ORIGINAL ARTICLE

Physician perceptions of surveillance: Wearables, Apps, and Chatbots for COVID-19

Alexandra R. Linares[1]*, Katrina A. Bramstedt[2], Mohan M. Chilukuri[3], P. Murali Doraiswamy[1]

[1]*Department of Psychiatry and Behavioral Sciences, Duke University School of Medicine, Durham, USA*
[2]*Department of Medicine, Bond University Medical Program, Queensland, Australia*
[3]*Department of Family Medicine, University of North Carolina School of Medicine, Chapel Hill, USA*

ABSTRACT

Background and Purpose: To characterize the global physician community's opinions on the use of digital tools for COVID-19 public health surveillance and self-surveillance. **Materials and Methods:** Cross-sectional, random, stratified survey done on Sermo, a physician networking platform, between September 9 and 15, 2020. We aimed to sample 1000 physicians divided among the USA, EU, and rest of the world. The survey questioned physicians on the risk-benefit ratio of digital tools, as well as matters of data privacy and trust. **Statistical Analysis Used:** Descriptive statistics examined physicians' characteristics and opinions by age group, gender, frontline status, and geographic region. ANOVA, *t*-test, and Chi-square tests with $P < 0.05$ were viewed as qualitatively different. As this was an exploratory study, we did not adjust for small cell sizes or multiplicity. We used JMP Pro 15 (SAS), as well as Protobi. **Results:** The survey was completed by 1004 physicians with a mean (standard deviation) age of 49.14 (12) years. Enthusiasm was highest for self-monitoring smartwatches (66%) and contact tracing apps (66%) and slightly lower (48–56%) for other tools. Trust was highest for health providers (68%) and lowest for technology companies (30%). Most respondents (69.8%) felt that loosening privacy standards to fight the pandemic would lead to misuse of privacy in the future. **Conclusion:** The survey provides foundational insights into how physicians think of surveillance.

Keywords: Apps, Privacy, Surveillance, Trust, Wearables

INTRODUCTION

Public health surveillance is the systematic collection and analysis of health-related data to prevent or control disease, followed by its application for public health action.[1] The global scale of the COVID-19 pandemic has accelerated the use of non-traditional, technology-based, public health, and self-surveillance mechanisms to control the spread of severe acute respiratory syndrome coronavirus 2 (SARS-CoV-2).[2-23] Examples of such tools include contact-tracing apps, analyses of global positioning systems and social media data for population movement tracking, fever-sensing infrared thermal detection systems, symptom self-screeners (e.g. chatbots), and smartwatch applications to detect physiological signs of infection.[4-8,10]

Digital technologies can rapidly collect, store, analyze, and share numerically encoded information, making them potentially highly useful in a pandemic such as COVID-19. Blue Dot, a Canadian digital health company, reportedly identified the emergence of COVID-19 through the aggregation of big data from sources such as social media and air travel, before even the WHO issued an alert.[14]

***Address for correspondence:**
Ms. Alexandra R. Linares
Department of Psychiatry and Behavioral Sciences, Duke University School of Medicine, DUMC Box: 3018, Durham, NC 27710, USA.
E-mail: alexandra.linares@duke.edu

Access this article online

Quick Response Code

Website: www.digitmedicine.com

DOI: 10.4103/digm.digm_28_21

How to cite this article: Linares AR, Bramstedt KA, Chilukuri MM, Doraiswamy PM. Physician perceptions of surveillance: Wearables, Apps, and Chatbots for COVID-19. Digit Med 2022;8:10.

Submitted: 09-Jun-2021 **Revised:** 02-Jun-2021
Accepted: 28-Jul-2021 **Published:** 12-May-2022

However, these digital surveillance tools are experimental, and their accuracy across different settings is not fully established.[15-20] For example, studies have shown that the accuracy of facial recognition technologies differs by race, gender, and age.[22] These tools also come with a number of potential legal and ethical risks,[18,24-28] such as privacy concerns, discrimination, and over-reach of the data mission that "highlight the long-standing tensions between individual and collective rights."[18]

Notably, the morbidity and mortality of the COVID-19 pandemic have heightened worldwide anxiety to an extent that digital public health surveillance has become ubiquitous (e.g. national requirements for downloading contact tracing apps; thermal scanning by employers and private businesses; personal location data collection via QR codes; texting of COVID-19 assay results to patients). COVID-19 is not the world's first pandemic, nor will it be the last. Thus, it is vital to understand the views of physicians, as they are involved in many facets of health data and its application to COVID-19 care. The aim of this report is to characterize the views of physicians regarding the benefits and risks of surveillance technologies.

