Journal of Privacy and Confidentiality
Vol. 10 (2) 2020

Editorial

Submitted June 2020
Published June 2020

ON PRIVACY IN THE AGE OF COVID-19

CYNTHIA DWORK[*], ALAN F. KARR[†], KOBBI NISSIM[‡], AND LARS VILHUBER[**]

[*] Editor-in-Chief, Journal of Privacy and Confidentiality, and Harvard University

[†] Editor, Journal of Privacy and Confidentiality, and AFK Analytics, LLC

[‡] Editor, Journal of Privacy and Confidentiality, and Georgetown University

[**] Managing Editor, Journal of Privacy and Confidentiality, and Cornell University

As a third of the world population has been in lockdown [1], nearly half a million people have died of COVID-19 [2], and the world's economies have nosedived, policy makers and the public clamor for good news, or even just less uncertainty. Questions such as "Might I be infected if I go to work?" or "Does wearing a mask help prevent the spread of the disease?" are being asked. Answering these questions requires data! We need data on the infectiousness of the disease, as well as the efficacy of interventions such as lockdowns, distancing, and protective measures. Because the disease is novel, we do not know whether scientifically collected data from previous pandemics are relevant. Both repurposing relevant existing data collections, and the quick and effective design of new data collections are top priorities for informed, high quality decision-making.

But, potentially relevant existing and currently growing data collections were not initiated with the intent of fighting a pandemic. Some data were collected by private entities for unrelated commercial applications, or by governments. Cell phone tracking, geo-located electronic purchase transactions, and vehicle trajectories—all givens of modern life—have suddenly became (potentially) relevant for diagnostics and policy planning, if appropriately informed by research. Access to these data by parties other than those originally collecting them has therefore become important, even critical.

This situation is the epitome of *mission creep*. Initially, the creeping seems to be in a socially positive direction. However, the (further) concentration of information, and the gathering of new information for the same good use, are vulnerable to future, unsavory, mission creep, not just for the data but also for the new mechanics of their collection. Among concerns are new operating systems for cell phones embraced in the fight against the pandemic: the helpful technology that records your prolonged proximity for notification of COVID-19 exposure gathers more about you than that. Whom you encounter also reveals information about your social and political contacts, which can be used for non-health

Key words and phrases: COVID-19, privacy, choice.

[*] The opinions expressed here are those of the authors, and do not reflect the opinions of any of the institutions that the authors are affiliated with. JPC Editor John M. Abowd has recused himself from this editorial, and was not involved in the drafting or final editing.

JPrivacy Confidentiality
www.journalprivacyconfidentiality.org
DOI:10.29012/jpc.749

purposes, from marketing and advertising to identification. As one extreme example: Who accompanied you, and whom did you meet, at the Black Lives Matter demonstration?

Balancing privacy (what to ask), confidentiality (what to keep and how to use it), and the societal value given the issues (lives and livelihoods)—have become (almost) front page news. About half of Americans (54%) think it is unacceptable for the government to use cellphones for contact tracing, possibly because 60% don't believe that it provides utility[1]. Respondents were not asked if they objected to private companies tracking their whereabouts—and yet numerous such companies have been doing so, and have recently published COVID-19-related datasets [4, 5]. Should national state or local governments publish much or little demographic detail on those infected [6]? What is to be done with tracing apps now appearing as society starts to exit the lockdown [7, 8, 9, 10, 11, 12]? Will governments use the data "for good" or for possibly nefarious purposes [13]?

Since its inception 11 years ago, this journal has been exploring the methods to protect privacy and confidentiality, and the methods to assess the consequences thereof. When the journal's founders (including some of the current authors) set out to provide a forum for the "many data users from all of the fields [that] perform analyses that are conditioned on the privacy and confidentiality protections imposed on their work without all the means to assess the consequences of those measures on the inferences they have made"[14], they knew these topics warranted scrutiny, collaboration, and multi-disciplinary approaches. Privacy concerns are not new [15, 16], but new paradigms, in particular differential privacy [17, 18], have provided a more complete toolkit to conceptualize, reason about, discuss, and address the issues. Even though technical details of the toolkit are not broadly accessible, that discussion is now so much more relevant.

