparency (that collection processes and applications of data be thoroughly explained to the public), and that there be due process (that any limitations on an individual’s rights or mobility be subject to legal challenges if they are unreasonable) (Guariglia & Schwartz, 2020). Another solution might be to institute data surveillance oversight boards, modeled after existing police surveillance oversight board. These community organizations have been created in various US cities to observe and hold accountable police departments as they increase their use of surveillance tools. Perhaps this framework can provide inspiration for a government or civilian oversight board that can ensure fair use of private health data. Others have called on governments to regulate big technology companies as a public utility, held to the same types of scrutiny as those companies that provide water and electricity to residents (Scott, 2020). Their monopolistic tendencies, along with their indispensable utility, align for a compelling parallel with the aforementioned essential services. Given how reliant individuals, and governments in the wake of this crisis, are on these services, stronger regulation and a closer relationship to government oversight is in order.

*Conclusion*

Although the information held on the servers of technology giants like Google, Facebook, and Amazon hold vast potential for good (especially in the wake of the coronavirus pandemic), there are significant privacy concerns surrounding this data’s use. From governments, citizens might fear a heightening of punitive measures. From corporations, consumers have reason to be wary of a marketing calculus that incorporates location data along with biometric data. Government oversight boards and stricter regulation, similar to public utility rules, provide some solutions for addressing these concerns. Given the scope of the global crisis that confronts humanity, protecting privacy is not without its costs. In a world where individuals’ privacy rights are abjectly disregarded, there is reason to believe that the virus’s spread, and the resulting human suffering, could be significantly limited. Yet a global shock like the pandemic provides the cover for permanent structural changes in our relationship to governments and corporations. It is of utmost importance that decisions about privacy during the crisis take into account the likely outcome that at least some of these practices outlast the virus.

References

Bernard, R., Bowsher, G., & Sullivan, R. (2020). COVID-19 and the rise of participatory SIGINT: An examination of the rise in government surveillance through mobile applications. American Journal of Public Health (1971), , e1-e6. doi:10.2105/AJPH.2020.305912

Brough, A. R., & Martin, K. D. (2020). Consumer privacy during (and after) the COVID-19 pandemic. Journal of Public Policy & Marketing, , 0743915620929999. doi:10.1177/0743915620929999

Cohen, J. K. (2020-03-21T01:00:00-0400). Alphabet's COVID-19 project underscores privacy concerns with big tech. Retrieved from https://www.modernhealthcare.com/operations/alphabets-covid-19-project-underscores-privacy-concerns-big-tech

Durkin, E. (03/29/20). New yorkers who break social distancing rules will now face fines up to $500. Retrieved from https://www.politico.com/states/new-york/albany/story/2020/03/29/new-yorkers-who-break-social-distancing-rules-will-now-face-fines-up-to-500-1269545

Goldenfein, J., Green, B. & Viljoen, S. (04/17/20). Privacy versus health is a false trade-off. Retrieved from https://jacobinmag.com/2020/04/privacy-health-surveillance-coronavirus-pandemic-technology

Guariglia, M., & Schwartz, A. (03/10/20). Protecting civil liberties during a public health crisis. Retrieved from https://www.eff.org/deeplinks/2020/03/protecting-civil-liberties-during-public-health-crisis

Harari, Y. N. (2020). Yuval noah harari: The world after coronavirus | free to read. Retrieved from https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedcca75

Hern, A. (04/02/20). Experts warn of privacy risk as US uses GPS to fight coronavirus spread. Retrieved from https://www.theguardian.com/technology/2020/apr/02/experts-warn-of-privacy-risk-as-us-uses-gps-to-fight-coronavirus-spread

Ram, N., & Gray, D. (2020). Mass surveillance in the age of COVID-19. Journal of Law and the Biosciences, 7(1) doi:10.1093/jlb/lsaa023

Scott, M. (2020). Coronavirus crisis shows big tech for what it is — a 21st century public utility. Retrieved from https://www.politico.eu/article/coronavirus-big-tech-utility-google-facebook/

U.S. Const. art. IV