MATERIALS AND METHODS

Ethics

This study was deemed as exempt research by Duke University Medical Center's Institutional Review Board.

Study sample

To characterize the opinions of physicians on this topic, we analyzed data from a cross-sectional, random, stratified survey of physicians registered with Sermo, a secure digital platform for medical crowdsourcing and anonymous surveys. The Sermo platform is exclusive to verified and licensed physicians and has over 800,000 registered physicians, of all specialties, worldwide.

Following informed consent, the English-language survey sampled physicians between September 9 and September 15, 2020 (before initiation of SARS-CoV-2 vaccination), with a target sample size of 1000 doctors equally divided between the US, EU, and rest of the world (RoW). The survey results were de-identified to create anonymized data for analysis.

Survey instrument

Five questions in the survey [Figure 1 and Supplemental Table 1] asked physicians their opinions on the benefits and risks/harms of using smartwatch sensor alerts, contact tracing apps, thermal cameras for mass fever screening, chatbots, and social media tracking for public

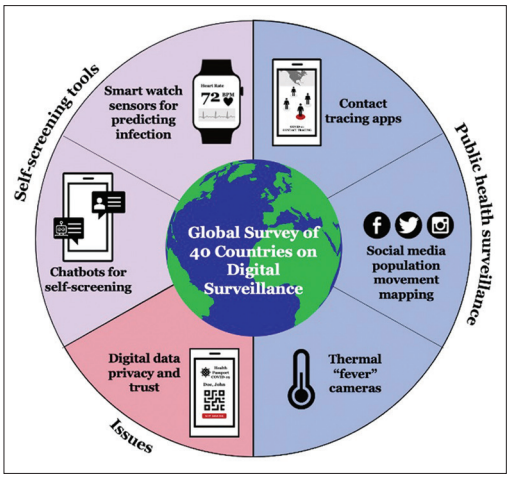

Figure 1 Schematic illustration of surveillance tools and issues queried in the survey. The survey examined the risk-benefit ratio of two self-screening (purple) and three public health (blue) surveillance digital tools. It also addressed issues around trust and misuse (red).

health or self-surveillance. These questions focused on the risk-benefit ratio, and the answer options were "Yes" "No" and "Uncertain" For the questions on sensors (wearables and thermal cameras), we provided accuracy estimates derived from published studies. We specified that informational chatbots do not require regulatory approval in most countries for the question on chatbots, as physicians may not be aware of this. The survey then asked about the level of trust in different organizations (technology companies, government, employer, medical providers, educational universities/nonprofit bodies, or no one) to protect private surveillance data. The answer choices for this question were "Very much" "Somewhat" "Neutral" "Not really" or "Not at all" Respondents were then asked about the impact of current surveillance on future privacy standards. A final question asked physicians to provide brief qualitative comments to elaborate on their views. The results of two survey questions are reported elsewhere.[29,30]

Data and statistical methods

Descriptive statistics examined physicians' characteristics and opinions by age group, gender, frontline status, and geographic region. To test the effect of age, subjects were grouped as "younger" or "older" by age 49 years. To test the effect of frontline status, physicians more directly involved in COVID-19 care were grouped as frontline (e.g. internal medicine, ICU, ED), whereas the rest were categorized as non-frontline (although we recognize that all physicians may interact with or consult on COVID-19 patients). For geographic analyses, we pooled doctors into three groups based on the location of practice (US, European Union, RoW),

Table 1: Physician perceptions of surveillance tools

Surveillance tool	Benefits outweigh risks (%)	Risks outweigh benefits (%)	Unknown (%)	χ^2, *P*
Smart watches for infection detection	65.5	17.3	17.1	468.58, <0.0001
Contact tracing apps	66.4	15.0	18.5	496.85, <0.0001
Infrared thermal "fever cameras"	58.9	25.0	16.1	306.34, <0.0001
Symptom screener chatbots	47.6	26.6	25.8	92.18, <0.0001
Social media for population movement tracking	50.9	27.8	21.3	145.68, <0.0001

while recognizing these subgroups are not homogeneous. The five categories relating to trust were combined into three categories as trusted ("Somewhat" or "Very much" responses), not trusted ("Not really" or "Not at all"), and "Neutral". Gender analyses were restricted to those who categorized themselves as male or female. ANOVA, *t*-test, and Chi-square tests with $P < 0.05$ were viewed as qualitatively different. As this was an exploratory study, we did not adjust for small cell sizes or multiplicity. We used JMP Pro 15 (SAS), as well as Protobi.

RESULTS

Sample characteristics

The final respondent sample consisted of 1004 physicians representing 40 countries in North and South America, Europe, and Asia-Pacific [Supplemental Table 2]. The average age of the sample was 49.1 ± 12.3 years and 49% of respondent physicians were characterized as frontline. Of the sample, 40% were male, 20.6% were female, and 39% opted out of indicating their gender.

