International Journal of E-Planning Research
Volume 10 • Issue 2 • April-June 2021

COVID-19 Contact Tracing:
From Local to Global and Back Again

Teresa Scassa, University of Ottawa, Canada

ABSTRACT

This article surveys the rise of contact tracing technologies during the COVID-19 pandemic and some of the privacy, ethical, and human rights issues they raise. It examines the relationship of these technologies to local public health initiatives, and how the privacy debate over these apps made the technology in some cases less responsive to public health agency needs. The article suggests that as countries enter the return to normal phase, the more important and more invasive contact tracing and disease surveillance technologies will be deployed at the local level in the context of employment, transit, retail services, and other activities. The smart city may be co-opted for COVID-19 surveillance, and individuals will experience tracking and monitoring as they go to work, shop, dine, and commute. The author questions whether the attention given to national contact tracing apps has overshadowed more local contexts where privacy, ethical, and human rights issues remain deeply important but relatively unexamined. This raises issues for city local governance and urban e-planning.

KEYWORDS

Centralized, Contact Tracing App, Decentralized, Ethics, Exposure Notification, Human Rights, Pandemic, Privacy, Surveillance, Workplace

1. INTRODUCTION

This article reflects on the trajectory of debates over the use of technology to assist in contact-tracing during the COVID-19 pandemic. It begins by exploring how global interest in contact-tracing apps took hold rapidly, generating international coalitions around technological development as well as around privacy and security concerns. It considers the role of technology in contact-tracing debates, and how privacy, at least at the global level, became a focal point overshadowing other important public policy, ethical and human rights issues. The article examines how the relevant geographies for contact-tracing apps shifted over the course of the pandemic – creating local, national, and international levels of engagement. As countries began to enter the 'return to normal' phase, attention became more centred on local concerns, shifting from a focus on apps to other methods (and spaces) for identifying relevant contacts. Although privacy, ethics and human rights issues exist in these spaces as well, in contrast with high-profile contact-tracing apps, they have received relatively little public attention. Despite the furor over national level contact-tracing apps, the 'return to normal' phase will likely entail a concentration of efforts – both public and private at the local level. This will inevitably raise technology governance issues for cities. It may also raise issues around the embedding of certain

DOI: 10.4018/IJEPR.20210401.oa4

types of surveillance technologies into urban e-planning frameworks. Although far less attention has been paid to privacy, ethics and human rights issues at these levels, when it comes to contact-tracing technologies and COVID-19, the issues and the particular way in which they manifest at the local level should not be overlooked.

This article is based upon a literature that has evolved rapidly and in real-time, including academic contributions, news reports, opinion pieces, privacy impact assessments, and government reports. The challenges of writing about a situation that has evolved rapidly and continues to change are frankly acknowledged. The author is a legal scholar, based in Canada, and recognizes the influences as well of both discipline and geography in this account.

2. THE RAPID RISE OF CONTACT-TRACING TECHNOLOGIES

2.1. Manual Contact-Tracing

Manual contact-tracing is a typical public health response to the outbreak of a contagious disease (CDC 2020, Kahn 2020). It often occurs at the local level, with data sharing with public health authorities at regional and national levels. People who are known to be infected are screened by a contact tracer who questions them about their movements and contacts during a window of time considered relevant to the contagious nature of the disease. Tracers then communicate with the infected person's contacts to notify them that they have been exposed to the disease and to advise them to take appropriate steps. Data about contacts collected by public health authorities can also be used in deidentified form for analysis and modeling of the spread of the disease and may prove useful in designing appropriate public health responses (Kahn 2020). The balance between privacy rights and the public interest is met by the fact that the person who is providing this information is known to be infected, and their close contacts may be at risk of contracting and spreading the disease.

2.2. Early Contact-Tracing Technologies

The high level of infectiousness of COVID-19 and the absence of pre-existing immunity within the population proved challenging to public health authorities (Kahn 2020) – some of whom, at least in North America, had seen their budgets and resources undermined over years of government cutbacks (Warnica 2020, Scheck & Hing 2020; Hawkins & Wang 2020). Additional weaknesses in manual contact-tracing for COVID-19 included the fact that people often had trouble remembering all the places they had been and people they had encountered in the two weeks preceding their positive test. In addition, while they might remember specific encounters with known individuals (family members, friends or colleagues) they might have also encountered many people whose identity would be unknown to them (for example, shopping in stores or riding public transit). In the contemporary big data and high-tech environment, it is not surprising that individuals, organizations, and governments began to speculate about whether technological solutions could supplement or replace manual contact-tracing.

