Smoke Signals

Signal messenger as a technical and ideological response to surveillance in 2020

Gerry LaBarbera
MA | New Media and Digital Culture
Student # 12986119
Word count: 1094
28/09/2020

Americans have a lot to say in 2020, and protests are the chosen platform of the year. With race-fueled police brutality reaching peak heights, people are occupying space physically and vocally to say their piece in the Black Lives Matter movement. However, this isn't the first time the American public is being heard, or more accurately, being listened to.

In the past half-century, the U.S. government has proven to be keen on surveillance technology, to an extent that the general public doesn't seem to mind, or simply isn't aware of. The most common surveillance tactics have tenure, including license plate tracking, mobile data interception, and facial recognition. The more provocative types of data supplied to law enforcement are coming from technology companies such as Apple, Google, and Amazon, with practices including access to cloud data of a suspect, geofence warrants for data histories harvested from crime scenes, and next-generation facial recognition that identifies, and misidentifies, suspects in a way that proves inherently discriminant. While the companies have been criticized for these practices, it's proven difficult for the public to truly hold them accountable after years of generative entrenchment (Bratton 2015, 47). In addition to the usual surveillance technology available to police, there were multiple instances of reconnaissance aircrafts detected over protesting cities in late May and in June.

Because of escalating police controversies before and during the protests, the public attention was focused on the physical safety and legal legitimacy of participants in the crosshairs of the law. With protestors feeling unsafe to communicate and organize on traditional media in an age where privacy is security, the emergent solution became an encrypted safe-space.

Signal is an end-to-end encrypted messaging application that circumvents traditional server-usage and data storage, giving users complete control of their communicated information and making it unavailable to any third parties, including the application itself. Signal Messenger as a company advocates a pro-privacy narrative that is very much in favor of the rights of the individual, and clearly chooses a side in the debate. Edward Snowden, whistleblower of the NSA in 2013, is not only a Signal user, but is featured prominently on the site as an endorser among other well known names, further embedding the intention of the company in prospective users (Light et al. 2018, 883).

In the late Spring of 2020, the benefits of using Signal were lauded in social media posts and articles on protest-preparedness. The hype caught on, and Signal saw downloads spike (figure3), with epicenters dated around contentious political developments. The most popular messaging platforms used in the U.S. are owned by Facebook, who harvests so much data from individuals while algorithmically feeding their user driven identities, it's hypothesized that people not on the site may already be ghosts in the machine (Bucher 2012, 482). Needless to say, people were open to the alternative option. It isn't enough to base judgment on industry narratives singing the praises of Signal, the truth lies within the key affordances of the application itself, what they allow the user to do, and especially the surveillance they prevent.

When investigating Signal's employment of interrelated mechanisms and conditions of affordance (Davis and Chouinard 2016, 242), it is evident that while encryption is the main defense, there are instances where the application has reinforced itself to withstand observation from various angles. Considering the promise of utmost protection, setting up a Signal account is not too arduous a task. Upon downloading the application, Signal demands a phone number for confirmation purposes (a code will be sent to the number for verification). The aforementioned protest-savviness article recommends using a trashable google number if anonymity is key. The user must choose a pin number which will be used to protect their encrypted profile on Signal, as well as to view and edit important settings. The pin must be at least 4 characters long, an alphanumeric option is possible, with no maximum limit. Encouraging users to provide longer pins prevents the surmising of passwords from other data collected on a given person, with this feature contributing to the vault-like presentation of the application. Signal requests pin input in periodically timed increments, allowing the user to remember longer and more complicated codes. Perhaps the Signal recognizes the pitfalls of our capabilities being conditioned by technology (McLuhan 1964, 17).

The privacy menu within the application grants a user many security allowances. A few of the more innovative options include a screen protection setting that hides the screen preview when switching between applications, which could prove paramount in refusing a glimpse from an unauthorized user, the opportunity to relay *all* calls through a Signal server to encourage further encrypted communications, and various gatekeeping methods when unsaved contacts initiate conversations. The inbox and conversational settings are where the remaining anti-surveillance options are located, as users can verify encryption keys with one another for authentic identification purposes, set a time limit on how long messages will remain visible before permanent deletion, as well as delete conversations and block another user. These options also work in favor of the user in the event of phone confiscation. The seemingly simple settings are another way in which Signal shares its ideologies through design and governance (Poell et al. 2019, 8).

One of the most distinguished features of Signal is the newly developed face-blurring technology for sharing photos. There were many critiques about sharing visuals during the protests, as facial recognition was picking up on participants and having imminent consequences. Signal allows users to take a picture, choose to auto-blur, and then use their fingertips to blur any remaining faces before sending or exporting the photo to a device. By ensuring that the entirety of this endeavor occurs within the encrypted application, Signal provides the user and those within photos a level of security that wasn't previously an option during such a process, which would have required multiple interfaces and potentially their servers. The creation of such a censored picture encourages for users to share across platforms without endangering protesters. The ease in which Signal facilitates this process is a testament to its vision and intention (Light et al. 2018, 889). Based on this feature, the application proves itself a modern artifact of reactive data activism, a counter move in a high-stakes surveillance culture (Milan 2017, 5). The company furthers their stance of solidarity in activism by producing physical facemasks for protest participants in a campaign encouraging users to 'encrypt your face.' With this added aspect, perhaps there is foreshadowing to Signal becoming a force for cultural change and normalization of activism through the introduction of end-to-end encrypted communications, and technology-based power to the people (Postman 2000, 10).