Utility of surveillance tools

Response rates for the support of various digital surveillance tools are shown in Figure 2 and Table 1. Smart watches were supported by 65.5% of respondents ($\chi^2 = 468.58$, $P < 0.0001$), contact tracing apps were supported by 66.4% ($\chi^2 = 496.85$, $P < 0.0001$), fever cameras were supported by 58.9% ($\chi^2 = 306.34$, $P < 0.0001$), symptom screener chatbots by 47.6% ($\chi^2 = 92.18$, $P < 0.0001$), and social media by 50.9% ($\chi^2 = 145.68$, $P < 0.0001$).

Age differences

Younger physicians (69.3%) were more likely to support the use of smart watch sensors compared with older physicians (61.3%) ($\chi^2 = 7.06$, $P = 0.03$). Younger physicians (69.7%) were marginally more likely to support the use of contact tracing apps compared to older physicians (62.8%) ($P = 0.02$). Younger physicians (63.6%) were more likely to support the use of mass fever screenings compared with older physicians (53.6%) ($\chi^2 = 11.62$, $P = 0.003$), whereas older physicians were more likely to be uncertain. Younger physicians (56.1%) were more likely to support the use of social media for population movement tracking versus older physicians (45.2%) ($\chi^2 = 14.34$, $P = 0.0007$), and older physicians tended to be more uncertain. Responses did not significantly differ by physician age for the utility of symptom screener chatbots.

Gender differences

Male physicians (60%) were slightly more likely to support the use of fever cameras than female physicians (51%) ($P = 0.012$). Responses did not differ by gender for the other surveillance tools.

Frontline status differences

Responses did not differ by frontline status.

Which entity do you trust the most with your personal surveillance data?

Physicians picked "medical providers" as the most trusted entity to protect the privacy of COVID-19 surveillance data, with about 68% of respondents reporting that they trusted their medical provider [Figure 3]. The second most trusted group was "educational/non-profit bodies" with a combined 52% of respondents reporting "somewhat" and "very much" levels of trust. Conversely, the most distrusted group was "technology companies" with only 30% of respondents reporting "somewhat" or "very much" and 46% reporting "not really" or "not at all". Following technology companies, respondents reported low levels of trust for the "government" with only 36% responding "somewhat" or "very much" Older physicians were more likely to be distrustful of technology companies (48.9%), the government (44.5%), and educational universities/non-profit bodies (26.9%) compared with younger physicians (42.4%, 33.9%, 16.9%, respectively) ($P = 0.038$, 0.001, <0.001). US physicians (54.1%) were more likely to be distrustful of technology companies, compared with both EU (41.0%) and RoW (41.3%) physicians ($P < 0.001$). US physicians (51.8%) were also more distrustful of the government, compared with RoW (38.6%) and EU (27.5%) physicians ($P < 0.001$).

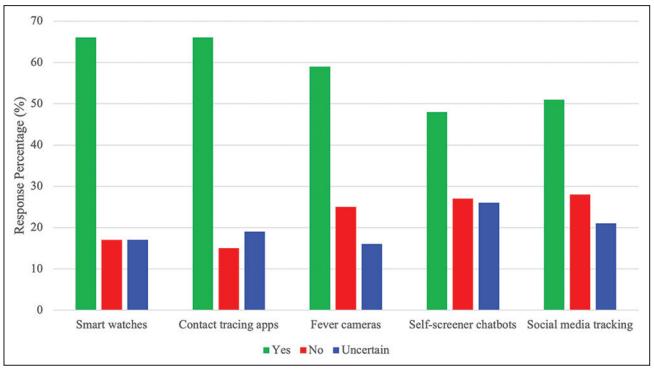

Figure 2 Physician perceptions of digital surveillance tools relevant to COVID-19. Graph illustrates percent of respondents who were supportive (green bars), uncertain (blue bars) or unsupportive of the use of surveillance tools. Please see text for statistical differences.

