Digitalization of contact tracing: balancing data privacy with public health benefit

Jeremy Wacksman¹

Accepted: 2 June 2021 / Published online: 10 June 2021
© The Author(s), under exclusive licence to Springer Nature B.V. 2021

Abstract

The COVID-19 pandemic has brought the long-standing public health practice of contact tracing into the public spotlight. While contact tracing and case investigation have been carefully designed to protect privacy, the huge volume of tracing which is being carried out as part of the pandemic response in the United States is highlighting potential concerns around privacy, legality, and equity. Contact tracing during the pandemic has gained particular attention for the new use of digital technologies—both on the consumer side in the form of Exposure Notification applications, and for public health agencies as digital case management software systems enable massive scaling of operations. While the consumer application side of digital innovation has dominated the news and academic discourse around privacy, people are likely to interact more intensively with public health agencies and their use of digital case management systems. Effective use of digital case management for contact tracing requires revisiting the existing legal frameworks, privacy protections, and security practices for management of sensitive health data. The scale of these tools and demands of an unprecedented pandemic response are introducing new risks through the collection of huge volumes of data, and expanding requirements for more adept data sharing among jurisdictions. Public health agencies must strengthen their best practices for data collection and protection even in the absence of comprehensive or clear guidance. This requires navigating a difficult balance between rigorous data protection and remaining highly adaptive and agile.

Keywords Contact tracing · COVID-19 · Digital case management · Data privacy · Public health

Background

Contact tracing as a standard public health tool

Contact tracing is a regularly used public health strategy with a robust record of efficacy (Bland, 2020). For hundreds of years contact tracing has been used in some form to manage the spread of infectious diseases (Fairchild et al., 2020). More recently it has been used to great effect during the Ebola pandemic and coronavirus outbreaks such as the SARS epidemic (Glasser et al., 2011; Sacks et al., 2015; Sun & Viboud, 2020). In the United States, contact tracing, sometimes branded as “partner notification,” is also a regularly used strategy for proactively notifying people of

potential exposure to reportable sexually transmitted infections (STIs) (Gostin & Hodge, 1998; Rietmeijer et al., 2011). While contact tracing is used globally, this analysis focuses on the United States—though the general themes are globally relevant.

For the purposes of this discussion, the term “contact tracing” is used to refer to both case investigation and contact tracing. Case investigation includes the identification and interview of individuals with confirmed or probable infections. As part of the case investigation process interviewers solicit a list of contacts—people who, based on meeting disease-specific criteria, were potentially exposed to the disease through their interaction with the case and are at elevated risk of infection. A contact tracer will then try to notify these potential contacts of their risk of exposure, and provide guidance on how to monitor their symptoms and minimize the risk of further disease transmission (CDC, 2020a, 2020b). Depending upon the scenario, public health agencies may issue orders for isolation or quarantine to cases and contacts, respectively (Adler et al., 2020).

✉ Jeremy Wacksman
jwacksman@vcu.edu

¹ Department of Health Administration, College of Health Professions, Virginia Commonwealth University (VCU), Richmond, VA, USA

Contact tracing is fundamentally designed to protect privacy while promoting the public good. Crucially, the identity of the case is generally not revealed to a contact. In some scenarios different sets of people will conduct case investigation and contact tracing which can reinforce this separation of data. While there are of course instances where a case's identity is unlikely to be effectively concealed (i.e., for an STI where a contact only had one recent partner), the strategy is still designed to minimize the risk of unnecessarily exposing private information (Gostin & Hodge, 1998). Revealing the identity of the index case could damage personal relationships or have other consequences if exposed to an employer or other business associate. As a result, building trust is a core element of effective contact tracing, requiring skill and careful judgement to effectively navigate an interview (Mooney, 2020).