Early attempts at digital contact-tracing did not necessarily involve apps and instead focused on the kind of data that was readily available because it was routinely collected by private sector organizations. This included cell phone location data and data from credit or debit card expenditures (Amit 2020, Daflos 2020). This data could be used to supplement the recollection of individuals, reminding them of places they had been so that they could reflect on those with whom they might have had contact. It could also be used to issue generalized warnings (e.g. that an infected individual had been on a particular public transit vehicle on a particular day and time). Public health authorities could also use this data for disease modeling and analytics. Data of the kind collected in so-called smart cities could also be conscripted for contact-tracing, including video-surveillance data (Kleinman & Merkel 2020, Kharpal 2020, COVID-19 National Emergency Response Center 2020). In countries such as South Korea, Singapore, Taiwan and China, multiple existing data sources were brought to

bear on pandemic control questions, sometimes in conjunction with new purpose-specific technologies. (Kleinman & Merkel 2020, COVID-19 National Emergency Response Center 2020)

Using pre-existing tracking data for contact-tracing raises obvious privacy concerns as it is capable or revealing a considerable amount of information about a person's activities. Privacy problems with using location data for contact-tracing led developers to explore the use of Bluetooth technology to either supplement or replace location data (Kitchin 2020). Bluetooth does not record location; rather it sends signals between one device and another; these signals vary in strength and duration. This data could be used to assess whether a particular encounter created a risk of infection. Bluetooth-enabled apps installed on multiple devices could register relevant proximity incidents. If a user tested positive, public health messaging could be communicated to those who had been in relevant proximity to infected persons. Singapore's TraceTogether app (https://www.tracetogether.gov.sg/), which later served as a basis for contact-tracing apps in other jurisdictions, relied upon Bluetooth proximity data (Guy 2020). Unlike cell phone tracking data, which is routinely collected from all phones, Bluetooth-based contact-tracing apps require a significant and deliberate uptake within the population to be useful (Kitchin 2020). Therefore, Bluetooth-based apps require high levels of public trust and willingness to adopt the technology.

2.3. Global Debates About Privacy/Surveillance

The growing interest in using technology to track individuals and to identify contacts inevitably triggered privacy concerns. Contact-tracing using pre-existing cell phone location or other location-based data created a new form of non-consensual state surveillance that made use of this data highly problematic. This is illustrated by the ultimate decommissioning of Norways GPS-based contact-tracing app based upon privacy concerns (Agence France Presse 2020). The idea that a user's 'social graph' – a record of their daily interpersonal interactions – could be generated by a Bluetooth-enabled contact-tracing app was also a cause of concern (Kleinman & Merkel 2020). These concerns were amplified by fears that the technologies might be repurposed by governments, or become normalized such that, post-pandemic, individuals might be asked to self-surveil for other purposes (van Kolfschooten & de Ruijter 2020). Privacy issues were not limited to concerns over intrusions by the state. Many were wary that contact-tracing apps created security risks that could expose users' personal information or place them at risk of malicious attacks (Vaudenay 2020, Kitchin 2020).

These concerns led to the relatively quick formation of coalitions of privacy experts and advocates who sought to identify appropriate parameters for the use of technology to assist in contact-tracing. The focus was on a purpose-specific app rather than the repurposing of existing data. This was because apps available for voluntary use were considered more privacy friendly than conscripted, repurposed data. Further, apps could be designed with privacy in mind. The Pan-European Privacy-Preserving Proximity Tracing group (PEPP-PT 2000) formed and proposed both decentralized and centralized solutions for privacy preserving contact-tracing apps (Vaudenay 2020). Centralized models were ones which provided for the central storage of data at some point in the process (e.g. after a user tested positive) while decentralized storage ensured that all relevant contact data was stored locally on a user's phone (Vaudenay 2000). This coalition soon fractured, with an offshoot, Decentralized Privacy Preserving Proximity Tracing (DP3T) emerging to advocate for a fully decentralized approach (DP3T 2000). National solutions such as Singapore's TraceTogether, France's StopCovid (https://www.economie.gouv.fr/stopcovid) and Australia's CovidSafe (https://www.health.gov.au/resources/apps-and-tools/covidsafe-app) were built using a centralized approach. Many other apps, including those in Germany (https://github.com/corona-warn-app), Ireland (https://covidtracker.gov.ie/) and Canada (https://www.covidshield.app/) have chosen the DP3T decentralized approach.