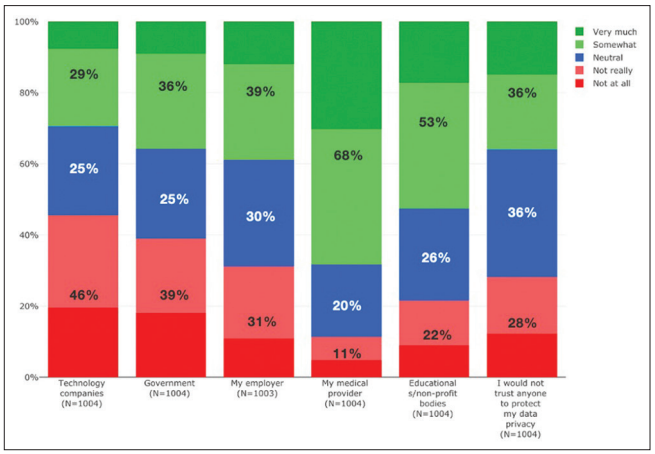

Figure 3 Physicians perceptions of trust in various entities to protect their personal data. Colors show the percentages reported for the 5 trust level categories. The percentages reported inside the bars combine "Somewhat"/"Very much" and "Not really"/"Not at all" categories.

Effect of current surveillance on future misuse of privacy

The majority of respondents (69.8%) believed that potentially loosening privacy standards to fight the pandemic would lead to misuse of privacy in future (χ^2 = 601.50, $P < 0.0001$) [Figure 4]. Frontline physicians (73.2%) were more likely to voice concern compared with nonfrontline physicians (66.5%) ($\chi^2 = 7.65$ $P = 0.022$). More male physicians (71.9%) believed that a loosening of privacy standards would lead to misuse, compared with female physicians (61.8%) (χ^2 = 9.58 $P = 0.048$).

Selected qualitative comments by physicians about digital surveillance

Respondents also had an option to provide qualitative comments on digital surveillance. Supportive comments [Supplemental Table 3] included statements such as "*the Future is here,*" "*must be made mandatory,*" "*anything that prevents deaths is fine, I don't worry about privacy,*" and "*During the 1940–1941 bombing of London called The Blitz, I believe there were zero residents of London who said 'I have a constitutional right to leave my lights on a night if I feel like it.*'" Concerns about efficacy [Supplemental Table 4] included statements like "*way too early,*" "*bad for patient and physician,*" and "*data should be analyzed in clinical trials.*" Concerns about harms [Supplemental Table 5] included statements such as "*Pandora's box,*" "*creepy, extreme slippery slope,*" "*any great idea can have unforeseen* consequences" and "*I fear the behavior of people not technologies.*"

DISCUSSION

Data is currency. Technology companies know this, governments know this, and so does the public. Like with any currency, data can be accumulated, bought and sold, or even be stolen. Hence, its storage needs to be secure. Health data are a form of personal information that generally people want to keep private, and many regulations have been implemented to safeguard personal data privacy rights.[31,32] During a pandemic, public health interests allow for broader powers, governments, and health systems to collect, use, store, and share personal information. However, as our survey shows, this creates concern among even the physicians who are part of this process (and concurrently attempting to prevent and treat the implicated illness).

Key findings

Overall, support varied from 48% to 66% for the various surveillance tools. Two-thirds of physicians voiced support for the use of smartwatches in self-monitoring. This appears consistent with recent studies documenting the promise of consumer smart watch-based physiological signals (e.g. heart rate, sleep, activity, skin temperature) for discriminating COVID-19 test positive cases from negative cases, as well as for detecting pre-symptomatic COVID-19 infection.[4,5] Further, a smartwatch-linked platform, Aura, recently received an EU CE mark for this purpose based on its sensitivity of 94% and ability to detect an infection signal on average 2.64 days after inoculation.[6] The minority of respondents who oppose smart watch-based infection detection technology were likely concerned about the potential for noisy data leading to misdiagnosis and unnecessary testing.[19]

Two-thirds of physicians also voiced support for contact tracing apps, even those that collected personal data. Many countries have implemented contact tracing apps, and physicians are well versed in traditional contact

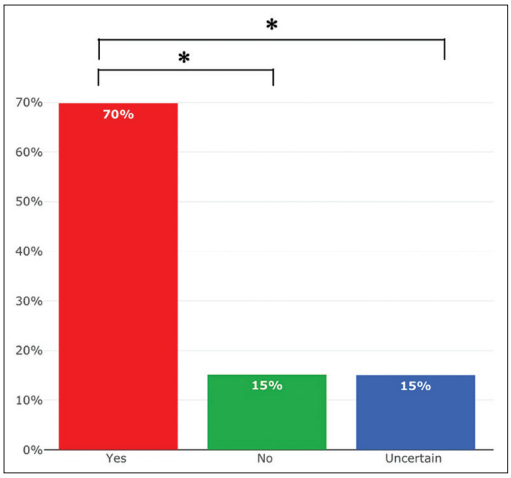

Figure 4 Physician perceptions of the risk for future misuse of data. Red illustrates the percent who agreed that loosening privacy laws would result in misuse. Green represents those who disagreed. Blue represents those who were uncertain. (*$P < 0.05$)

tracing principles for infection control, both of which likely increased physician confidence in their utility. However, since our survey, some studies have questioned the effectiveness (e.g. sensitivity of only 7% in one study) and ethics of digital contact tracing.[20-22] This suggests that the optimism of respondents in our survey may have been premature.