Contact tracing during the COVID-19 pandemic

Historically contact tracing was relatively unknown to the general public in the United States; however, during the COVID-19 global pandemic contact tracing came into the spotlight. In 2020, contact tracing emerged as one of the key tools that public health agencies could use to respond to and manage the scope of the COVID-19 pandemic. It is one of the key pillars of the “test and trace” strategy which many localities have employed (“TestAndTrace”, 2020). While the U.S. Centers for Disease Control and Prevention (CDC) provides national guidance, contact tracing is generally carried out by state and local health agencies. As a result, there are many variations on how tracing is carried out, and each state is making its own investments to quickly adapt to the huge increase in demand on its resources. Beyond the growing case count volumes seen across the U.S., the particulars of COVID-19 and its transmission window require that contact tracing be carried out very quickly; if contacts are not notified promptly (i.e., within several days) then the benefit of contact tracing is largely undermined (Ferretti et al., 2020).

New technologies for contact tracing

The global nature of COVID-19 and the need for relatively rapid follow-up has inspired significant exploration of and investment in technology to support contact tracing. Through the pandemic two general categories of contact tracing technologies have gained prominence: (1) exposure notification and (2) digital case management applications/systems (CDC, 2020a, 2020b).

- (1) **Exposure notification**, or proximity tracking, relies on smartphones or similar devices with Bluetooth or GPS functions that can automatically catalog proximity and duration of contact between two people. If one of

them later has a confirmed positive test, other individuals who met the thresholds for proximity and duration can be notified of potential exposure without revealing the identity of the source case or the specific location where the exposure occurred.

- (2) **Case/Record management** systems are software platforms which public health agencies use to support the digitalization and streamlining of case investigation and contact tracing. Public health authorities or other organizations use these systems as both database and job aid, employing standardized workflows (e.g., transferring cases to other jurisdictions, managing attempts to reach contacts, guiding staff through interviews, etc.) and gathering information to support the core tasks of contact tracing (e.g., identities of potential contacts, details of disease progression, requests for additional resources, etc.). These systems have been developed to streamline the labor-intensive process of conventional public health contact tracing, a necessity given the exceptional volume of cases during the COVID-19 pandemic.

Popular media, as well as academic analyses, have been very focused on the privacy implications of exposure notification apps, given the novelty of these systems and the public's limited understanding of how these systems protect privacy (Cohen et al., 2020; Klenk & Duijf, 2020; Ranisch et al., 2020). There has been much less discussion about case management applications and systems used by public health agencies and other organizations. The digitalization of contact tracing is in many ways analogous to the digitalization of other health data in medical records but presents unique challenges around privacy. It also enables a new level of scale and reach for contact tracing which is stretching the existing legal and ethical frameworks around public health management and use of data (Gasser et al., 2020).

Digital case management tools are designed to improve many elements of the contact tracing process, each component of which requires sensitive personal data (CDC, 2020a, 2020b). These include:

- Improved efficiency by streamlining the collection and management of data and storing it in hosted databases, enabling rapid deployment and testing of new protocols.
- Enabling more staff to participate in related activities by working in a shared environment accessible from any location.
- Digitizing otherwise manual workflows which enable direct outreach to cases and contacts (e.g., automatically sending quarantine and isolation notices by email, conducting daily monitoring through text messaging, etc.).

Many barriers to the public's willingness to participate in contact tracing remain. While many of these barriers are logistical (e.g., difficulty in getting people to answer phone calls from unknown numbers), or cultural (e.g., distrust of government), digital case management presents both opportunities and challenges for preserving data privacy while engaging in effective contact tracing at scale. Additional privacy issues are emerging as organizations other than government health agencies attempt to adopt contact tracing. Digital case management tools, purpose built for contact tracing, are lowering the barrier of entry and enabling organizations such as universities or private companies to engage in contact tracing activities (Jones Day, 2020).

This analysis highlights several of the specific challenges and opportunities that digital case management systems present related to data privacy and security in the United States.