It has been suggested that citizens of society are objects of information but never subjects in communication (Foucault 2008, 5). Signal answers that call.

Works cited

Bratton, Benjamin H. *The Stack, On Software Sovereignty*. The MIT Press, 2015. https://mitpress.mit.edu/books/stack.

Brody, Liz. "Google's Geofence Warrants Face a Major Legal Challenge." Medium, June 11, 2020.https://onezero.medium.com/googles-geofence-warrants-face-a-major-legal-challenge-ac6da1408fba.

Bucher, Taina. "The Friendship Assemblage: Investigating Programmed Sociality on Facebook." *Television & New Media*, August 24, 2012. https://doi.org/10.1177/1527476412452800.

Davis, Jenny L., and James B. Chouinard. "Theorizing Affordances: From Request to Refuse." *Bulletin of Science, Technology & Society* 36, no. 4 (December 1, 2016): 241–48. https://doi.org/10.1177/0270467617714944.

Signal Messenger. "Encrypt Your Face," June 8, 2020. https://signal.org/blog/encrypt-your-face/.

Foucault, Michel. "'Panopticism' from Discipline & Punish: The Birth of the Prison." *Race/Ethnicity: Multidisciplinary Global Contexts* 2, no. 1 (2008): 1–12.

"How to Protest Safely: What to Bring, What to Do, and What to Avoid." *Wired*. Accessed September 27, 2020. https://www.wired.com/story/how-to-protest-safely-gear-tips/.

Light, Ben, Jean Burgess, and Stefanie Duguay. "The Walkthrough Method: An Approach to the Study of Apps." *New Media & Society* 20, no. 3 (March 1, 2018): 881–900. https://doi.org/10.1177/1461444816675438.

Signal Messenger. "Looking Back at How Signal Works, as the World Moves Forward," June 5, 2020. https://signal.org/blog/looking-back-as-the-world-moves-forward/.

McLuhan, Marshall. *Understanding Media: The Extensions of Man*. The MIT Press, 1964.

Milan, Stefania. "Data Activism as the New Frontier of Media Activism." SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, January 31, 2016. https://papers.ssrn.com/abstract=2882030.

Ng, Alfred. "How Police Are Using Protesters' Phones against Them." CNET. Accessed September 20, 2020. https://www.cnet.com/news/geofence-warrants-how-police-can-use-protesters-phones-against-them/.

O'Flaherty, Kate. "Apple Halted ICloud Encryption Plans After FBI Warning—Report." Forbes. Accessed September 20, 2020. https://www.forbes.com/sites/kateoflahertyuk/2020/01/21/apple-halted-icloud-encryption-plans-after-fbi-warningreport/.

Poell, Thomas, David Nieborg, and José van Dijck. “Platformisation.” *Internet Policy Review* 8, no. 4 (November 29, 2019). https://policyreview.info/concepts/platformisation.

Postman, Neil. “The Humanism of Media Ecology.” *Media Ecology Association* 1 (2000): 7.

Rivero, Nicolás. “Signal App Downloads Spike as US Protesters Seek Message Encryption.” Quartz. Accessed September 22, 2020. https://qz.com/1864846/signal-app-downloads-spike-as-us-protesters-seek-message-encryption/.

Signal Support. “Signal PIN.” Accessed September 24, 2020. http://support.signal.org/hc/en-us/articles/360007059792.

Kanno-Youngs, Zolan. “U.S. Watched George Floyd Protests in 15 Cities Using Aerial Surveillance - The New York Times.” Accessed September 24, 2020. https://www.nytimes.com/2020/06/19/us/politics/george-floyd-protests-surveillance.html?fbclid=IwAR1v0bUEDSncLfosF51zhbptuxb_OVwBNQ-2taCXuEOHWat8PtgObY6D6wQ.

Vincent, James. “Gender and Racial Bias Found in Amazon’s Facial Recognition Technology (Again).” The Verge, January 25, 2019. https://www.theverge.com/2019/1/25/18197137/amazon-rekognition-facial-recognition-bias-race-gender.

Images

Signal. Accessed September 25, 2020. https://signal.org/#signal

Quartz. Accessed September 25, 2020. https://qz.com/1864846/signal-app-downloads-spike-as-us-protesters-seek-message-encryption

Signal Blog Signal Pins. Accessed September 25, 2020. https://signal.org/blog/signal-pins/

Signal Blog Blur Tool. Accessed September 25, 2020. https://signal.org/blog/blur-tools/