Progress has been made. Statistical agencies [19] and private companies [20, 21, 22, 23] have started to implement strong privacy safeguards. It is thus encouraging to see new data publications in the current crisis become rapidly available with such strong confidentiality protections [24, 25].

However, while we have made big strides toward understanding privacy-preserving data analytics, the same cannot be said for contact tracing via cell phone apps, a process that has not yet undergone rigorous threat modeling. (Information obtained via contact tracing through commercial mechanisms does not currently carry the same legal confidentiality protections as that obtained by public health officials.) The lack of threat modeling flies in the face of decades of experience and deeply ingrained best practices—in theory and in real life!—in cryptography and privacy. While a crisp statement of the problem to be solved may be easy, the contact tracing literature, which is mostly in the form of websites describing proposed solutions and apps, lacks a clear description of the goals and resources of the privacy adversary. We must take into account that the adversary may be government or industry, keeping in mind that the former can buy data from the latter, or even an arbitrary member of the population.

For example, exchanges of random ephemeral cell phone identifiers are described as "not revealing geographic location", but cellphones adversarially placed in fixed locations can, *ex post facto*, reconstruct the movements of anyone using the app who receives a positive

[1] Pew Research Center [3]. The exact question is "Do you think it is acceptable or unacceptable for the government to use people's cellphones to track the location of people [...] who may have had contact with someone who tested positive for the coronavirus." The utility question was "If the government tracked people's location through their cellphone during the coronavirus outbreak, do you think this would [...] not make much of a difference in limiting the spread."

diagnosis and follows the notification protocol. In part because, historically, analytical approaches to privacy have not addressed harm, there is no recognition that a loss in privacy is incurred by those who are made vulnerable, by their infected status, to hate crimes [26]. Moreover, there is no analysis justifying concessions made on the privacy front to accommodate utility and efficiency.

It is also important to frame the problem in a truly societal context. Tracing systems that only address the needs of those who can afford cell phones, or that do not accompany notice of exposure with the assistance needed to endure quarantine and to obtain treatment, smack of technological imperialism and will be of low utility: If we forget that the apps track devices, not people, we will fail to reckon with existential economic choices.

The confluence of the COVID-19 pandemic and broadening awareness of structural racism and economic inequality worldwide appropriately engender deeper scrutiny of surveillance writ large. Policing practices already carry their own privacy and confidentiality issues, such as use of CCTV and facial recognition software that performs differently across racial groups [27, 28, 29, 30, 31]. By the same token, contact-identifying apps, even when used solely for the purposes for which they were designed, have an “us” versus “them” sensibility, protecting the advantaged without benefiting, for instance those who must work outside the home in order to eat.

These disparities in impact underscore the urgent need for *real and equitable* solutions: increased access to affordable health care and testing, relief from jobs with high exposure, and opportunities to move away from congested areas. The contrast with patchy surveillance techniques exhibiting poorly understood privacy properties that exacerbate distrust could not be sharper. Science needs to be both smart and wise in order to be of value to society, and to resist political forces that seek to abrogate it. To this end, we solicit thoughtful contributions on technology and its application in the fight against COVID-19, from across the broad array of disciplines represented in the JPC stakeholder communities.

References

[1] Statista Infographics. Infographic: What Share of the World Population Is Already on COVID-19 Lockdown?, April 2020. https://www.statista.com/chart/21240/enforced-covid-19-lockdowns-by-people-affected-per-country/ (accessed 2020-06-19).

[2] World Health Organization. Coronavirus disease (COVID-19) Situation Report. Technical Report 155, World Health Organization, June 2020. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200623-covid-19-sitrep-155.pdf?sfvrsn=ca01ebe_2 (accessed 2020-06-24).