Analysis

In 2009, Lee and Gostin proposed a framework for national privacy protection of public health data (Lee & Gostin, 2009). They presciently anticipated that as the role of technology grew, public health agencies would need new strategies and approaches to demonstrate appropriate treatment of data. However, guidelines for managing digital health data remain highly fragmented, as many issues are determined at the state or locality level. The rapid expansion of contact tracing tools has demonstrated that while the prediction of an expanded role of technology was correct, the frameworks and laws that Lee and Gostin suggested did not fully materialize. It appears unlikely that new policies and legal guidance will be implemented with sufficient speed and clarity to effectively clarify some of the key open questions around digitalization of contact tracing. This analysis highlights several key contributors to the tension between privacy and increased data collection, a tension which has been exacerbated by the increasingly prominent role of technology.

The absence of a clear policy solution

Many members of the public in the United States may assume that public health agencies will handle their data in accordance with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 or other laws that guide the management of health data. However, the Privacy Rule under HIPAA does not preempt local laws that allow for a variety of public health uses of data to manage the spread of communicable diseases such as COVID-19 (HHS Office for Civil Rights (OCR), 2009; Shachar, 2020). Infectious diseases like COVID-19 must be reported to public health agencies, even without a patient's consent, and that data may be used to inform public health activities such as

contact tracing. The Common Rule (i.e., "The Federal Policy for the Protection of Human Subjects") is another notable law which aims to protect health data. While the Common Rule is primarily focused on the protection of research subjects, many public health activities blur the line between research and public health operations and may therefore not be covered. Several new laws are under discussion but have not progressed at a pace that will help to address the urgent demands of the COVID-19 pandemic (OHRP, 2020). This leaves a good bit of ambiguity about what data is in bounds for collection during contact tracing, and what data protection standards and practices are required.

The distributed nature of public health laws at the state level limit the role of the federal government in navigating contact tracing. According to a recent analysis from the Government Accountability Office (GAO), it is unclear the extent to which the federal government can regulate state databases, though there is precedent to suggest some regulation is possible (Liu, 2020). While direct regulation may not be feasible, there is certainly precedent for tying funds to compliance with certain standards (i.e., Medicare payments contingent upon compliance with privacy requirements). While further federal regulation would certainly simplify standards around public health data, such a shift is unlikely to be popular and is not necessarily desirable. Outside of what is legally feasible, there are political and institutional barriers which make the development and implementation of clear, directive guidance unlikely in the near term. Following are some key implementation and policy areas that affect digitalization and expansion of contact tracing and related public health activities but remain unresolved.

What is the scope of public health data?

While the proximate driver for adopting a digital tool may be efficient case management, the introduction of these systems makes it easier to increase the scope of data collected beyond the core required fields. The incremental inclusion of additional data may be useful or necessary as the scope of services available during the pandemic expands. For example, linking people to relevant resources will be more feasible if additional screening is conducted and data is gathered. Digital systems also present a unique opportunity to gather additional data for research purposes. However, the ease of adding new fields to digital systems obscures hidden costs.

While additional data *may* present concrete benefits to public health activities, each additional piece of data collected has potential negative implications and introduces new risk. There is no bright line in the scope of what constitutes relevant data for public health activities, and justifications can be found for the inclusion of many additional data fields. However, participants may become increasingly suspicious of contact tracers and investigators asking for

lots of information. The inclusion of more data may also increase the duration of activities such as interviews, potentially limiting the number of people reached or discouraging participation. More private data collected and shared also increases the consequences should there be a data breach or other accidental exposure.

Even without detailed government regulation, there are best practices that can be employed to manage the scope of data collected during contact tracing activities:

- For every new piece of data that is proposed to be added to a system for collection, explicitly discuss both the benefits and drawbacks to gathering this additional information.
- Consider employing a checklist to evaluate each new question or data type to clarify whether there are alternative means of accomplishing the desired workflow or obtaining the required information from existing sources.
- Periodically audit the scope of data collected to remove fields that are no longer relevant and stop collecting data which is not used.
- Meet regularly with system users, and review collected data to detect common trends in data quality and use.
- Where feasible, clearly identify and focus on the standard minimum set of data required for core contact tracing work.

