The rise and regulation of thermal facial recognition technology during the COVID-19 pandemic

Meredith Van Natta, Paul Chen, Savannah Herbek, Rishabh Jain, Nicole Kastelic, Evan Katz, Micalyn Struble, Vineel Vanam and Niharika Vattikonda

Duke University Initiative for Science and Society, Durham, NC 27710, USA

*Corresponding author. E-mail: Meredith.Van.Natta@duke.edu

INTRODUCTION

As the current COVID-19 pandemic sweeps the globe and dramatically alters society, governments and corporations are turning to novel uses of biometric technologies to limit contagion and maintain economic opportunities. Technologies that may have once seemed like the province of science fiction—such as thermal facial recognition, remote fever detection, or smartphone-based immunity certificates—are now not only possible but also already in use. This raises important questions about the potential privacy implications of the widespread collection and use of such personal data. While multimodal biometric surveillance technologies such as these may prove useful in slowing the spread of SARS–CoV-2, we caution that the ability of governments and corporations to leverage these technologies will likely persist beyond the current public health emergency. Just as many of the privacy concessions made in the USA Patriot Act have become permanent since the emergency circumstances of September 11, 2001, the privacy-limiting technologies unleashed during this pandemic may well persist unless policies are enacted now to regulate their use and ensure responsible oversight. Recognizing that these emergent technologies may become entrenched long after this
public health crisis subsides, we focus here on the case of fever checks and thermal facial recognition technology to illustrate the current state of the technology, existing policies related to its use, and suggestions for proactive policies to govern its deployment during and beyond the present pandemic.

**FEVER CHECKS AND COVID-19**

While SARS–CoV-2 (the virus that causes COVID-19) is particularly pernicious due to its high rate of asymptomatic transmission, identifying symptomatic individuals is nevertheless crucial to containing its spread.1 Among a growing list of COVID-19 symptoms, fever (defined as a body temperature above 100.4°F/38°C) is one of the tell–tale symptoms of infection.2 As the pandemic has gained momentum, government agencies and corporations are increasingly turning to fever checks as a mechanism for gauging the potential presence of SARS–CoV-2 among citizens, travelers, and employees. This includes using traditional thermometers as well as infrared cameras that assess internal temperature by measuring the energy emanating from the inner corner of the eye and running the data through a machine learning algorithm—technologies that have been used with limited success in previous pandemics.3 Such remote thermal detection would be particularly useful in situations where it is impractical to take individuals’ temperature (such as in a crowd), but existing studies cast doubt on the ability of these technologies to accurately and consistently measure core temperature.4 Fever check technologies are known to misidentify individuals under certain conditions that may elevate core temperature (such as through recent exercise) or lower

---

1 U.S. Centers for Disease Control and Prevention, Clinical Questions about COVID-19: Questions and Answers (Apr. 16, 2020), https://www.cdc.gov/coronavirus/2019-ncov/hcp/faq.html (accessed Apr. 18, 2020).
2 At the time of this writing, symptoms of COVID-19 include fever, cough, shortness of breath, chills, repeated shaking with chills, muscle pain, headache, sore throat, and/or new loss of taste or smell. See U.S. Centers for Disease Control and Prevention, Coronavirus Disease 2019 (COVID-19): Symptoms of Coronavirus (Mar. 20, 2020), https://www.cdc.gov/coronavirus/2019-ncov/symptoms-testing/symptoms.html (accessed March 30, 2020) and U.S. Centers for Disease Control and Prevention, CARE: Check and Record Everyday (Mar. 11, 2020), https://www.cdc.gov/coronavirus/2019-ncov/downloads/COVID-19_CAREKit_ENG.pdf (accessed April 16, 2020).
3 Patricia C. Priest et al., Thermal Image Scanning for Influenza Border Screening: Results of an Airport Screening Study, 6 PLoS One 1 (2011); G. Samaan et al., Border Screening for SARS in Australia: What Has Been Learnt? 180 Med. J. Aust. (2004); ECDC. Technical Report: Infection Prevention and Control Measures for Ebola Virus Disease, Entry and Exit Screening Measures, (2014); C.W Lee et al., A Loophole in International Quarantine Procedures Disclosed During the SARS Crisis, 4 Travel Med. Infect. Dis. (2006); Hiroshi Nishiura & Kazuko Kamiya, Fever Screening During the Influenza (H1N1-2009) Pandemic at Narita International Airport, Japan, 11 BMC Infect. Dis. (2011).
4 Alex Andrade Fernandes et al., Validity of Inner Canthus Temperature Recorded by Infrared Thermography as a Non-invasive Surrogate Measure for Core Temperature at Rest, During Exercise and Recovery, 62 J. Therm. Biol. 50–55 (2016); Ottawa (ON): Canadian Agency for Drugs and Technologies in Health, Non-Contact Thermometers for Detecting Fever: A Review of Clinical Effectiveness (Nov. 20, 2014), https://www.ncbi.nlm.nih.gov/books/NBK263237/ (accessed April 15, 2020); Varvara A. Mouchtouri et al., Exit and Entry Screening Practices for Infectious Diseases among Travelers at Points of Entry: Looking for Evidence on Public Health Impact, 16 Int. J. Environ. Res. Public Health 23 (2019), https://doi.org/10.3390/ijerph16234638 (accessed May 4, 2020); D. Bitar et al., International Travels and Fever Screening During Epidemics: A Literature Review on the Effectiveness and Potential Use of Non-contact Infrared Thermometers, 14 EUROSurveillance 6 (Feb. 12, 2009), https://www.eurosurveillance.org/images/dynamic/EE/V14N06/art19115.pdf (accessed May 4, 2020); U.S. Centers for Disease Control and Prevention, Non-contact Temperature Measurement Devices: Considerations for Use in Port of Entry Screening Activities (2014), http://wwwnc.cdc.gov/travel/pdf/ebola-non-contact-temperature-measurementguidance.pdf (accessed May 4, 2020); M.R. Tay et al., Comparison
it (such as having been in the cold for an extended time or having used medicine to mask a fever). Additionally, researchers considering the asymptomatic transmission of SARS–CoV-2 and its incubation period alongside data on the sensitivity of thermal scanning technology have estimated that 46 per cent of infected travelers may escape detection.