[3] Pew Research Center. 2020 Pew Research Center's American Trends Panel-wave 65 - April 2020 - Final Topline. Technical report, Pew Research Center, 2020. https://www.pewresearch.org/wp-content/uploads/2020/04/Topline-COVID-cellphones.pdf (accessed 2020-06-18).

[4] Unacast. Covid-19 Migration Patterns, 2020. https://www.unacast.com/covid19/covid-19-migration-patterns (accessed 2020-06-19).

[5] umlaut analyzes network behavior changes as COVID-19 spreads, March 2020. https://www.rcrwireless.com/20200325/big-data-analytics/umlaut-analyzes-network-behavior-changes-as-covid-19-spreads (accessed 2020-06-19).

[6] Thomas Fuller. How Much Should the Public Know About Who Has the Coronavirus? The New York Times, March 2020. https://www.nytimes.com/2020/03/28/us/coronavirus-data-privacy.html (accessed 2020-06-18).

[7] Hyunghoon Cho, Daphne Ippolito, and Yun William Yu. Contact Tracing Mobile Apps for COVID-19: Privacy Considerations and Related Trade-offs. arXiv:2003.11511 [cs], March 2020. http://arxiv.org/abs/2003.11511 (accessed 2020-06-18). arXiv: 2003.11511.

[8] DP-3T partners. Decentralized Privacy-Preserving Proximity Tracing Github, June 2020. https://github.com/DP-3T/documents (accessed 2020-06-18).

[9] Patrick Howell O'Neill, Tate Ryan-Mosley, and Bobbie Johnson. A flood of coronavirus apps are tracking us. Now it's time to keep track of them., 2020. https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/ (accessed 2020-06-18).

[10] Andy Moss, Connor Spelliscy, and John Borthwick. Demonstrating 15 contact tracing and other tools built to mitigate the impact of COVID-19. TechCrunch. https://techcrunch.com/2020/06/05/demonstrating-15-contact-tracing-and-other-tools-built-to-mitigate-the-impact-of-covid-19/ (accessed 2020-06-18).

[11] Jason Horowitz and Adam Satariano. Europe Rolls Out Contact Tracing Apps, With Hope and Trepidation. The New York Times, June 2020. https://www.nytimes.com/2020/06/16/world/europe/contact-tracing-apps-europe-coronavirus.html (accessed 2020-06-18).

[12] Kobi Leins, Christopher Culnane, and Benjamin IP Rubinstein. Tracking, tracing, trust: contemplating mitigating the impact of COVID-19 through technological interventions. The Medical Journal of Australia, 213(1), June 2020. https://doi.org/10.5694/mja2.50669.

[13] Dave Gershgorn. We Mapped How the Coronavirus Is Driving New Surveillance Programs Around the World, May 2020. https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9 (accessed 2020-06-18).

[14] John M. Abowd, Kobbi Nissim, and Chris J. Skinner. First Issue Editorial. Journal of Privacy and Confidentiality, 1(1), April 2009. https://doi.org/10.29012/jpc.v1i1.562.

[15] Rebecca Kraus. Statistical Déjà Vu: The National Data Center Proposal of 1965 and Its Descendants. Journal of Privacy and Confidentiality, 5(1), August 2013. https://doi.org/10.29012/jpc.v5i1.624.

[16] Margo J. Anderson and William Seltzer. Federal Statistical Confidentiality and Business Data: Twentieth Century Challenges and Continuing Issues. Journal of Privacy and Confidentiality, 1(1), April 2009. https://doi.org/10.29012/jpc.v1i1.563.

[17] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating Noise to Sensitivity in Private Data Analysis. In Theory of Cryptography, volume 3876, pages 265–284, Berlin, Heidelberg, 2006. Springer Berlin Heidelberg. https://doi.org/10.1007/11681878_14.

[18] Cynthia Dwork, Frank McSherry, Kobbi Nissim, and Adam Smith. Calibrating Noise to Sensitivity in Private Data Analysis. Journal of Privacy and Confidentiality, 7(3): 17–51, May 2017. https://doi.org/10.29012/jpc.v7i3.405.