Physician support was slightly lower (59%) for "fever cameras" but still optimistic, consistent with the utility for mass screening offered by their high negative predictive value,[8] However, the positive predictive value (<20% in one study) of these systems remains low,[8,9] suggesting the need for further optimization to reduce false positives.

Support for the use of social media tracking (51%) and chatbots (48%) was also slightly lower. Social media tracking is a promising tool that offers real-time data for public health officials to monitor citizen movement or social interactions during lockdowns.[10-13] However, questions remain about lack of consent, accuracy, and misuse potential. Chatbots, especially those designed using WHO or CDC guidelines, very likely helped large numbers of users (over 200 million messages by some estimates) quickly get reliable information. However, to our knowledge, there are no published accuracy or outcomes data on the utility of chatbots for pandemic self-screening. Hence, there is a need for further research into the effectiveness and potential for the spread of misinformation.[20,21]

Respondents in our survey also voiced concerns over privacy risks and over-reach of the data mission. Respondents had low trust in technology companies (30%) and governments (36%) to safeguard surveillance data. Trust was highest with medical providers (68%), followed by non-profit organizations. The higher level of trust among EU physicians may be due to the stricter data privacy laws in the EU versus the US.[31] These concerns are legitimate since some technology platforms rely on selling user data to advertisers,[27] and studies have found apps and chatbots share information with a variety of third parties.[20,27-29] The risks also go beyond privacy breaches.[27] Historically, surveillance has worsened stigmatization and discrimination against racial or religious minorities who were often falsely blamed for disease outbreaks.[27] Further, some governments have reportedly used the pandemic to rank citizens by health status or analyze personal telecommunications traffic.[27] Hence, surveillance done wrong may "invite mission creep into adjacent fields, such as automated policing and content control."[24]

"No turning back" is a famous quote used in many settings, and our research makes it pertinent to digital health as well. The fast portability of health data, along with the complexity of legal regulations and voluminous "Terms of Use" documents that are rarely read by users,[30] create a reality of data that has the potential to quickly bounce to all corners of the world. In addition, there is the very real presence of hackers.[31] Therefore, some of the data receivers have motives that have nothing to do with "public interest" Accordingly, the fears and lack of trust we observed are likely well-founded and highlight the need for risk mitigation to harness the full promise of public health surveillance during a pandemic.

Strengths and limitations

This is the first global survey, to our knowledge, to investigate the opinions of physicians about the utility, trust, and risks of commonly used public health digital surveillance tools. Our survey data is from a relatively large and diverse sample of verified practicing physicians. Potential limitations include cross-sectional design, the limited number of respondents from developing countries, inability to control for all possible confounding variables (e.g. personal medical history, socio-political beliefs, local data privacy regulations, knowledge about digital tools), and inability to deduce causality. Further, physician perceptions may change over time if infection risk and prevalence decrease, due to vaccination and herd immunity. Our findings should be interpreted within this context. Nevertheless, they provide a useful baseline for future surveys.

Interpretation and implications

Physicians were optimistic but not equally supportive of all surveillance tools suggesting the need for further research on effectiveness. There was also variation in physician opinions by age group. This may in part reflect differences in physician knowledge about emerging technologies and/or risk-benefit analyses, which would benefit from further education. The low level of trust in technology companies to protect personal data suggests that independent entities (governed by stricter privacy laws) should be the gatekeepers of such data. Current regulations fall short of addressing the risks posed by these new technological developments. It has been said that "data moves at the speed of trust." During public health emergencies, any data collection through such newer tools should be both time-limited and scope-limited, with decisions made in a transparent way before the launch of surveillance activity.[22,27] In parallel, we may need to strengthen other data privacy rules to ensure any temporary loosening during public health emergencies does not result in future misuse in normal times. We hope that insights from surveys such as this may spur public health agencies and technology innovators to work together to develop the evidence base and balance individual versus societal versus commercial needs.[24] As aptly noted by one of the survey respondents, "we can learn from films like Spiderman and The Dark Knight – with great power comes great responsibility."

Financial support and sponsorship

Sermo provided non-financial technical platform support for the study.

Conflicts of interest

PMD has received research grants and/or advisory/board fees from health and technology companies. PMD owns shares in companies and is a co-inventor on patents. MMC reported personal fees outside the submitted work. KB has received consulting fees outside of the submitted work. ARL has no conflicts of interest to report.