Despite the potential inaccuracies and limitations of these technologies, they have been widely adopted for the purpose of detecting COVID-19 symptoms. While the Americans with Disabilities Act prohibits companies in the USA from requiring workers to submit to medical exams, the Equal Employment Opportunity Commission recently announced revised rules that permit employers to take workers’ temperatures regularly and withdraw employment offers if a newly hired worker received a COVID-19 diagnosis. Even before that announcement, Amazon had begun supplementing traditional thermometers with thermal cameras to monitor employees’ temperatures at several warehouse locations, as well as to check for fevers among employees and customers at their Whole Foods stores. Anyone flagged as febrile must undergo a second forehead thermometer check to verify temperature. At the time of this writing, other examples of mandatory fever checks have ranged from several cruise lines and grocery stores, to jails, co-working spaces, the White House, statewide employee...
Thermal facial recognition technology during COVID-19 pandemic testing, numerous cloud technology firms, hospitals, hotels, and some European borders. Liechtenstein has partnered with Swiss researchers to institute a voluntary campaign in which users’ wearable bracelet technology will collect temperature (as well as breathing and heart rate) data to monitor and curb coronavirus transmission. Emirates Airlines is even conducting blood tests (for SARS–CoV-2 antibodies), along with temperature and heart and respiratory rate monitoring, on prospective passengers prior to boarding.

In China, which experienced the earliest wave of infections, state law enforcement agents have conducted temperature checks at highway checkpoints, and in some cases state officers have forcibly entered private residences to perform these checks. In South Korea, officials have begun conducting fever checks and limiting travel certificates to the USA only for those who registered a body temperature below 99.5°F/37.5°C. Thailand also recently employed fever-detecting cameras into its biometric border screening system to measure travelers’ temperatures and notify border officers of febrile individuals. Clearly, fever check technology—particularly remote fever detection—is becoming ubiquitous throughout the post-COVID-19 world.

14 Andrew J. Tobias, Ohio Gov. Mike DeWine Asks Employers to Make Daily Temperature Checks of Workers, Cleveland (Mar. 18, 2020), https://www.cleveland.com/open/2020/03/ohio-gov-mike-dewine-asks-state-employers-for-daily-temperature-checks-of-workers.html (accessed Apr. 6, 2020).
15 Paresh Dave, Coronavirus Work-from-Home Push Means Long Nights, Employee Health Checks for Cloud Firms, Reuters (Mar. 13, 2020), https://www.reuters.com/article/us-health-coronavirus-cloud/coronavirus-work-from-home-push-means-long-nights-employee-health-checks-for-cloud-firms-idUSKBN21031M (accessed Apr. 8, 2020).
16 Omer Kabir, Face Recognition Startup AnyVision to Deploy Thermal Cameras at Tel Aviv Hospital, CTECH (Apr. 7, 2020), https://www.calcalistech.com/ctech/articles/0,7340,L-3806587,00.html (accessed Apr. 10, 2020).
17 Bryan Horwath, Wynn Resorts to Use Thermal Cameras to Check Guests for Fever, Las Vegas Sun (Mar. 13, 2020), https://lasvegassun.com/news/2020/mar/13/wynn-resorts-to-use-thermal-cameras-to-check-guest (accessed Apr. 8, 2020); AFP Relax News, New Normal in Virus-hit China: High-tech Tracking and Fever Checks, Yahoo! News (Mar. 4, 2020), https://news.yahoo.com/normal-virus-hit-china-high-tech-tracking-fever-154511422.html (accessed Apr. 10, 2020).
18 Reuters, Slovenia to Introduce Health Checks on Border with Austria, Reuters (Mar. 24, 2020), https://www.reuters.com/article/us-health-coronavirus-slovenia-austria/slovenia-to-introduce-health-checks-on-border-with-austria-idUSKBN21B2SB (accessed Apr. 16, 2020).
19 Luana Pascu, Liechtenstein to Provide Citizens with Biometric Bracelets to Contain Coronavirus Biometric Update (Apr. 16, 2020), https://www.biometricupdate.com/202004/liechtenstein-to-provide-citizens-with-biometric-bracelets-to-contain-coronavirus (accessed Apr. 30, 2020).
20 Karla Cripps, Airline Passengers Undergo Covid-19 Blood Tests Before Boarding (Apr. 16, 2020), https://www.cnn.com/travel/article/emirates-passengers-blood-test-covid-19/index.html (accessed Apr. 20, 2020).
21 Donald G. McNeil Jr., Inside China’s All-Out War on the Coronavirus, New York Times (Mar. 4, 2020), https://www.nytimes.com/2020/03/04/health/coronavirus-china-aylward.html (accessed Apr. 7, 2020).
22 Donald G. McNeil Jr., The Virus Can Be Stopped, but Only with Harsh Steps, Experts Say, New York Times (Mar. 22, 2020), https://www.nytimes.com/2020/03/22/health/coronavirus-restrictions-us.html (accessed Apr. 6, 2020).
23 Song Sang-ho (송상호), Government to Conduct Fever Checks This Week on Passengers Traveling to U.S. Yonhap News Agency (Mar. 10, 2020), https://en.yna.co.kr/view/AEN20200310005700325 (accessed Apr. 12, 2020).
24 DERMALOG Identification Systems GmbH, DERMALOG Provides the World’s First Biometric Border Control System with Integrated Fever Detection (Feb. 13, 2020), https://www.prnewswire.com/in/news-releases/dermalog-provides-the-world-s-first-biometric-border-control-system-with-integrated-fever-detection-858822644.html (accessed Apr. 11, 2020).
THERMAL FACIAL RECOGNITION TECHNOLOGY: PRIVACY AMIDST PANDEMIC?

In such exceptional times, one could argue that fever checks offer substantial population health benefits with limited long-term impacts on personal privacy. Yet, several private companies have integrated thermal imaging with facial recognition technology. Despite the aforementioned limitations of thermal detection technology and known shortfalls of facial recognition technology,25 firms around the world are marketing such multimodal biometric technologies as effective tools for combating the pandemic. Collectively these companies’ claims, which have yet to be systematically evaluated in the empirical literature, suggest clear benefits of combining thermal detection with facial recognition capabilities to detect and track potentially infected individuals. For example, police in China are currently using devices from Hanwang Technology that claim to identify an individual’s name within a second upon detecting a temperature over 99.5°F/37.5°C.26 The company claims that the technology is 95 percent accurate, even in a group of 30 individuals or among people wearing masks.27 China-based firms SenseTime and Sunell are also selling similar technology.28 Sunell recently unveiled a body temperature detection network camera that they assert is able to identify individuals, collect real-time biometric data, and trigger a warning system upon detecting an unusual temperature.29 Additionally, Chinese startup Rokid has developed multimodal biotechnology that includes thermal-imaging wearable glasses, a technology they are currently marketing to US hospitals and local municipalities.30 These smart glasses, which Rokid suggests can be paired with facial recognition software, use an infrared sensor that Rokid claims can detect temperatures of up to 200 people as far away as 3 m, and they are already being used in China in national parks, schools, and by national authorities.31