How should data be shared?

The COVID-19 pandemic includes numerous outbreaks that cross jurisdictional boundaries. In addition, despite a variety of orders to minimize movement and travel, contacts and cases regularly move across counties and states, requiring careful coordination. Many public health agencies have data sharing agreements that specify a permission structure for sharing data. However, there are limits to the practical use of these agreements, particularly in the face of massive numbers of cases and contacts moving quickly around the country. A huge influx in the size of the public health workforce adds additional complications as staff become oriented to rules that can be very complex to remember and follow. Combined with the dynamic scope of data being collected and the proliferation of a variety of different digital tools, data sharing remains a persistent challenge.

Absent clear, centralized standards on data sharing, organizations that conduct contact tracing can take steps to clarify how data should be shared:

- Government agencies like the CDC, and professional organizations like the Association of State and Territorial Health Officials (ASTHO), can serve as central advisory resources that guide the adoption of data sharing standards (ASTHO, 2020).

- Manage risk by minimizing the set of data that is shared across jurisdictions to a clearly defined subset of critical fields.
- Define clear tools and processes for data sharing, so that staff do not fall back on insecure, ad hoc approaches, and so that urgent data transfer activities are not delayed.
- Provide clear communication materials for staff that summarize data sharing agreements in easily understood language.

How should data be protected?

The range of issues around digital security of health data is covered by many policy frameworks and laws. Management of digital health information is not new to public health agencies. However, the new generation of digital case management tools, just as they introduce new potential, also introduce a new range of vulnerabilities. These tools enable rapid scaling of a workforce and will often equip new or volunteer tracers or investigators with access to sensitive datasets. Volunteers or rapidly trained staff may not be familiar with standard practices regarding health data or may have trouble recalling how to handle nuanced situations. Even health practitioners may not be familiar with the specific laws that guide the handling of public health data in a pandemic situation, and a dynamic environment with time-sensitive demands may push people to take actions that do not adequately protect data.

Absent specific guidance for data protection, public health agencies can fall back on healthcare industry regulations like HIPAA which can provide best practices, keeping in mind the exceptional uses of public health data that may be required to carry out contact tracing activities:

- Build robust tools that map as closely as possible to local laws; in other words, make it very difficult for users to access data to which they should not have access.
- Provide a discrete set of standard tools and processes to protect data when downloaded or when being shared.
- Where data is flowing between a contact tracing system and other disease reporting systems, ensure that the data is adequately protected at all points across all systems, and that sharing permissions are aligned.

How can public health agencies build confidence and trust?

A theme which emerges from the above data privacy considerations is the importance of public trust for contact tracing to be successful (Cohen et al., 2020; McGraw et al., 2012). For manual contact tracing to work, people must be willing to divulge sensitive personal information to a government representative that they have never met, and will be asked to

provide information that triggers the health agency to reach out to their contacts. Any occurrence that undermines public confidence in the privacy and security of their personal health data could erode the efficacy of the overall tracing strategy. Notably, the recent focus on Exposure Notification systems and publicity around privacy concerns may undermine core public health efforts to use digital solutions to expand conventional contact tracing. There are technically rigorous explanations of why Exposure Notification is by design exceptionally secure, but these explanations rely on both a technical understanding of the issue and a willingness to invest time and effort to understand. Put another way, it is a technology that by default does not seem trustworthy to many people and requires substantial effort to encourage people to participate. Some public health professionals may be frustrated to see people freely giving away extremely personal information to private technology companies like Google and Facebook, but hesitant to provide it to local health agencies (Khazan, 2020).

Agencies can work to build public confidence in data privacy and protection for contact tracing by:

- Ensuring that language around data privacy and protection is easily understood and is incorporated into all scripts.
- Mitigating the risk of accidental data exposure through robust organizational policies and practices.
- Designing workflows that demonstrate the commitment to data protection by obscuring identifiable data in communication materials where feasible, gathering informed consent, and reinforcing the silo of data between cases and contacts.
- Explaining clearly to all stakeholders exactly how their data will be used and protected.