REFERENCES

1. Lee LM, Thacker SB. Public health surveillance and knowing about health in the context of growing sources of health data. Am J Prev Med 2011;41:636-40.
2. Gunasekeran DV, Tham YC, Ting DS, Tan GS, Wong TY. Digital health during COVID-19: Lessons from operationalising new models of care in ophthalmology. Lancet Digit Health 2021;3:e124-34.
3. Murray CJ, Alamro NM, Hwang H, Lee U. Digital public health and COVID-19. Lancet Public Health 2020;5:e469-70.
4. Mishra T, Wang M, Metwally AA, Bogu GK, Brooks AW, Bahmani A, *et al*. Pre-symptomatic detection of COVID-19 from smartwatch data. Nat Biomed Eng 2020;4:1208-20.
5. Quer G, Radin JM, Gadaleta M, Baca-Motes K, Ariniello L, Ramos E, *et al*. Wearable sensor data and self-reported symptoms for COVID-19 detection. Nat Med 2021;27:73-7.
6. Empatica. Aura Receives First of Its Kind European CE Mark for Early Detection of COVID-19 Empatica; 2021. Available from: https://www.empatica.com/blog/aura-and-care-receive-ce-mark-for-early-detection-of-covid-19-and-other-respiratory-infections.html. [Last accessed on 2021 Jun 04].
7. Huang Z, Guo H, Lee YM, Ho EC, Ang H, Chow A. Performance of digital contact tracing tools for COVID-19 response in Singapore: Cross-sectional study. JMIR Mhealth Uhealth 2020;8:e23148.
8. Nguyen AV, Cohen NJ, Lipman H, Brown CM, Molinari NA, Jackson WL, *et al*. Comparison of 3 infrared thermal detection systems and self-report for mass fever screening. Emerg Infect Dis 2010;16:1710-7.
9. Martinez-Jimenez MA, Loza-Gonzalez VM, Kolosovas-Machuca ES, Yanes-Lane ME, Ramirez-GarciaLuna AS, Ramirez-GarciaLuna JL. Diagnostic accuracy of infrared thermal imaging for detecting COVID-19 infection in minimally symptomatic patients. Eur J Clin Invest 2021;51:e13474.
10. Our Work on COVID-19; 2021. Available from: https://dataforgood.fb.com/docs/covid19/. [Last accessed on 2021 Jun 07].
11. Beria P, Lunkar V. Presence and mobility of the population during the first wave of Covid-19 outbreak and lockdown in Italy. Sustain Cities Soc 2021;65:102616.
12. Pérez-Arnal R, Conesa D, Alvarez-Napagao S, Suzumura T, Català M, Alvarez-Lacalle E, *et al*. Comparative analysis of geolocation information through mobile-devices under different COVID-19 mobility restriction patterns in Spain. ISPRS Int J Geo Inf 2021;10:73.
13. Morinishi L, Barkume K, Kim E, Reinhart A. Home for the Holidays? The Impact of US Holidays on Social Behaviors and Preventative Measures. Delphi Group; 2021. Available from: https://delphi.cmu.edu/blog/2021/02/02/home-for-the-holidays-the-impact-of-us-holidays-on-social-behaviors-and-preventative-measures/. [Last accessed on 2021 Jun 7].
14. Stieg C. How this Canadian Start-Up Spotted Coronavirus before Everyone Else Knew About It; 2020. Available from: https://www.cnbc.com/2020/03/03/bluedot-used-artificial-intelligence-to-predict-coronavirus-spread.html. [Last accessed on 2021 Jun 04].
15. Sweeney Y. Tracking the debate on COVID-19 surveillance tools. Nat Mach Intell 2020;2:301-4.
16. Mbunge E. Integrating emerging technologies into COVID-19 contact tracing: Opportunities, challenges and pitfalls. Diabetes Metab Syndr 2020;14:1631-6.
17. Colizza V, Grill E, Mikolajczyk R, Cattuto C, Kucharski A, Riley S, *et al*. Time to evaluate COVID-19 contact-tracing apps. Nat Med 2021;27:361-2.
18. Sekalala S, Dagron S, Forman L, Meier BM. Analyzing the Human Rights Impact of Increased Digital Public Health Surveillance during the COVID-19 Crisis. Health Hum Rights 2020;22:7-20.
19. Zhu T, Watkinson P, Clifton DA. Smartwatch data help detect COVID-19. Nat Biomed Eng 2020;4:1125-7.
20. Miner AS, Laranjo L, Kocaballi AB. Chatbots in the fight against the COVID-19 pandemic. NPJ Digit Med 2020;3:65.
21. Fan X, Chao D, Zhang Z, Wang D, Li X, Tian F. Utilization of self-diagnosis health chatbots in real-world settings: Case study. J Med Internet Res 2021;23:e19928.
22. Zimmermann BM, Fiske A, Prainsack B, Hangel N, McLennan S, Buyx A. Early perceptions of COVID-19 contact tracing apps in German-speaking countries: Comparative mixed methods study. J Med Internet Res 2021;23:e25525.
23. Grother P, Ngan M, Hanaoka K. Face Recognition Vendor Test (FRVT): Part 3: Demographic Effects. Gaithersburg, MD: USDo Commerce, National Institute of Standards and Technology; 2019.
24. Cohen J, Hartzog W, Moy L. The Dangers of Tech-Driven Solutions