In Singapore, Ramco Innovation Lab is promoting its integrated thermal imaging and facial recognition technology to launch an attendance tracking system that will ostensibly enable organizations to track employees and visitors with elevated

25 See e.g., Joy Adowaa Buolamwini, Gender Shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers, Master of Science Thesis for the Massachusetts Institute of Technology (2017); and Inioluwa Deborah Raji et al. Saving Face: Investigating the Ethical Concerns of Facial Recognition Auditing AIES ’20: Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society (2020), https://doi.org/10.1145/3375627.3375820 (accessed May 2, 2020).
26 Thor Benson, Surgical Masks Are No Match for China’s Facial Recognition Technology, Inverse (Mar. 26, 2020), https://www.inverse.com/innovation/china-now-has-facial-recognition-that-can-identify-people-wearing-surgical-masks (accessed Apr. 10, 2020).
27 Martin Pollard, Even Mask-wearers Can be ID’d, China Facial Recognition Firm Says, Reuters (Mar. 9, 2020), https://www.reuters.com/article/us-health-coronavirus-facial-recognition/even-mask-wearers-can-be-idd-china-facial-recognition-firm-says-idUSKBN20W0WL (accessed Apr. 10, 2020).
28 Rebecca Heilweil, Coronavirus is the First Big Test for Futuristic Tech that Can Prevent Pandemics, Vox (Feb. 27, 2020), https://www.vox.com/recode/2020/2/27/21156358/surveillance-tech-coronavirus-china-facial-recognition (accessed Apr. 15, 2020).
29 Sunell Security, AI Thermal-Body Temperature Measurement Camera, https://sunellsecurity.com/pro_detail.php?id=232 (accessed Apr. 10, 2020).
30 Jake Bright & Rita Liao, Chinese Startup Rokid Pitches COVID-19 Detection Glasses in US (Apr. 16, 2020), https://techcrunch.com/2020/04/16/chinese-startup-rokid-pitches-covid-19-detection-glasses-in-u-s/ (accessed Apr. 20, 2020).
31 Id.
temperatures. This multimodal technology includes contact tracing that sends notifications to event attendees if any person exhibits COVID-19 symptoms and uses facial recognition to capture both an employee’s presence and their temperature. A visitors feature also sends notifications to management when anyone with an elevated temperature enters the premises. The company touts that this contactless tracking system can be integrated with sliding doors, kiosks, and turnstiles to mitigate SARS–CoV-2 exposure by restricting access based on temperature range and recommending testing of flagged individuals, and they will share contract-tracing data with health agencies if mandated by the government.

Beyond Asia, Australia recently reached a deal with drone manufacturer Draganfly to develop ‘pandemic drones’ equipped with thermal recognition technology that they say can monitor temperatures, heart rates, and respiratory patterns, as well as sneezing and coughing in coronavirus hotspots. In the UK, Silent Sentinel is marketing a line of what they describe as highly sensitive, high-resolution fever detection cameras that can be deployed as a standalone system or part of a network to conduct precise temperature detection and profiling. In Italy, the government recently purchased kits from Beijing-based biotechnology company Polysense with optional integrated thermal facial recognition technology to monitor populations at airports, train stations, schools, shopping centers, and on public transportation to aid COVID-19 containment efforts. The Polysense devices also purport to offer optional biometric features, including infrared technology, the ability to store up to 65,000 facial images, and integrated gate and door access protocols.

ETHICAL CONCERNS, RISKS, AND BENEFITS
While studies suggest that multimodal biometric systems increase overall identification accuracy compared with individual component technologies, their deployment has been limited historically by cost constraints. As the examples listed above indicate, however, the rapid progression of the current coronavirus pandemic has sufficiently alarmed governments, corporations, and other institutions to justify aggressive

32 Ramco Innovation Lab, Ramco Innovation Attendance Tracking with Facial Recognition and Thermal Scanning Detects COVID-19, Kiosk Marketplace (Mar. 29, 2020), https://www.kioskmarketplace.com/news/ramco-innovation-attendance-tracking-with-facial-recognition-and-thermal-scanning-detects-covid-19/ (accessed Apr. 16, 2020).
33 Id.
34 Ramco Innovation Lab. Move to a Touchless Employee Experience (Apr. 10, 2020), https://campaigns.ramco.com/ramco-time-and-attendance-with-temperature-recording-system?ga=2.250062478.946614035.1587064799-1313882007.1587064799 (accessed Apr. 16, 2020).
35 Luke Dormehl, Pandemic Drones that Can Detect Fevers and Coughing will Soon Take to the Sky (Mar. 26, 2020), https://www.digitaltrends.com/cool-tech/draganfly-drones-detecting-covid-19/ (accessed Apr. 7, 2020); Luke Dormehl, Using Drones to Detect Coronavirus? It’s Not as Crazy as it Sounds (Feb. 22, 2020), https://www.digitaltrends.com/cool-tech/draganfly-drone-coronavirus/ (accessed Apr. 7, 2020).
36 Silent Sentinel. Silent Sentinel Launches New Standoff Fever Detection Camera, https://silentsentinel.com/fever-detection-camera/ (accessed Apr. 16, 2020).
37 Chris Burt, Fever Detection and Facial Recognition Systems Launched to Help Prevent Virus Spread (Mar. 25, 2020), https://www.biometricupdate.com/202003/fever-detection-and-facial-recognition-systems-launched-to-help-prevent-virus-spread (accessed Apr. 10, 2020).
38 Id.
39 DAVID MALTONI ET AL., HANDBOOK OF FINGERPRINT RECOGNITION (2009).
Thermal facial recognition technology during COVID-19 pandemic

investment in such technologies. Within this emergency context, it may seem reasonable to integrate thermal scanning with facial recognition technology as an effective and efficient means to identify and track infected individuals.\textsuperscript{40} We argue, however, that the emergence of this type of multimodal biometric system blurs the lines between ‘over-the-skin’ and ‘under-the-skin’ surveillance in ways that demand closer scrutiny and potential regulation. While traditional biometrics such as fingerprinting have relied on external features, thermal facial recognition offers a physically unobtrusive way to obtain both external and internal biometric information purely via external scan.\textsuperscript{41} Thus, despite the significant privacy risks it poses, thermal facial recognition may be misconstrued as a minimally invasive technology, as it is significantly more discreet and anatomically noninvasive than other methods of collecting under-the-skin biometric data (e.g., a blood draw or buccal swab for DNA analysis or tympanic or rectal temperature checks). This development represents a new biometric frontier that should be approached critically now rather than on a post hoc basis once the technology is already ubiquitous.