The middle ground: striking a balance

Moving forward with contact tracing and related public health activities, it will be critical to strike a balance between carefully protecting public health data, and remaining agile and responsive in the face of a pandemic. Agencies working on the pandemic response face intense demands from multiple stakeholders and very rapid timelines to implement changes. Public health data regulations are inherently somewhat flexible to enable rapid adaptation and action. While it may be easy to claim that every effort will be made to protect data, this is in tension with the desire to make every effort to be responsive to the needs of the pandemic response effort. Incremental actions to increase data privacy may mean that other work is less effective. For example, if emails with quarantine and isolation notices are transmitted through a secure portal, this might improve security but might limit the number of people who are able to successfully access the

information. This unsatisfying tension requires a foundation of data protection standards and robust security practices while enabling professional judgement.

As the transformation of contact tracing demonstrates, finding the appropriate balance between privacy and sharing has become an increasingly central ethical issue for public health agencies and other organizations. Without a clear policy framework, lacking centralized protocols, and with myriad different digital platforms, the pressures on this balance are growing:

- The potential **value** of public health data continues to increase, as public health workflows and analysis/dissemination can happen very quickly, and more sophisticated analyses can drive policy decisions.
- The potential **risk** of collecting more data increases the consequences of a potential data leak incident or other privacy violations.

With constant changes in technology and changing public expectations around privacy, this balance will likely be a moving target, requiring regular reflection and re-evaluation of practices and procedures. While contact tracing is one of the most notable examples of the recent rapid scaling of scope and scale for public health data, it is also in many ways exemplifies a tension that will continue to be felt across many different public health activities.

Looking beyond the pandemic

The COVID-19 pandemic has potential to dramatically accelerate long-term change in how contact tracing is practiced and how public health data is managed. While most states, territories, and tribal nations already had digital case management systems, the COVID-19 pandemic quickly pushed forward the move to a new generation of tools for public health data collection, management, and assessment. These digital platforms may also support a wide range of infectious diseases that require contact tracing or other follow-up activities. The concept of contact tracing is likely to remain familiar to many people, and individual perceptions and experiences may affect their interest in participating in related public health activities in the future. The impact on the management of other infectious diseases through contact tracing is not yet clear.

Looking ahead, this shift in contact tracing may converge with other trends, including the individual's role in the active management of their own health data (Tolmie & Crabtree, 2018). Just as the U.S. rebranded contact tracing around STIs as “partner notification,” there may be other efforts to develop and rebrand more specialized workflows, especially ones that rely more heavily on technology. To date, health agencies maintain the authoritative record of diseases

and have facilitated contact tracing through their record of official lab results. Experimental services that enable the individual to drive their own contact notification have not taken off, but as more people become familiar with the core concept, one can imagine more experiments like this in the future (Rietmeijer et al., 2011). Given the skepticism some people hold towards the government, providing ways that people can trigger and manage their own contact tracing may be appealing to some parts of the population. Just as moving from paper forms to ad hoc spreadsheets to robust digital systems has amplified concerns about how public health data is managed, these emerging trends around how people are willing to share or interact with their personal data will introduce new challenges and complexity.

Conclusions

Management of data privacy is critical to stabilizing and building public confidence in contact tracing; a lack of confidence has presented a barrier to effective management of the pandemic response (McClain & Raine, 2020). Digital technologies, rapid scaling, and expansion of scope have dramatically affected contact tracing efforts. Exposure Notification systems, which are designed to make it impossible to determine the source of a contact's exposure, are attracting exceptional levels of scrutiny. Meanwhile the digitization of manual contact tracing is moving huge volumes of sensitive personal data through strained public health agencies with much less public attention. Cross cutting these technologies and approaches is a general skepticism about contact tracing that has the potential to undermine its efficacy. It is critical that public health agencies adapt their processes to emphasize the centrality of data privacy and security to cases, contacts, and staff. While it is important to advocate for local, state, and national policy that guide the balance of data privacy and robust response, organizations will not be able to wait for these and will need to constantly balance these frequently conflicting priorities.