It is important to note that the global debate over centralized vs. decentralized contact-tracing apps focused almost entirely on privacy issues. With centralized data storage there were some concerns about surveillance – in other words, what governments might do with the data that they collected. With the fully decentralized models, the primary privacy concerns related to security;

security-related concerns were also present for centralized storage models (Vaudenay 2020). Yet the use of contact-tracing or exposure notification technologies raise a host of other issues which have been far less prevalent in discussions around their deployment. These involve questions of ethics and human rights that include access to the technologies, the deployment of unproven technologies on vulnerable populations, the risks of false positives and negative notifications and the potential for differential impacts on vulnerable communities, and the raising of false expectations that might lead to more risk-taking behaviours (Millar 2020, Kahn 2020, Scassa et al 2020; Kitchin 2020, Gasser et al 2020). The focus on privacy, and in particular, the debate over centralized and decentralized storage, also framed the discussion as one about which *type* of contact-tracing app to adopt, rather than one of whether contact-tracing apps were ethically appropriate or even useful technologies.

2.4. GAEN and the Role of Global Tech Giants

Although smart phones are not the only platform for deploying digital contact-tracing technologies, their relatively broad diffusion combined with user familiarity with downloading and using apps made smart phones an obvious vehicle. Google and Apple, the companies that dominate smart phone operating systems paired together with privacy advocates who favoured PP3T solutions to create the application programming interface (API) for the Google/Apple Exposure Notification System (GAEN). The GAEN uses only Bluetooth signals to determine proximity events, relies entirely on decentralized data storage (which means that data about relevant contacts is stored only on users phones and is never uploaded to a central system), and has an anonymized protocol for providing exposure notifications once an app user tests positive for COVID-19.[1] Some refer to apps built on this protocol as 'exposure notification' rather than contact-tracing apps, since the exposure-notification apps are not integrated with public health contact-tracing activities. The shift in vocabulary is interesting as it marks the sharp divergence of the technology away from specific public health objectives for contact-tracing, towards a simple individual-focused technological notification system.

The GAEN model is relatively prescriptive. Its Terms of Service[2] make certain parameters mandatory for apps built on this protocol. For example, apps must be for voluntary and not mandatory use, they may use only decentralized storage; they must be endorsed by a government; and only one app is possible per country (unless a country adopts a regional approach). Further, the apps must be decommissioned at the end of the pandemic. Data about relevant proximity events is stored by the apps only for a limited period of time and is routinely purged.

The prescriptive and normative nature of GAEN had the effect of constraining state options for using contact-tracing technology. This has raised serious issues about the power of tech giants to dictate privacy norms (Foer 2020, Newton 2020). Some jurisdictions were reluctant to use GAEN because it allowed only for decentralized exposure notification and did not integrate with public health initiatives. Countries such as the UK, Australia, France, and Germany began work on their own contact-tracing apps that would provide for some centralized storage of data and for the involvement of human contact tracers. Although Australia and France released centralized apps, the UK was forced to abandon its considerably more complex app after testing revealed significant problems (Sabbagh & Hern 2020). Germany, which initially pursued a centralized model, eventually opted for a fully decentralized system (Busvine & Rinke 2020).

Not only were DP3T advocates more vocal in insisting on the privacy superiority of decentralized storage (Vaudenay 2020), some centralized storage apps had compatibility problems with Android or iOS, which impacted their functionality (Taylor 2020, OIPC 2020). The result was that the GAEN gradually became dominant in Western countries. However, because GAEN requires fully decentralized data storage, it has the particular disadvantage – from a public health point of view – of not being integrated with public health agency efforts, and of not providing useful data for public health authorities in mapping, modeling or analyzing disease progression or infection hotspots. Nevertheless, it now seems possible to collect some additional data if attempts to do so comply with

the GAEN terms of service (e.g.: Government of Ireland 2020), although only a few countries seem to have chosen this route.

3. GEOGRAPHICAL DIMENSIONS

Debates over contact-tracing technologies have taken place at different levels (local, regional, national, international) at different times during the pandemic. While decision-making authority around public-sector adoption of contact-tracing technologies lay with regional or national governments, the privacy debates took place on both the national (Lieber 2020, Agence France-Presse 2020) and international levels (DP3T 2020, PEPP-T 2020). At the same time, the most significant contacts between individuals occur at the local level, including schools, workplaces, retail stores, and local public spaces. As noted earlier, reinforced by Google and Apple, national-level contact-tracing app decisions, particularly in Western countries, shifted towards minimalist approaches that did not integrate easily with public health activities. This was even though it was possible to created integrated models that were capable of satisfying privacy regulators (e.g.: Australia's CovidSafe and Alberta's ABTraceTogether).