In the short term, the expansion of novel multimodal biometric surveillance may be partially excused as a necessary technological compromise to protect health and safety by bolstering our capacity to manage contagion and prevent future pandemics.\textsuperscript{42} However, the concession of such sensitive data (and the personal information it may reveal) opens new avenues for misuse and suggests the need for responsive, responsible policymaking at this time. We suggest taking a step back to ask what problem thermal facial recognition technology intends to solve, whether it does so accurately and effectively, and—if so—how it can best be deployed and regulated. Just as the use of smartphone geolocation services for pandemic tracing can reveal sensitive personal and health information about individuals, the continual, passive monitoring of individuals’ temperatures could reveal previously private health information based on body temperature variances over time (e.g., menstrual cycle, pregnancy, menopause, or substance use) and link that to identifying documents in ways that are poorly understood as this technology begins to roll out worldwide.\textsuperscript{43} This is especially problematic given the nascent nature of fever-based biometric technologies. We currently do not know the extent of information that can be deduced using data gathered by these technologies. Existing scholarship suggests that future developments in data analysis techniques may allow for these data to be used in a manner that increasingly violates privacy, and

\begin{itemize}
\item Bright & Liao, \textit{supra} note 30.
\item Yuval Noah Harari, Yuval Noah Harari: the World after Coronavirus, Financial Times (Mar. 20, 2020), https://www.ft.com/content/19d90308-6858-11ea-a3c9-1fe6fedca75 (accessed Apr. 14, 2020).
\item Mark McClellan et al., \textit{A National COVID-19 Surveillance System: Achieving Containment}, Duke University Margolis Center for Health Policy (Apr. 17, 2020), https://healthpolicy.duke.edu/sites/default/files/atoms/files/covid-19_surveillance_roadmap_final.pdf (accessed Apr. 19, 2020).
\item ML Cuddy, \textit{The Effect of Drugs on Thermoregulation}, 15 AACN CLIN. ISSUES (2015), https://www.ncbi.nlm.nih.gov/pubmed/15461041 (accessed Apr. 14, 2020); William D Hicks, Jefferson E Holcomb & Melissa A Alexander, \textit{Drug Testing and Community Supervision Outcomes}, 47 CRIM. JUSTICE BEHAV. 419–436 (2020), https://journals.sagepub.com/doi/abs/10.1177/0093854819898219 (accessed Apr. 14, 2020); Ottawa (ON): Canadian Agency for Drugs and Technologies in Health, \textit{Non-Contact Thermometers for Detecting Fever: A Review of Clinical Effectiveness} (Nov. 20, 2014), https://www.ncbi.nlm.nih.gov/books/NBK263237/ (accessed May 1, 2020).
\end{itemize}
such scholars recommend caution as they are deployed.44 Unless clear protections are in place, it is likely that data brokers, advertisers, employers, and law enforcement agencies could use such data to extract information about underlying health conditions or stigmatized behaviors in ways that may undermine individuals’ privacy.45

Even if temperature monitoring is limited to a one-time event, such as attempting to enter a grocery store, airport, or train station in the form of an ostensible on-the-spot immunity certificate, questions remain about the precision and accuracy of some thermal detection technologies and their integration with multimodal biometric surveillance devices. While some firms claim an ability to discern between increases in body temperature caused by exercise versus spikes caused by viral infection, there is no guarantee that such features are accurate or will be universally incorporated in system designs.46 Under normal circumstances, the US Food and Drug Administration would regulate thermal detection devices intended for medical use, but the agency recently announced that it does ‘not intend to object to the distribution and use of telethermographic systems intended for initial body temperature assessment for triage use […] where such devices do not create an undue risk in light of the public health emergency […]’.47 While the FDA does recommend that remote temperature devices only be used on one subject at a time in conjunction with a secondary, clinical-grade temperature measurement device, this recommendation is included as a labeling suggestion rather than a firm mandate.48 Without adequate regulation, unmonitored inaccuracies may inadvertently harm individuals who are flagged while attempting to shop, travel, or work and who, absent robust regulations, may have little recourse for rectification. In the event that individuals’ health profiles are logged continuously in the form of virtual, multimodal immunity certificates, such harms could be ongoing in discriminatory ways.49

BIOMETRICS, PANDEMIC, AND THE CURRENT POLICY TERRAIN

In the USA, six states have passed legislation that governs the collection and use of biometric information by commercial entities—laws that could serve as a model for regulating multimodal biometric technologies during and beyond the present

44 See e.g., ARVIND NARAYANAN ET AL., A PRECAUTIONARY APPROACH TO BIG DATA PRIVACY, in DATA PROTECTION ON THE MOVE (2016); Margaret Hu, Bulk Biometric Metadata Collection, 96 North Carolina Law Rev. 5 (2018); Sharon Naker & Dov Greenbaum, Now You See Me: Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy, 23 B.U. J. Sci. & Tech. L. 88 (2017).
45 Federal Trade Commission, Data Brokers: A Call for Transparency and Accountability (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerrreport.pdf (accessed Apr. 10, 2020); Lois Beckett, Everything We Know About What Data Brokers Know About You, ProPublica (June 13, 2014), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you (accessed Apr. 10, 2020).
46 Kabir, supra note 16.
47 U.S. Food and Drug Administration, Enforcement Policy for Telethermographic Systems During the Coronavirus Disease 2019 (COVID-19) Public Health Emergency Guidance for Industry and Food and Drug Administration Staff (Apr. 2020), https://www.fda.gov/media/137079/download (accessed Apr. 30, 2020).
48 Id. at 5–6.
49 Sheridan Prasso, Coronavirus Surveillance Helps, But the Programs Are Hard to Stop (Apr. 6, 2020), https://www.bloomberg.com/news/articles/2020-04-06/coronavirus-surveillance-helps-but-the-programs-are-hard-to-stop (accessed Apr. 16, 2020); Cripps, supra note 20.
pandemic. However, with the exception of Illinois and California (which have passed legislation that regulates the commercial use of thermal and facial information for fever checks), the scope of most of these laws does not extend to the collection of thermal facial data for noncommercial purposes. 50