Funding No funds, Grants, or other support was received.

Declarations

Conflict of interest The author is employed by a company which develops digital case management software and supports multiple public health agencies.

References

- Adler, S., Kappagoda, M., Johnson, R., & Glass, P. (2020). *Isolation and quarantine* | ChangeLab solutions. Change Lab Solutions.
- ASTHO. (2020, October 20). Legal Challenges to State COVID-19 Orders. <https://www.astho.org/generickey/GenericKeyDetails.aspx?contentid=22924&folderid=5156&catid=7203>. Accessed 8 Nov 2020
- Bland, S. (2020, July 13). Reflections on the History of Contact Tracing | O'Neill Institute. <https://oneill.law.georgetown.edu/reflections-on-the-history-of-contact-tracing/>. Accessed 1 Nov 2020
- CDC. (2020, February 11). Coronavirus Disease 2019 (COVID-19). *Centers for Disease Control and Prevention*. <https://www.cdc.gov/coronavirus/2019-ncov/php/contact-tracing/index.html>. Accessed 1 Nov 2020
- CDC. (2020, October 10). Contact Tracing: Using Digital Tools. CDC. <https://www.cdc.gov/coronavirus/2019-ncov/php/open-america/contact-tracing/index.html>. Accessed 1 Nov 2020
- Cohen, I. G., Gostin, L. O., & Weitzner, D. J. (2020). Digital smartphone tracking for COVID-19: Public health and civil liberties in tension. *JAMA*, 323(23), 2371. <https://doi.org/10.1001/jama.2020.8570>
- Fairchild, A. L., Gostin, L. O., & Bayer, R. (2020, July 20). Contact tracing's long, turbulent history holds lessons for COVID-19. *Ohio State University News*. <https://news.osu.edu/contact-tracings-long-turbulent-history-holds-lessons-for-covid-19/>. Accessed 1 Nov 2020
- Ferretti, L., Wymant, C., Kendall, M., Zhao, L., Nurtay, A., Abeler-Dörner, L., et al. (2020). Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. *Science*, 368(6491), eabb6936. <https://doi.org/10.1126/science.abb6936>
- Glasser, J. W., Hupert, N., McCauley, M. M., & Hatchett, R. (2011). Modeling and public health emergency responses: Lessons from SARS. *Epidemics*, 3(1), 32–37. <https://doi.org/10.1016/j.epidem.2011.01.001>
- Gasser, U., Ienca, M., Scheibner, J., Sleight, J., & Vayena, E. (2020). Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid. *The Lancet Digital Health*, 2(8), e425–e434. [https://doi.org/10.1016/S2589-7500\(20\)30137-0](https://doi.org/10.1016/S2589-7500(20)30137-0)
- HHS Office for Civil Rights (OCR). (2009, January 7). Disclosures for Public Health Activities. *HHS.gov*. Text. <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-public-health-activities/index.html>. Accessed 6 Nov 2020
- Jones Day. (2020, July). COVID-19 Contact Tracing in the Private Sector. Jones Day. <https://www.jonesday.com/en/insights/2020/07/a-guide-to-navigating-cybersecurity-privacy-and-employment-law-issues-with-covid19-contact-tracing-in-the-private-sector>. Accessed 11 Nov 2020
- Khazan, O. (2020, August 31). The Most American COVID-19 Failure Yet. *The Atlantic*. <https://www.theatlantic.com/politics/archive/2020/08/contact-tracing-hr-6666-working-us/615637/>. Accessed 11 Nov 2020
- Klenk, M., & Duijf, H. (2020). Ethics of digital contact tracing and COVID-19: who is (not) free to go? *Ethics and Information Technology*. <https://doi.org/10.1007/s10676-020-09544-0>
- Lee, L. M., & Gostin, L. O. (2009). Ethical collection, storage, and use of public health data: A proposal for a national privacy protection. *JAMA*, 302(1), 82. <https://doi.org/10.1001/jama.2009.958>
- Liu, E. C. (2020). Constitutional authority to regulate the privacy of state-collected contact-tracing data. *Constitutional Authority to Regulate the Privacy of State-Collected Contact-Tracing Data*, 1, 1–4.
- LO Gostin JGJ Hodge. (1998). Piercing the veil of secrecy in HIV/AIDS and other sexually transmitted diseases: theories of privacy and disclosure in partner notification. *Duke J. Gender L. & Pol'y.*, 5, 80.
- McClain, C., & Raine, L. (2020, October 30). The Challenges of Contact Tracing as U.S. Battles COVID-19. *Pew Research Center: Internet, Science & Tech*. <https://www.pewresearch.org/inter>