In the early days of the pandemic, when countries essentially went into 'lockdown', contact-tracing had a particularly local nature. Schools and businesses shut down, those who could began working from home, and air travel ground almost to a complete halt. The focus was very much upon containing local spread. As interest in contact-tracing technologies grew during this period, their adoption was contemplated even at the purely local level. For example, municipal public health officials in Ottawa, Canada, at one point floated the idea of releasing their own contact-tracing app. (Jones 2020). Nevertheless, the procurement of contact-tracing apps shifted quietly to the state or provincial level in federations or at the national level for unitary states.

As policymakers began contemplating a 'return to normal', interoperability of contact-tracing apps grew in importance as an issue. Interoperability would be a particular challenge in federal states such as Canada or the U.S., where regional adoption of different apps could create problems (Scassa 2020) or for confederations such as the European Union, with its mobility of nationals across member state boundaries (European Commission 2020). Interoperability became a more important factor and added impetus to the growing shift toward the GAEN in many countries.

Although the return to normal phase would involve travel across regional or national boundaries, a return to normal also meant a steep increase in the types of interactions people would be having within their local communities. Bars, restaurants, public parks, and beaches reopened. In-person retail, personal care and professional services became available. More people returned to their workplaces and began to circulate in an increasingly broad range of contexts.

This expansion of local activity was something that governments anticipated in rolling out contact-tracing apps. However, it also generated new and different contact-tracing issues. In the first place, it created a need to have local contact-tracing supports that were not dependent on technology either because the technology was not yet available, or it was not yet sufficiently adopted or reliable to fulfill its purposes. Manual contact-tracing remained an important public health function and governments increased their supports for such activities (Osman 2020, Simmons-Duffin 2020). In some cases, businesses were asked to manually record the names and contact information of customers (Government of Scotland 2020; Government of Ontario 2020; Gov.uk 2020) or individuals were asked to keep manual logs of where they had been and with whom they had interacted in case such information became necessary for contact-tracing (New Zealand 2020). Secondly, the return to normal phase shifted contact-tracing from serving only government and public health objectives towards other goals held by private actors. These included the desire of some businesses to provide public assurances that they were taking appropriate care to ensure customer safety, as well as the interest of amongst employers with larger workforces to limit any potential disease outbreaks in order to be able to keep their workers safe and capable of performing their duties.

3.1. Workplaces

Serious outbreaks in different workplaces during the pandemic highlighted the risks to employees – and to their employers' operations – posed by COVID-19 (Molteni 2020; Dryden 2020; Nack 2020). It is not surprising, therefore, that workplace health and safety has been a preoccupation of many employers in the 'return to normal' phase (Chyi 2020; Bond 2020; Knight 2020; Singer 2020). Not only is providing a safe and healthy workplace necessary to ensure sufficient staffing and to enable continuous operations, it is typically a legal obligation under workplace health and safety legislation. In unionized environments workplace health and safety is also addressed under collective bargaining agreements.

The relationship between worker and employer reflects a considerable power imbalance which make it easier to implement new modes of technological surveillance. Resistance is more challenging for employees; whose rights are more limited than those of citizens challenging state actions. Employees may also be reluctant to risk their livelihoods by challenging their employers.

Although it may prove to be easier to implement mandatory COVID-19 surveillance technologies in the workplace, there will still be significant privacy, ethical and human rights issues (Clarke 2020; Knight 2020; Singer 2020). The extent of available recourse for employees may vary considerably from one country to the next and may also depend on whether workplaces are unionized (Kiss & Mosco 2005). Some have raised concerns that workplace surveillance measures introduced for COVID-19 could normalize new forms of employee monitoring (Ravindranath 2020; Bloomberg 2000).

One point of difference is voluntariness. From a national government perspective, making a contact-tracing app voluntary responds to concerns over privacy and civil liberties, and is therefore important to make such apps acceptable (Kahn 2020, Thomson 2020). In a workplace, both the employers' legal obligations to provide a safe workplace and employees' interests in a safe work environment may make mandatory tracking and tracing acceptable – or at least difficult for employees to resist (Chyi 2020; Bond 2020). In deciding how to manage COVID-19 detection and control, employers have a number of different options (Singer 2020). Their choice might depend on the size and resources of the business, the size and deployment of its workforce, and the availability of pre-existing surveillance technologies.