Among all such state-level laws, the most comprehensive is Illinois’ Biometric Information Privacy Act (BIPA), which regulates the collection, use, and sharing of biometric information by commercial entities. 51 BIPA requires commercial entities to gain informed consent from individuals prior to scanning for biometric information and make publicly available a written policy of the process employed to destroy the biometric information. The law also creates a right of action for individuals whose biometric information was collected or used in violation of the law, regardless of whether the violation caused such individuals harm. Since the definition of biometric information in BIPA includes any information, regardless of capture method, that relies on biometric identifiers such as facial scans or eye scans, this law would regulate any technologies that use facial recognition technology to capture the temperature of a specific facial location. That would ostensibly include the aforementioned thermal facial recognition systems deployed by governments using products from companies like Sunell and Rokid; however, this right of action is limited to Illinois. For example, while Patel v Facebook (2010) established that Facebook violated Illinois’ BIPA by failing to delete biometric information within a certain timeframe, this precedent does not apply nationally. 52

In contrast to the passage of an independent biometric information privacy law in Illinois, California regulated the collection of biometric information through an extension of the California Consumer Privacy Act (CCPA), which establishes privacy protections on the use of personal information by commercial entities that have at least $25 million in annual revenue, have personal data on at least 50,000 individuals, or make half of their annual revenue from the sale of personal data. In 2019, the definition of personal information was appended to cover biometric information, which includes any physiological characteristics that can be combined with other identifying data to establish individual identity, such as health data and facial imagery. 53 Temperature measurements, which are physiological characteristics, would consequently fall within the scope of this law. The law requires businesses to inform consumers of which categories of their personal information are subject to collection and the purposes of collection prior to the time of collection. Consumers also have the right to request disclosure of the method and source of collection, access to any information collected from them, and deletion of any such information. Lastly, consumers have the right to opt out of the sale of their personal information, wherein the term ‘sale’ includes any transfer of personal information from the business to a third party for ‘valuable

50 See 740 ILCS/14, Public Act 095-994 (2010); 1.81.5. CAL. CIV. CODE § 1798.100-1798.199 (2018); 11 Texas Business and Commerce Code § 521, 19 Revised Code of Washington § 375, 4(7) Arkansas Code § 110 (2010), and New York Stop Hacks and Improve Electronic Data Security Act (“SHIELD” Act), N.Y. GEN. BUS. § 899-aa (2019).
51 Biometric Information Privacy Act of 2010, 740 ILCS/14, Public Act 095-994.
52 290 F. Supp. 3d 948 (N.D. Cal. 2018); see also Emily Birnbaum, Supreme Court Declines to Hear Facebook Facial Recognition Case, The Hill (Jan. 21, 20), https://thehill.com/policy/technology/479126-supreme-court-declines-to-hear-facebook-facial-recognition-case (accessed Apr. 7, 2020).
53 CAL. CIV. CODE § 1798.100-199.
Thermal facial recognition technology during COVID-19 pandemic

Hence, businesses may invoke this clause to share thermal information from fever checks, which seems likely given the recent sales of smart thermometer data for targeted advertisements and the generation of nationwide fever tracking maps.

While the CCPA generates a private right of action for certain breaches of the law, the scope of this right is substantially narrower than the right generated by BIPA. Individuals have a private right of action only if specified categories of their unencrypted personal information are subject to unauthorized access due to failure to use reasonable security precautions. The specified categories of personal information do not include biometric information, leaving individuals with no private recourse options upon the breach of their facial or thermal information. Instead, it is the responsibility of the Attorney General to bring about action for other types of violations. Therefore, while the CCPA may apply to a wider range of information collected from fever checks due to its protection of all physiological data in addition to facial data, it attributes substantially fewer enforcement rights to consumers than BIPA.

Beyond state-level legislation, a number of federal policies have some capacity to regulate multimodal biometric surveillance in ways that may impact the use of thermal facial recognition technology during the COVID-19 pandemic. For example, commercial entities that employ thermal recognition technologies are subject to federal standards of fairness and transparency through the Federal Trade Commission Act (FTC). Section 5 of the Act explicitly bans ‘unfair or deceptive acts or practices in or affecting commerce’, where an unfair practice includes any practice that causes substantial injury to a consumer acting reasonably and a deceptive practice includes any omission or practice that is likely to mislead a consumer acting reasonably.

While there is no specific judicial precedent supporting FTC authority to govern the collection or use of thermal information, there is substantial precedent to support FTC governance of personal information generally. The FTC has brought numerous actions against companies that misled consumers regarding the collection and use of their personal information or threatened the privacy of their personal information. Historically, the FTC has primarily prosecuted ‘deceptive’ privacy practices, such as the use of misleading disclosures or illegitimate mechanisms for consumers to

54 Id.
55 Sapna Maheshwari, This Thermometer Tells Your Temperature, Then Tells Firms Where to Advertise, New York Times (Oct. 23, 2018), https://www.nytimes.com/2018/10/23/business/media/fever-advertisements-medicine-clorox.html (accessed May 5, 2020).
56 US Health WeatherMap by Kinsa, https://healthweather.us/?mode=Atypical (accessed May 5, 2020).
57 15 U.S.C. § 45(n).
58 James C. Miller III, FTC Policy Statement on Deception (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf (accessed Apr. 10, 2020).
59 While Kyllo v. United States (2001) established that the use of thermal imaging technology from a public vantage point to monitor the radiation of heat from a person's home constituted a 'search' under the Fourth Amendment, and therefore required a warrant, there is no similar precedent for the use of thermal detection and/or multimodal thermal facial recognition technology as we describe here. See 533 U.S. 27 (2001); see also Christopher Slobogin, Peeping Techno-Toms and the Fourth Amendment: Seeing Through Kyllo's Rules Governing Technological Surveillance, 86 Minn. Law Rev. 1393 (2002) and Joel R. Reidenberg, Privacy in Public, 69 U. Miami L. Rev. 141 (2014), https://repository.law.miami.edu/umlr/vol69/iss1/6 (accessed Apr. 30, 2020).
60 William R Denny, CYBER CENTER: Cybersecurity as an Unfair Practice: FTC Enforcement under Section 5 of the FTC Act, Business Law Today (2016), https://www.americanbar.org/groups/business_law/publications/blt/2016/06/cyber_center_denny/ (accessed May 5, 2020).
61 402 F. Supp. 3d 767 (N.D. Cal. 2019).
specify privacy protections.\textsuperscript{62} However, within the last two decades,\textsuperscript{63} the FTC has also begun prosecuting ‘unfair’ practices, such as privacy practices that led to anticipatable cybersecurity attacks and consumer information breaches.\textsuperscript{64} Therefore, given the use of Section 5 to regulate how businesses collect and use other types of personal information, the FTC could foreseeably use this law to ensure that companies honestly represent their policies for the collection and use of thermal information to consumers and securely manage the thermal information collected from consumers.