to COVID-19; 2020. Available from: https://www.brookings.edu/techstream/the-dangers-of-tech-driven-solutions-to-covid-19/. [Last accessed on 2021 Jun 07].

25. Valade P. Jumbo Privacy Review: North Dakota's Contact Tracing App; 2020. Available from: https://blog.jumboprivacy.com/jumbo-privacy-review-north-dakota-s-contact-tracing-app.html. [Last accessed on 2021 Jun 07].
26. Mozur P, Zhong R, Krolik A. In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags. The New York Times; 2020. Available from: https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html. [Last accessed on 2021 Jun 07].
27. Global Mobile Consumer Survey: US Edition; 2017. Available from: https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-tmt-2017-global-mobile-consumer-survey-executive-summary.pdf. [Last accessed on 2021 Jun 04].
28. Koppel R, Kuziemsky C. Healthcare data are remarkably vulnerable to hacking: Connected healthcare delivery increases the risks. Stud Health Technol Inform 2019;257:218-22.
29. Doraiswamy PM, Chilukuri MM, Linares AR, Bramstedt KA. Are we ready for COVID-19's golden passport? Insights from a global physician survey. J Health Soc Sci 2021;6:079-86.
30. Doraiswamy PM, Chilukuri MM, Ariely D, Linares AR. Physician perceptions of catching COVID-19: Insights from a global survey. J Gen Intern Med 2021;36:1832-4.
31. EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.
32. The Health Insurance Portability and Accountability Act (HIPAA). Washington, D.C.: U.S. Dept. of Labor, Employee Benefits Security Administration. US 1996.

Supplemental Table 1 Survey questions reported in the study.

Question 1: Contact tracing apps on smart phones are being promoted by governments to monitor and curb the spread of COVID-19. Such apps use your personal identity and cell phone GPS signals to track your movements, the places you visited and who you have been in contact with for the past 2 weeks. Do you believe that the possible benefits to the public of COVID-19 contact tracing apps will outweigh the possible risks/harms?
Options: Yes/no/uncertain.
Question 2: Smart watches and wearables may soon be able to predict if a person has an infection before they can self-recognize it (presymptomatic stage) based on changes in temperature, heart rate, respiration and sleep. If 15% of the population have an infection, a device that is 90% accurate will have a 96% NPV and a 60% PPV. Do you believe that the possible benefits of such an infection detection alert will outweigh the possible risks/harms?
Options: Yes/no/uncertain.
Question 3: "Fever cameras" (infrared temperature detection systems) are being used for mass screening of the public for fever (e.g., at airports, schools). Current research suggests that such systems have 85% accuracy, a 99% NPV and a 15% PPV for detecting true fever. Do you believe that the possible benefits of such a mass fever screening system will outweigh the possible risks/harms?
Options: Yes/no/uncertain.
Question 4: Chatbots were used by large numbers of people during COVID-19 to screen themselves for symptoms and determine the need for further evaluation. In most countries, such chatbots do not need prior regulatory approval. Do the possible benefits of such COVID-19 symptom screening chatbots outweigh the possible risks/harms?
Options: Yes/no/uncertain.
Question 5: Social media postings (e.g., on Facebook) are being aggregated to create "COVID-19 symptom maps" and population movement maps. Anonymized maps are being shared with public health officials and researchers. Do the possible benefits of such social media tracking outweigh the possible risks/harms?
Options: Yes/no/uncertain
Question 6: If COVID-19 surveillance technologies were offered, how much would you trust the following groups to protect your privacy? (choose one)
Options: Technology companies; Government; my employer; my medical provider; educational universities/nonprofit bodies; I would not trust anyone to protect my data privacy
Question 7: If privacy standards are loosened to fight the pandemic, do you believe that in the future this will also lead to misuse of privacy in other areas of personal life?
Options: Yes/no/uncertain.

GPS: Global positioning system, PPV: Positive predictive value, NPV: Negative predictive value

Supplemental Table 2 Country where the respondent physician practices (*n*=1004)*.