For many businesses, simple and easily available options might be preferable to custom-built solutions. Piggybacking on a free and widely available contact-tracing or exposure notification app might seem to many like a logical step. Thus, one option might be to require employees to download and use the available national or regional contact-tracing app, and to require employees to carry their phones at work, with the app running. This was considered enough of a possibility that one concern with the unrolling of national-level contact-tracing apps was that these apps, although explicitly voluntary in many countries, might become *de facto* mandatory if employers or businesses required their use as a condition either of return to work or entry on premises. This concern was raised in the *Privacy Impact Assessment* (Maddocks 2020) for Australia's contact-tracing app, for example, and it was recommended that the government pass legislation to prevent private sector actors from requiring use of the app. (Maddocks 2020) Such a law was passed in May 2020 (Privacy Amendment (Public Health Contact Information) Bill 2020).

Another option for employers is to leverage existing tracking or surveillance technology for contact-tracing (Howell et al 2020). Workplaces with surveillance cameras, digital pass keys governing access to certain areas, and so on, could leverage these technologies to monitor where employees have been and with whom they may have had contact should someone within the workplace test positive for COVID-19.

Larger corporations with greater resources have the option of building their own apps, sourcing one from app developers, or subscribing to workplace contact-tracing systems offered by companies such as Salesforce (https://www.salesforce.com/ca/products/contact-tracing/overview/). There is an astonishing proliferation of new tracking and tracing technologies for coronavirus in the workplace (Chesler 2020). Employers with their own contact-tracing systems can require employees to either

adopt the prescribed app (if that is the route chosen) or submit to the workplace monitoring scheme, so long as it is consistent with applicable laws. Contact-tracing is simpler within a workplace and easier to justify (Towers-Clark 2020), it is also sometimes more challenging for employees to resist (Chesler 2020).

3.2. Retail Spaces

In some jurisdictions, tracking technologies have been used to monitor access to public spaces such as shopping malls, or transportation systems (Bloomberg 2020). Smart city sensors can be repurposed for contact-tracing purposes, or new monitoring technologies may be introduced (Coronavirus France 2020). For example, those seeking to enter a shopping mall might be required to scan a QR code that would allow them to be notified should it later be determined that someone who was COVID-19 positive was in the same location at roughly the same time. In many Asian cities in particular, such systems have been mandated by government (Gan & Culver 2020, Setboonsarang & Kuhakan 2020). Many retailers and transportation agencies are also deploying thermal cameras (Bloomberg 2020).

Some countries and/or cities repurposed data from surveillance cameras and other urban sources to aid in contact-tracing activities. Transit data from smart cards, for example, can be used to determine who might have been on a specific bus or train at the same time as an infected person. While this ubiquitous tracking raises significant privacy concerns, as does its normalization in a time of crisis, Bouffanais & Lim (2020) suggest that more data about human movement and interaction in cities would greatly assist in understanding how the virus is spread – and by extension how it might better be contained. There is therefore a tension between dealing with the crisis and resisting surveillance creep and a normalized loss of privacy within the smart city.

Of course, technological solutions are not always necessary. Some jurisdictions have also opted for a more basic analog methods of tracking. Ontario, Canada, for example, has asked operators of hair salons and other personal care services to keep a log of customers and contact information to facilitate contact-tracing should an outbreak occur. Many bars and restaurants are doing likewise. The logging of data by private enterprises for the purposes of subsequently sharing this data with contact tracers raises privacy issues that are different but no less important than those raised by contact-tracing apps. Yet compared to the attention paid to digital contact-tracing or exposure notification apps, these practices have received relatively little attention.

4. DISCUSSION

It is interesting to note the disjunction between the broad national and international concern over contact-tracing technologies and their impacts on privacy and civil liberties as compared with relatively limited public attention given to the use of the same or similar technologies to track and monitor people within workplaces, retail outlets or at more local levels in general. There are several possible explanations for this.

4.1. Technology as a Lightning Rod

The global debates – and the tremendous amount of energy expended on developing contact-tracing and exposure notification apps – is interesting, particularly given that it has yet to be determined the extent to which these technologies will be capable of usefully contributing to pandemic responses. MacDonald (2020) argues that much of what has taken place around these apps was "technology theatre"; a distraction focusing attention on a particular, and not necessarily very useful technology, rather than on broader debates of underlying social and public health concerns.