Additionally, antidiscrimination statutes may offer another avenue to regulate the use of fever checks or facial recognition technologies. While the aforementioned changes in Equal Employment Opportunity Commission guidelines have allowed employers to test for COVID-19 outbreaks in their workplaces, the Americans with Disabilities Act still bars them from firing employees based on this information.\textsuperscript{65} Furthermore, studies have shown that facial recognition algorithms demonstrate algorithmic bias.\textsuperscript{66} Such bias against protected categories, such as race, sex, nationality, or religion, may be illegal in applications such as employment and housing.\textsuperscript{67} The Department of Housing and Urban Development has sued Facebook for allowing such discrimination.\textsuperscript{68} If fever detection systems are found to have bias against these protected categories, similar arguments may apply to restrict their use.

The public use of facial recognition technology also represents a new dimension to discussions about privacy under the Fourth Amendment. Historically, courts have ruled that individuals generally have no reasonable expectation of privacy once they have entered the public realm and that objects in plain view do not constitute a search under the Fourth Amendment. \textit{Katz v. U.S.} (1967) established that anything someone ‘seeks to preserve as private, even in an area accessible to the public’ is protected under the Fourth Amendment, implying that if someone purposefully attempts to conceal their face, it is not lawful to use thermal facial recognition to biometrically track them.\textsuperscript{69} While the Supreme Court suggested the lack of privacy interest to one’s face in \textit{U.S. v. Dionisio} (1973), legal scholars have argued that its response to privacy challenges presented by 21st century surveillance technologies may not uphold this expectation.\textsuperscript{70} In \textit{U.S. v. Jones} (2012), the Supreme Court reiterated that it had never ‘deviated from

---

\textsuperscript{62} Complaint before the Federal Trade Commission in the Matter of PayPal, Inc., a corporation, Commissioned by Maureen K. Ohlhausen and Terrell McSweeney (2017), https://www.ftc.gov/system/files/documents/cases/venmo_complaint.pdf (accessed Apr. 7, 2020).
\textsuperscript{63} Denny, supra note 63.
\textsuperscript{64} 799 F.3d 236 (3d Cir. 2015).
\textsuperscript{65} See 42 U.S.C. §§ 12111–12117, 12201–12213 and U.S. Equal Opportunity Employment Commission, Pandemic Preparedness in the Workplace and the Americans with Disabilities Act, (Mar. 21, 2020), https://www.eeoc.gov/laws/guidance/pandemic-preparedness-workplace-and-americans-disabilities-act (accessed Apr. 30, 2020).
\textsuperscript{66} National Institute of Standards and Technology, Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects (Dec. 2019), https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf (accessed Apr. 19, 2020); see also Buolamwini, Raji supra, note 25.
\textsuperscript{67} 42 U.S.C. §§ 2000, 3601.
\textsuperscript{68} Nat’l Fair Housing Alliance et al. v. Facebook, Inc., No. 18 Civ. 2689 (2018), Complaint (detailing allegations), https://nationalfairhousing.org/wp-content/uploads/2018/03/NFHA-v.-Facebook.-Complaint-w-Exhibits-March27-Final-pdf.pdf (accessed May 9, 2020).
\textsuperscript{69} 389 U.S. 347 (1967).
\textsuperscript{70} 410 U.S. 1, 14 (1972); see also Julian R Murphy, Chilling: The Constitutional Implications of Body-Worn Cameras and Facial Recognition Technology at Public Protests , 75 Wash. & Lee L. Rev. Online 1 (2018) and
the understanding that mere visual observation does not constitute a search. Merely 2 years later, in the Riley v California (2014) decision, the Court disagreed that the search of a smartphone upon arrest is ‘materially indistinguishable’ from the search of a pocket upon arrest. The Court further established in Carpenter v U.S. (2018) that the mass collection of public data through cell-site location information (CSLI) services had unique implications for individual liberty, saying that CSLI’s ‘depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection...does not make it any less deserving of Fourth Amendment protection.’ Guthrie Ferguson argues that although previous cases about society’s rights against surveillance have been rejected because they did not focus on singular defendants, Jones, Riley, and Carpenter all indicate that the pervasive nature of digital surveillance provides grounds for protection of everyone’s rights against novel surveillance.

Scholars have also suggested that mass surveillance creates First Amendment implications. Murphy and Kaminski discuss ways in which the kind of mass surveillance that facial recognition technology enables may impede rights to freedom of expression and association, and they discuss how taking these rights into account may bolster Fourth Amendment protections against such harms. Additionally, Skinner–Thompson proposes the notion of ‘performative privacy’—actions aimed at preserving one’s privacy in public spaces—as a kind of public privacy behavior that is protected under the First Amendment and doctrinally supported by existing jurisprudence. Such considerations are particularly important for individuals and communities who may be disproportionately surveilled by emerging technologies, including racial and sexual minorities.

At the federal level, access to recorded thermal detection information collected by commercial entities may also be subject to federal regulations under the Foreign Intelligence Surveillance Act (FISA). Section 501 of FISA allows the Federal Bureau of Investigation to seek a court order to acquire records, papers, documents, and other ‘tangible objects’ for individual investigations into suspected acts of international terrorism or clandestine intelligence by a US citizen. FISA can be applied to seek court

---

Rachel Levinson-Waldman, Hiding in Plain Sight: A Fourth Amendment Framework for Analyzing Government Surveillance in Public, 66 EMORY L.J. 527 (2017).

71 Clare Garvie et al., The Perpetual Line-up: Unregulated Police Face Recognition in America, Georgetown Law Center on Privacy & Technology (2016), https://www.perpetuallineup.org/sites/default/files/2016-12/The%20Perpetual%20Line-Up%20-%20Center%20on%20Privacy%20and%20Technology%20at%20Georgetown%20Law%20-%20121616.pdf (accessed Apr. 16, 2020), citing Riley v. California, 134 S. Ct. 2473, 2488 (2014).

72 Carpenter, 138 S. Ct. at 2217, cited in Andrew Guthrie Ferguson, Facial Recognition and the Fourth Amendment, 105 Minn. L. Rev., https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3473423 (accessed Apr. 30, 2020).

73 Andrew Guthrie Ferguson, Facial Recognition and the Fourth Amendment, 105 Minn. L. Rev. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3473423 (accessed Apr. 30, 2020).

