IN THE AGE OF COVID-19, THE CREDIT CARD KNOWS ALL

ALBERT FOX CAHN, ESQ. &
MELISSA GIDDINGS

JULY 15, 2020

STOP
SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

SURVEILLANCE TECHNOLOGY OVERSIGHT PROJECT

@ The Urban Justice Center:
40 Rector Street, 9th Floor
New York, New York 10006

www.StopSpying.org | (646) 602-5600

In the Age of COVID-19, the Credit Card Knows All

By Albert Fox Cahn, Esq. and Melissa Giddings

As the U.S. struggles to contain COVID-19, government agencies and Silicon Valley increasingly turn to mass surveillance as the solution. While high-tech offerings from Google and Apple are currently dominating the news, it's lower-tech systems, such as cell phone records and payment history, that are likely to play a much larger role in public health monitoring.

Many of the technical innovations that have commentators excited by the tech behemoths' new Bluetooth approach to COVID-19 tracking will likely prevent it from taking off until long after this crisis has passed. Instead, we're more likely to see increasingly widespread use existing tracking systems, raising privacy questions that have only begun to be answered.

While it's unclear if data dragnets help fight this disease, it is clear that they create long-term risks for public privacy, and we must ensure that our emergency responses do not give rise to a permanent surveillance regime. The bare minimum is to create legal protections, limiting how our data can be harvested, who can use it, and how long it's retained.

In the United States, one of the most powerful tracking tools available isn't GPS or some new form of artificial intelligence: it's our wallet. Payment records paint a vivid picture of our daily lives, from where we eat to what we buy to who we see. Financial data is generated with each purchase, and every transaction involves multiple parties such as retailers, credit card companies, mobile apps, mobile phone carriers, banks, and the consumers themselves. Data about a single transaction can be linked to purchase history, creating a detailed picture of the person behind the payment.

Digital wallets and contactless payment systems like smart chips have been around for years. The introduction of Apple Pay, Amazon Pay, and Google Pay have all contributed to the e-commerce movement, as have fast payment tools like Venmo and online budgeting applications. In response to COVID-19, the public is increasingly looking for ways to reduce or eliminate physical contact. With so many options already available, contactless payments will inevitably gain momentum. Contactless payments and smart card use for financial transactions has implications for other personal data as

well, as government-issued IDs[1] and transportation systems[2] increasingly employ the same technology.

Payment history reveals sensitive information about a person's family, job, political views, health, sexuality, and religion. Weak[3] and nonexistent[4] privacy laws[5] in the United States give companies significant leeway when it comes to how they use and store data, and how much data is collected. When companies share this data with third parties for advertising or to study trends, it is nearly impossible to ensure anonymity.[6]

Location data revealed by payment histories is uniquely difficult to anonymize as records often still include important details. In 2015, researchers reviewing three months of credit card records demonstrated that four data points associated with a financial transaction were enough to correctly identify 90% of the 1.1 million individuals included in their study; including the price of a transaction increased the risk of identification by 22% on average.[7] Last year, researchers accurately identified 99.98% of persons included in an anonymized data set using 15 data points like age, gender, and marital status.[8] This suggests that large data sets of personal information are not protected by touted methods of anonymization, and that without requiring improved security measures, our data is not safe.

An unexpected global event can catalyze a change in consumer behavior,[9] and in reaction to COVID-19 the United States will experience a rise in the use of chip cards and digital wallets.[10]

---

[1] *See, e.g.*, Jason Hutchinson, Joel Bellman, and Steve Hurst, *The Digital Citizen*, DELOITTE (June 24, 2019), https://www2.deloitte.com/us/en/insights/industry/public-sector/government-trends/2020/government-digital-identity.html; Jennifer Hefty, *Colorado Governor Oks Use of Electronic Driver's Licenses*, COLORADOAN (Oct. 31, 2019), https://www.coloradoan.com/story/news/2019/10/31/colorado-governor-jared-polis-approves-digital-drivers-license-id/4109010002/; Edward C. Baig, *Upgrading Your Wallet: How Soon Can I Get a Digital Driver's License*, USA TODAY (Mar. 6, 2019), https://www.usatoday.com/story/tech/2019/03/06/how-soon-can-get-digital-drivers-license/3072888002/. *See also* https://www.lawallet.com/; https://www1.nyc.gov/site/idnyc/index.page.

[2] *See, e.g.*, https://new.mta.info/easypay; https://www.ventrachicago.com/; https://www.mbta.com/projects/fare-transformation; http://paymentpilot.wmata.com/.

[3] *See, e.g.*, 12 CFR § 1016.10, https://www.law.cornell.edu/cfr/text/12/1016.10.

[4] *See generally* Steven Chabinsky and F. Paul Pittman, *USA: Data Protection 2019*, WHITE AND CASE (Mar. 7, 2019), https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa.

[5] *See The Appropriate Use of Customer Data in Financial Services*, WORLD ECON. FORUM (Sep. 2018), www3.weforum.org/docs/WP_Roadmap_Appropriate_Use_Customer_Data.pdf.

[6] *See* Boer Deng, *People Identified Through Credit-Card Use Alone*, NATURE (Jan. 29, 2015), https://www.nature.com/news/people-identified-through-credit-card-use-alone-1.16817.

[7] Yves-Alexandre de Montjoye, Laura Radaelli, Vivek Kumar Singh, and Alex Pentland, *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, SCIENCE (Jan. 30, 2015), https://science.sciencemag.org/content/347/6221/536.full?ijkey=4rZ2eFPUrlLGw&keytype=ref&siteid=sci.