[19] John M. Abowd. The U.S. Census Bureau Adopts Differential Privacy. In Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining, pages 2867–2867, London United Kingdom, July 2018. ACM. ISBN 978-1-4503-5552-0. https://doi.org/10.1145/3219819.3226070.

[20] Úlfar Erlingsson, Vasyl Pihur, and Aleksandra Korolova. RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response. In Proceedings of the 21st ACM Conference on Computer and Communications Security, Scottsdale, Arizona, 2014. https://arxiv.org/abs/1407.6981.

[21] Apple Differential Privacy Team. Learning with Privacy at Scale - Apple. Apple Machine Learning Journal, 1(8), December 2017. https://machinelearning.apple.com/2017/12/06/learning-with-privacy-at-scale.html (accessed 2020-06-19). cccccclulnjigtvnuhthglfhhjdktevbekjkvdcvtkhh.

[22] Sarah Bird. Introducing the new differential privacy platform from Microsoft and Harvard's OpenDP, May 2020. https://cloudblogs.microsoft.com/opensource/2020/05/19/new-differential-privacy-platform-microsoft-harvard-opendp/ (accessed 2020-06-24).

[23] Carey Radebaugh and Ulfar Erlingsson (TensorFlow BLOG). Introducing tensorflow privacy: Learning with differential privacy for training data, 2019. https://blog.tensorflow.org/2019/03/introducing-tensorflow-privacy-learning.html (accessed 2020-06-24).

[24] Ahmet Aktay, Shailesh Bavadekar, Gwen Cossoul, John Davis, Damien Desfontaines, Alex Fabrikant, Evgeniy Gabrilovich, Krishna Gadepalli, Bryant Gipson, Miguel Guevara, Chaitanya Kamath, Mansi Kansal, Ali Lange, Chinmoy Mandayam, Andrew Oplinger, Christopher Pluntke, Thomas Roessler, Arran Schlosberg, Tomer Shekel, Swapnil Vispute, Mia Vu, Gregory Wellenius, Brian Williams, and Royce J. Wilson. Google COVID-19 Community Mobility Reports: Anonymization Process Description (version 1.0). arXiv:2004.04145 [cs], April 2020. http://arxiv.org/abs/2004.04145

(accessed 2020-06-18).

[25] Amaç Herdağdelen, Alex Dow, Bogdan State, Payman Mohassel, and Alex Pompe. Protecting privacy in Facebook mobility data during the COVID-19 response, June 2020. https://research.fb.com/blog/2020/06/protecting-privacy-in-facebook-mobility-data-during-the-covid-19-response/ (accessed 2020-06-24).

[26] Helier Cheung, Zhaoyin Feng, and Boer Deng (BBC News). Coronavirus: What attacks on asians reveal about american identity, 2020. https://www.bbc.com/news/world-us-canada-52714804 (accessed 2020-06-23).

[27] Joy Buolamwini and Timnit Gebru. Gender shades: Intersectional accuracy disparities in commercial gender classification. In Conference on fairness, accountability and transparency, pages 77–91, 2018.

[28] Reuters (NBC News). Facial recognition leads to first wrongful u.s. arrests, activists say, 2020. https://www.nbcnews.com/tech/security/facial-recognition-leads-first-wrongful-u-s-arrests-activists-say-n1231971 (accessed 2020-06-23).

[29] Bobby Allyn (NPR). Ibm abandons facial recognition products, condemns racially biased surveillance, 2020. https://www.npr.org/2020/06/09/873298837/ibm-abandons-facial-recognition-products-condemns-racially-biased-surveillance (accessed 2020-06-23).

[30] Karen Weise and Natasha Singer (The New York Times). Amazon pauses police use of its facial recognition software, 2020. https://www.nytimes.com/2020/06/10/technology/amazon-facial-recognition-backlash.html (accessed 2020-06-23).

[31] Brian Fung (CNN Business). Microsoft says it won't sell facial recognition technology to us police departments, 2020. https://www.cnn.com/2020/06/11/tech/microsoft-facial-recognition-police/index.html (accessed 2020-06-23).