74 See Murphy, supra note 73; Margot E. Kaminski, PRIVACY AND THE RIGHT TO RECORD 97 Boston U. Law Rev 1 (2017).

75 Scott Skinner-Thompson, Performative Privacy, 50 UC Davis L. Rev. 4 (2017) at 1677.

76 Id. at 1738.
orders for access to medical and health records—which may include thermal data if they appear within such records.\textsuperscript{77}

Furthermore, the current pandemic constitutes a public health emergency, requiring rapid action by state governments to prevent calamitous harm. As of March 27, all 50 states, dozens of localities, and the federal government have declared emergencies for COVID-19. During this time of emergency, strict adherence to ordinary legal standards can inadvertently limit, or even prohibit, necessary response efforts. To combat this risk, states have public health emergency laws that grant governors extraordinary power and flexibility to respond to emergency situations. These powers range from halting business operations and restricting freedom of movement to limiting civil liberties and commandeering property.\textsuperscript{78} In some states, public health emergency laws grant governors the broad authority to remove all legal barriers to an effective response to a declared emergency. Governors have exercised this power to relax hospital license rules to create alternative treatment centers, to expand healthcare providers’ scope of practice to allow paramedics to provide vaccinations, and more.\textsuperscript{79}

Additionally, most states’ public health emergency laws enable the governor to temporarily change statutes or regulations during a declared emergency. In total, 42 states explicitly permit the governor to change statutes or regulations during an emergency.\textsuperscript{80} In 35 states, governors are explicitly permitted to suspend or amend both statutes and regulations that interfere with an effective response to an emergency.\textsuperscript{81} States like North Carolina and New Hampshire specifically permit governors to create new statutes and regulations during emergencies.\textsuperscript{82} The substantial executive leeway granted by public health emergency laws has been effective in the past. For example, during the influenza epidemic of 2018, New York Governor Andrew Cuomo declared a public health emergency and suspended state statutes and regulations that normally prohibited pharmacists from vaccinating children.\textsuperscript{84} As a result, authorized pharmacists were able to vaccinate children—a demographic particularly susceptible to influenza.

Despite their benefits, it is still worth noting that there are no clear thresholds for terminating emergency powers under state public health emergency laws. For most states, emergency powers end automatically 30–90 days after a public health emergency was declared.\textsuperscript{85} However, the governor can renew the determination for additional time periods of 30–90 days, depending on the state.\textsuperscript{86} In Massachusetts and Washington,
there is no time limit; only the governor can terminate the emergency powers. As a result, these laws create the possibility that critical legal protections might be suspended indefinitely in response to the pandemic.

At the supranational level, the Organization for Economic Cooperation and Development (OECD) published recommendations in 2013 to guide its member countries in the collection and use of personal information, such as biometric information, through the OECD Privacy Framework. This framework advises member countries to develop comprehensive national privacy standards that set legal boundaries for the collection and use of personal information. The OECD has proposed several guidelines as a template for minimum standards for national policies but advises member countries to supplement such standards with a more thorough national privacy standard. The proposed guidelines encourage limitations on the collection and use of personal information, policies for openly informing individuals, maintenance of data quality, implementation of privacy management programs and security safeguards, and accountability. Despite membership in the OECD, the USA lacks a national privacy standard and therefore does not comply with these proposed guidelines.

**PROPOSED BIOMETRIC POLICY GUIDANCE FOR THERMAL FACIAL RECOGNITION AND BEYOND**

As we consider whether, when, and how to use multimodal biometric technology like thermal facial recognition to stem pandemic disease, there are a number of steps we can take to optimize its public health potential while limiting its impact on individuals’ privacy. The first step is to ask whether (i) thermal detection is an accurate and effective way of containing viral spread and (ii) if so, whether it is necessary to combine facial recognition technology with thermal detection devices. Depending on the answers, it may then be necessary to define clearly the purpose of biometric data collection and the specific use(s) to which they will be put and demonstrate how the technology design honors these parameters. By what standards will we measure the accuracy and effectiveness of such technologies to solve the problem at hand—that is, tracing contagion through a population in order to contain it? Will such data be used purely on a one-time basis to detect the presence of symptoms? Will the practice continue after the emergency has subsided, and how will we know when that is? If data will be stored, how will they be stored, by whom, and for how long?

As we consider such questions during the present pandemic, we can build upon existing recommendations to craft policies that will best marshal multimodal biometric technology for the context of contagion. To begin, designers of these emerging technologies should make clear to the public and to the agencies and companies deploying their technology how they have engineered devices to avoid harm to user privacy in the first place. Additionally, we can look to the Fair Information Practice Principles

---

87 Haffajee et al., supra note 88.
88 Organisation for Economic Co-operation and Development (OECD), The OECD Privacy Framework (2013), https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (accessed Apr. 11, 2020).
89 See Woodrow Hartzog & Neil M Richards, Privacy’s Constitutional Moment and the Limits of Data Protection, 61 Boston College Law Rev. (Forthcoming 2020), http://dx.doi.org/10.2139/ssrn.3441502 (accessed Apr. 30, 2020); Woodrow Hartzog, The Inadequate, Invaluable Fair Information Practices, 76 Md. L. Rev. 952 (2017) and Ari Ezra Waldman, Privacy Law’s False Promise 97 Wash. U. L. Rev. 2 (2020)
underlying the 1914 Fair Trade Commission Act and 1974 Privacy Act—principles that overlap significantly with the OECD fair information principles and European Union’s General Data Protection Regulation (GDPR) principles. These principles include making clear to individuals when and how facial recognition data are being collected, stored, and used; developing data management practices that consider how individuals are enrolled and what the risks, harms, and benefits may be to that (in)voluntary enrollment; specifying use limitations and third-party data sharing; safeguarding data and regularly evaluating the effectiveness of security measures; maintaining the accuracy and integrity of any stored data; and providing a process for accountability and problem resolution for individuals whose data are collected, stored, and/or used. Both approaches require greater transparency around technology design and use than currently exists, and we should act quickly to institutionalize such expectations before these technologies become entrenched in the post-pandemic world.

At present, as multimodal biometric technologies proliferate in the unusual regulatory space of this pandemic, it remains to be seen whether thermal detection is an accurate and effective way of containing viral spread and whether it is necessary to combine facial recognition technology with thermal detection devices. A recent report by the American Civil Liberties Union expressed the need for expert analysis of various temperature screening technologies and cautioned that those instruments deemed accurate must be deployed in a deliberate, equitable, and optional manner. This report warns that failing to do so could exacerbate existing inequalities by creating additional barriers to public transit and essential service access by requiring a kind of ‘public health theater’ predicated on the mistaken belief that mass temperature screenings in public places are an effective mechanism for containing viral spread. If independent scientific analysis establishes that one-time, remote thermal detection is indeed sufficient to assess the presence of febrile individuals in public spaces and that doing so may prove effective in identifying and removing infected individuals from public spaces, is it necessary to link such information to personal identifiers through facial recognition? What is the added utility of tracking an individual’s face if contact tracing is already in place?