- [net/2020/10/30/the-challenges-of-contact-tracing-as-u-s-battles-covid-19/](https://doi.org/10.1002/pds.2319). Accessed 11 Nov 2020
- McGraw, D., Rosati, K., & Evans, B. (2012). A policy framework for public health uses of electronic health data. *Pharmacoepidemiology and Drug Safety*, 21(S1), 18–22. <https://doi.org/10.1002/pds.2319>
- Mooney, G. (2020). “A menace to the public health” — Contact tracing and the limits of persuasion. *New England Journal of Medicine*. <https://doi.org/10.1056/NEJMp2021887>
- OHRP. (2020, April 8). OHRP Guidance on Coronavirus. *HHS.gov*. Text. <https://www.hhs.gov/ohrp/regulations-and-policy/guidance/ohrp-guidance-on-covid-19/index.html>. Accessed 13 Nov 2020
- Ranisch, R., Nijssingh, N., Ballantyne, A., van Bergen, A., Buyx, A., Friedrich, O., et al. (2020). Digital contact tracing and exposure notification: Ethical guidance for trustworthy pandemic management. *Ethics and Information Technology*. <https://doi.org/10.1007/s10676-020-09566-8>
- Rietmeijer, C. A., Westergaard, B., Mickiewicz, T. A., Richardson, D., Ling, S., Sapp, T., et al. (2011). Evaluation of an online partner notification program. *Sexually Transmitted Diseases*, 38(5), 359–364. <https://doi.org/10.1097/OLQ.0b013e31820ef796>
- Sacks, J. A., Zehe, E., Redick, C., Bah, A., Cowger, K., Camara, M., et al. (2015). Introduction of mobile health tools to support ebola surveillance and contact tracing in Guinea. *Global Health: Science and Practice*, 3(4), 646–659. <https://doi.org/10.9745/GHSP-D-15-00207>
- Shachar, C. (2020, May 19). Protecting privacy in digital contact tracing for COVID-19: Avoiding a regulatory patchwork | Health affairs blog. *Health Affairs*. <https://doi.org/10.1377/hblog20200515.190582/full>. Accessed 11 Nov 2020
- Sun, K., & Viboud, C. (2020). Impact of contact tracing on SARS-CoV-2 transmission. *The Lancet Infectious Diseases*, 20(8), 876–877. [https://doi.org/10.1016/S1473-3099\(20\)30357-1](https://doi.org/10.1016/S1473-3099(20)30357-1)
- TestAndTrace: A Strategy to Contain COVID-19 Outbreaks. (2020). *#TestAndTrace: The Best Contact Tracing Resource*. <https://testandtrace.com/>. Accessed 11 Nov 2020
- Tolmie, P., & Crabtree, A. (2018). The practical politics of sharing personal data. *Personal and Ubiquitous Computing*, 22(2), 293–315. <https://doi.org/10.1007/s00779-017-1071-8>

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.