Country	*n* (%)
United States	340 (33.9)
Italy	116 (11.6)
Spain	83 (8.3)
United Kingdom	53 (5.3)
Germany	47 (4.7)
Mexico	44 (4.4)
France	40 (4.0)
Russia	36 (3.6)
Canada	33 (3.3)
Brazil	30 (3.0)
Venezuela	30 (3.0)
India	27 (2.7)
China	18 (1.8)
Australia	17 (1.7)
Turkey	14 (1.4)
Japan	12 (1.2)
Portugal	9 (0.9)
South Korea	7 (0.7)
South Africa	7 (0.7)
Poland	6 (0.6)
Belgium	5 (0.5)
Greece	5 (0.5)
Argentina	3 (0.3)

*Two respondents (0.2%) each from the Philippines, Switzerland, Austria, Colombia, and Sweden are not shown in the Table. One respondent (0.1%) each from Malaysia, the Netherlands, Honduras, Jordan, New Zealand, Ukraine, Czech Republic, Kazakhstan, United Arab Emirates, Hungary, Saudi Arabia, and Nigeria are also not shown in the table.

Supplemental Table 3 Selected comments supportive of digital surveillance tools.

During the 1940-41 bombing of London called The Blitz, I believe there were zero residents of London who said "I have a constitutional right to leave my lights on a night if I feel like it".
Generally speaking, I favor almost all methods for identification, contact tracing, and isolation.
I believe it will become a necessity in order to flatten the curve and prevent rampant infections.
They are helpful for healthy travelers and commuters.
Using the phone to warn possible exposure would be helpful when you are in area outside your routine or interact with many people.
The future is here.
I believe that in the future digital surveillance technology will be indispensable.
I believe that a full-fledged record of contact and sick people with their timely isolation is the best way to localize foci. And using digital tracking technologies to do this is a good way to make this function complete.
Digital surveillance technologies will play an increasingly important role in current and future pandemics.
Anything that prevents deaths is fine with me. I don't worry about privacy.
There is already extensive digital surveillance and data sharing for law enforcement and mercantile purposes, so why not harness it for the public health.
It works! We have seen it work in other countries.
Using it to map areas of high activity makes sense (home address, not the location the positive test occurred).
The unstoppable future. It must be mandatory, not optional.

Supplemental Table 4 Selected comments about efficacy gaps with surveillance tools.

Digital surveillance is not ready for prime time. Too much risk for: abuse, false results causing more confusion. Would favor if the PPV and NPV were=95%.
We do not know enough about the virus, and technologies are not enough reliable.
Way too early. Data should be accumulated and analyzed in context of controlled trials by reputable scientists.
I fear the behavior of some people, not the technologies. Need deep cultural change for compliance.
The bad will eventually outweigh the initial good. There must be an ending period established before it is employed.
Bad for patient and physician; useless. It is not medicine.
It's not the acquisition of the data that concerns me, but more those who collect and analyze.
None of them can perform better than an accurate history of symptoms, and the persons' ability to refrain from locally spreading their germs.
Better leadership and reliance on scientific medicine is far more important than unproven and invasive technologies.

PPV: Positive predictive value, NPV: Negative predictive value.

Supplemental Table 5 Selected comments about ethics, privacy and harms of surveillance.

Afraid of where we are going…I was afraid before COVID, even more so now.
I think digital surveillance is a slippery slope. First COVID, then what is next?
Big brother is salivating. Re-read 1984. Read Hariri×s 21 lessons for the 21st century.
The winners will be private investors.
Digitalize schools and universities, not daily life.
Only totalitarian governments are able to control and surveil this kind pandemics.
A lot of power to the state, and that's not good for anyone.
Like the atomic bomb, any great idea can have unforeseen consequences.
Tech companies have no conscience and compensate for that by overemphasizing support of liberal programs. The rights and wellbeing of the average citizen have no place in their thinking. .will never get our privacy back once it has been given away.
Too much potential for corruption and misuse. Violates essential freedoms.
This country is based on personal freedoms. This is a significant invasion of privacy. Will need Socialism for this to work. I am against that.
Creepy. Extreme slippery slope. We've already given up so very many of our privacy rights in our society.
Setting a precedent for abuse. Don't even give an inch because they will take a mile.
I am very concerned about privacy issues and that any "temporary" relaxation of standards will become permanent.
Digital surveillance technologies in the hands of an autocratic government are a slippery slope to the loss of liberty.
These tools will facilitate discrimination and other rights abuse against racial minorities and people living in poverty.
Pandora's box.
Lots of potential for corruption. Criminals and corrupt politicians will use this to track their unsuspecting victims.
We can use incredible technology for the benefit of mankind, the problem we have is we keep handing this power to whoever can afford it, not those who deserve it.