If epidemiologists or public health officials determine that integrating facial recognition technology with thermal detection is essential to interrupting virus transmission, scientific testing should first assess the accuracy and effectiveness of each of its component functions (e.g., facial recognition, fever detection, infrared imaging) before deploying it broadly. Designers of such technologies should also demonstrate the degree to which they have engineered privacy safeguards into the design of the technology itself—for example, by limiting the types of data to be collected and stored and elaborating protections over data access. Further, companies collecting biometric data should be transparent about the duration in which they intend to collect sensitive

90 National Telecommunications and Information Administration. *Privacy Best Practices Recommendations for Commercial Facial Recognition Use* (2016), https://www.ntia.doc.gov/files/ntia/publications/privacy_best_practices_recommendations_for_commercial_use_of_facial_recognition.pdf (accessed Apr. 12, 2020).
91 Id.
92 ACLU, *Temperature Screening and Civil Liberties During an Epidemic* (May 19, 2020), https://www.aclu.org/sites/default/files/field_document/aclu_white_paper_-_temperature_checks.pdf (accessed May 20, 2020).
93 Id. at 6.
data (e.g., during an officially recognized pandemic, subsequent flu seasons, etc.). They should also offer recourse procedures for suspected false positives. Just as Article 16 of the GDPR provides a right to rectification, subjects of multimodal biometric collection should be assured that inaccurate or incomplete personal data will be expeditiously rectified and/or completed.\(^\text{94}\)

We also recommend that commercial establishments notify consumers when thermal recognition technology is in use. Entrances should provide signage in plain language that notifies individuals that biometric data are being collected, with specific indications of what will be stored and for how long the data will be retained. If the thermal recognition technology used by the establishment employs facial recognition or saves personally identifiable information beyond the point of collection and processing (to determine acceptable temperature levels), the establishment should highlight that on public signage and provide two modes to enter: passing through the facial recognition technology or undergoing a thermometer-based fever check. Choosing a thermometer-based fever check should not place an additional burden on the individual, as that will adversely impact the exercise of informed consent. Additionally, the aforementioned ACLU report recommends hygienic self-serve or voluntary temperature-checking facilities rather than mandatory checks on the basis that voluntary measures to combat disease are generally more effective than mandatory ones.\(^\text{95}\) They further stress that anyone whose screened temperature denies them access to ‘a critical service or function (such as applying for benefits or appearing in court)’ should be granted some other means of accessing that service or function.\(^\text{96}\)

For companies using thermal facial recognition technology to monitor employee health and attendance, employees should undergo a thorough informed consent process that outlines how long their biometric data will be stored and what policies are in place it is determined that they are beyond the threshold for a ‘safe’ working temperature. For example, will the employee have the opportunity to contest the measurement or be offered a thermometer-based fever check, will they be sent to a testing center, and/or will they be dismissed? Further, for companies using thermal facial recognition and/or thermal cameras alongside a contact tracing system, such as the Ramco technology discussed above, there should be data limitation measures in place to maximize the privacy of the individual. Notice of fever detection should not include personally identifying information.

Beyond consumer notifications, however, the protection of biometric data privacy demands that biotechnology companies practice transparency by focusing on ‘reasonable expectations of entrustees’ instead of passive disclosure of information.\(^\text{97}\) Ohm further calls for companies to be forthright by ‘anticipat(ing) what a consumer does not understand and volunteer(ing) that information’ in a non-biased way.\(^\text{98}\) Biotechnology companies developing and implementing thermal facial recognition technology can establish trust now through honest communication of the capabilities of the technology in a way that is accessible to all members of society.

---

\(^{94}\) GDPR Art. 16, https://gdpr.eu/article-16-right-to-rectification/ (accessed May 4, 2020).

\(^{95}\) Id. at 7–8.

\(^{96}\) Id. at 7.

\(^{97}\) Id.

\(^{98}\) Paul Ohm, Forthright Code, 56 HOUS. L. REV. 471, 472–73 (2018).
Additionally, to halt mission creep, we recommend against passive, continuous monitoring of individuals’ temperature over time. If thermal recognition technology continues to be integrated with other multimodal biometric technologies, such as smartphone-linked wearables that collect and share protected health information with government agencies, commercial sites, and/or employers, stringent data protections must be in place. Particularly as the notion of immunity certificates suggests the ability to reopen the post-COVID-19 world, we need to consider seriously which biometric data are essential and effective for preserving health, how they will be used and stored in and beyond the pandemic, and what we can do to ensure adequate safeguards are in place.99

Despite evidence that thermal imaging technology is at present insufficiently sophisticated to combat the spread of SARS–CoV-2 (or any similar virus), governments and firms around the world are widely embracing it as part of a multimodal biometric surveillance strategy to curb the pandemic. We should not wait until the chaos of the present moment subsides to adjudicate the effectiveness of technologies that will have major privacy implications once they become entrenched. It is precisely at this moment, when the technologies are emerging and quickly evolving, we should anticipate these privacy concerns and demand transparency and accountability. We should be aware that governments and corporations may use these nascent technologies to collect temperature and other biometric data alongside other personal identifiers like names, passports, and/or social security numbers. Now is the time to design technologies with privacy in mind alongside institutionalizing multipronged, proactive oversight, and redress mechanisms for the future.

As governments in the USA and abroad begin to haltingly reopen societies under intensifying economic and public pressure, the demand for reliable symptom detection and contact tracing systems will continue to increase. Both the public and private sectors have reacted quickly to these needs, undertaking partnerships and technological collaborations to curb the spread of COVID-19. In a climate driven by such urgency, relatively unproven technologies like thermal facial recognition will continue to proliferate rapidly, deeply entrenching themselves in society. Without a high standard of independent technical validation, holistic comparison of risks and benefits, and proactive policy enactment, many of the changes to how our biological information is collected, stored, and analyzed may be irreversible.

ACKNOWLEDGMENTS

We are grateful to the Duke University Bass Connections program for guidance and funding. Dr. Van Natta also receives funding from the National Human Genome Research Institute (7R01HG009923-02).

99 Lydia Smith, GERMANY TO INTRODUCE CORONAVIRUS ‘IMMUNITY CERTIFICATES’ FOR RECOVERED PUBLIC, Newsweek (Mar. 30, 2020), https://www.newsweek.com/germany-antibodies-tests-generic-public-immunity-certificates-1494934 (accessed Apr. 18, 2020); see also Henry T. Greely, COVID-19 Immunity Certificates: Science, Ethics, Policy, and Law, J. Law Biosci. (2020), https://academic.oup.com/jlb/advance-article/doi/10.1093/jlb/lsaa035/5848136?searchresult=1 (accessed May 8, 2020).