[8] Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TECHCRUNCH (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data/.

[9] *See* Kate Rooney, *Electronic Payments Look More Appealing as People Fear Cash Could Spread Coronavirus*, CNBC (Mar. 16, 2020), https://www.cnbc.com/2020/03/16/electronic-payments-look-more-appealing-as-coronavirus-spreads.html.

[10] *See* Jessica Dickler, *Germ-ridden Cash May Boost Use of Contactless Payments*, CNBC (Mar. 18, 2020), https://www.cnbc.com/2020/03/18/germ-ridden-cash-may-boost-use-of-contactless-payments.html; Kate Rooney, *Electronic Payments Look More Appealing as People Fear Cash Could Spread Coronavirus*, CNBC (Mar. 16, 2020), https://www.cnbc.com/2020/03/16/electronic-payments-look-more-appealing-as-coronavirus-spreads.html; Jim Wang, *How to Simplify Money During the Coronavirus Crisis*, FORBES (Mar. 14, 2020),

Across the country, stores are requesting customers to use contactless card payments only or avoid cash where possible.[11] As the pandemic boosts the use of electronic payments and reduces our use of paper currency, it will further enhance the ability of payment networks to track our every move at a time when governments are consistently using digital footprints to trace the spread of the virus.[12]

Location data around mass movements[13] or use of public spaces[14] is limited. The United States could easily turn to using data generated by financial transactions to determine whether people are complying with social distancing advisements or businesses are staying shut down as this data is often more specific or revealing.

Without strong federal laws regulating the use of our data, we're left to rely on private companies that have consistently failed to protect our information. To prevent long-term surveillance, we need to limit the data collected and shared with the government to only what is needed. Any sort of monitoring must be secure, transparent, proportionate, temporary, and must allow for a consumer to find out about or be alerted to implications for their data. If we address these challenges now, at a time when we will be generating more and more electronic payment records, we can ensure our privacy is safeguarded.

Cahn (@FoxCahn) is the founder and executive director of The Surveillance Technology Oversight Project (S.T.O.P.) at the Urban Justice Center, a New York-based civil rights and privacy group and a fellow at the Engelberg Center for Innovation Law & Policy at N.Y.U. School of Law.

Giddings is a civil rights intern at The Surveillance Technology Oversight Project (S.T.O.P.) at the Urban Justice Center and a third-year student at N.Y.U. School of Law.

---

https://www.forbes.com/sites/jimwang/2020/03/14/how-to-simplify-your-money-during-the-coronavirus-crisis/#2e5858ca578a; Samantha Murphy Kelly, *Dirty Money: The Case Against Using Cash During the Coronavirus Outbreak*, CNN (Mar. 7, 2020), https://www.cnn.com/2020/03/07/tech/mobile-payments-coronavirus/index.html; Mary Meisenzahl, *How to Use Apple Pay and Other Contactless Payments to Avoid Touching Cash, Cards, and Payment Machines in the Age of Coronavirus*, BUS. INSIDER (Mar. 6, 2020), https://www.businessinsider.com/use-apple-pay-google-pay-avoid-coronavirus-2020-3; *Covid-19: Don't Reach Out and Touch That*, WALL STREET J. (Mar. 4, 2020), https://www.wsj.com/articles/covid-19-dont-reach-out-and-touch-that-11583366713.

[11] *See, e.g.*, Dawson White, *Going to Grocery Store During Coronavirus Outbreak? Here are Tips for Shopping Safely*, MIAMI HERALD (Mar. 23, 2020), https://www.miamiherald.com/news/coronavirus/article241423761.html; Jefferson Graham, *Will Coronavirus Make Mobile Payment Systems like Apple Pay, Google Pay Mainstream?*, USA TODAY (Mar. 16, 2020), https://www.usatoday.com/story/tech/2020/03/16/apple-google-samsung-may-see-mobile-pay-boost-coronavirus/5058876002/.

[12] *See, e.g.*, Casey Newton, *Tech Companies Could Face More Pressure to Share Location Data with Governments to Fight Coronavirus*, VERGE (Mar. 20, 2020), https://www.miamiherald.com/news/coronavirus/article241423761.html; Ephrat Livni, *Israel is Now Using Counterterrorism Tactics to Track Possible Coronavirus Patients*, QUARTZ (Mar. 17, 2020), https://qz.com/1819898/israel-to-use-invasive-surveillance-to-track-coronavirus-patients/; Brian Kim, *Lessons for America: How South Korean Authorities Used Law to Fight the Coronavirus*, LAWFARE (Mar. 16, 2020), https://www.lawfareblog.com/lessons-america-how-south-korean-authorities-used-law-fight-coronavirus; Vincent Manancourt, *Coronavirus Tests Europe's Resolve on Privacy*, POLITICO (Mar. 10, 2020), https://www.politico.eu/article/coronavirus-tests-europe-resolve-on-privacy-tracking-apps-germany-italy/.

[13] *See, e.g.*, Issie Lapowsky, *Facebook Data Can Help Measure Social Distancing in California*, Protocol (Mar. 17, 2020), https://www.protocol.com/facebook-data-help-california-coronavirus.

[14] *See, e.g.*, COVID-19 Community Mobility Reports, Google (accessed Apr. 10, 2020), https://www.google.com/covid19/mobility/.

Surveillance Technology
Oversight Project, Inc.
40 Rector Street
9th Floor
New York, NY 10006
www.STOPSpying.org

STOP
SURVEILLANCE TECHNOLOGY
OVERSIGHT PROJECT