The privacy coalitions that formed around contact-tracing technologies were very much focused on the technologies by which contact-tracing could be carried out, and not on privacy and contact-tracing more generally. Their focus was also on the power dynamics between individuals and the state, rather than on, for example, employer-employee power relationships. A baseline assumption

seemed to be that contact-tracing was a legitimate activity and its impacts on privacy were justifiable; the main issue was to ensure that technologies adopted for contact-tracing did not create additional privacy risks or concerns cast in terms of state surveillance and data security issues.

4.2. Privacy as a Focal Point

Privacy has become a central issue when it comes to technology and has been a focus of considerable attention at the national and international level. From the introduction of the *General Data Protection Regulation* (GDPR) in 2018 to California's new privacy law in early 2020, there has been a great deal of recent legislative activity around digital data protection. In addition, there have been a string of high-profile privacy breaches and scandals accompanied by equally high-profile lawsuits and actions by regulators. There is no question that privacy, particularly in the technological context, is a hot-button issue, and it is one around which there is considerable civil society organization. At the same time, there is substantial legal infrastructure around which to frame and shape privacy arguments that can compel government or private sector action.

The infrastructure and organization around privacy perhaps explains why privacy became a focal point for challenges to contact-tracing apps, leading to the adoption of systems that ultimately did little to directly support manual contact-tracing systems. The focus on privacy deflected attention away from a broad range of other issues relating to the adoption and implementation of contact-tracing or exposure notification apps, including accessibility, transparency, reliability, metrics for success, the ethics of using an untested technology on a vulnerable population, potential adverse impacts on certain communities of false notifications, and so on. In contrast to the legal context for privacy protection, ethics and human rights arguments are more complex, focus more on marginalized communities, special cases, or more remote or intangible harms. Existing legal frameworks for ethical and human rights issues are also less universal, less well articulated in the context of technology, and in many cases far less robust. Focusing on privacy was easy by comparison, and as a result, it dominated discourse.

4.3. National vs. Local

The debates about contact-tracing apps and privacy were very much focused at the national and international level. This may be due to the liberal/libertarian belief that the state should not intrude into the private lives of its citizens. This centres resistance against surveillance on state actions, for example, evoking concerns over increased surveillance in the post 9-11 period. Certainly, in countries with less liberal traditions of government, it was much easier to implement not just digital contract tracing, but a range of other digital surveillance technologies designed to combat the spread of COVID-19.

Rooted as it is in capitalism, the liberal discourse around the relationship between the individual and the state when it comes to privacy and surveillance does not map onto the context of the workplace or to private businesses, where the needs/interests of capital (in the form of employers or business owners) are important factors in the balance against the rights of employees. Indeed, given the diverse nature and size of businesses and the different relationships between employers and employees, the workplace becomes a complex context. Business owners have personal stakes in the business, responsibilities towards shareholders, as well as legal obligations to maintain safe workplaces. Further, the interests of employees are also complex. They may wish to be free of undue surveillance. However, employees have an interest in the viability of a business; they also have an interest in a safe and secure workplace. This is reflected in the legal context, where although there are legal limits on acceptable workplace surveillance, in cases where health and safety are involved there is considerable legal tolerance for different surveillance practices.

Despite the complexity of these relationships, the fact remains that individuals are often at their most vulnerable when it comes to inclusion or exclusion from workplaces, stores or other facilities. Surveillance and control at the local level, especially if relatively unchecked, can lead to considerable

injustice and oppression. The massive protests against police abuse of power in relation to racialized communities around the world highlight the global scale of localized oppression.

Nevertheless, the mobilization of privacy advocates and high-tech companies to arrive at privacy protective solutions for surveillance technologies at the global level has been notably absent at the local level. Employees are relatively powerless when it comes to workplace policies imposed by employers, although where it is present unionization can help to mitigate some of this power imbalance. While human rights legislation may provide individuals wrongfully excluded from commercials spaces or workplaces in some circumstances, the employee must be able to establish that the exclusion was discriminatory, and they generally bear the burden of bringing individual actions. Another phenomenon that seemed to fly well below the organized privacy advocacy radar has been the deployment of more risky and invasive practices at the local level. For example, recording names and phone numbers of all customers of a store or restaurant has more privacy implications than most contact-tracing apps, and far less attention has been paid to secure storage, data limitation, data retention and other privacy issues in relation to these practices. Actions taken at the local level also come from multiple sources and are therefore less easy to organize against than actions taken at the regional or national level. Ubiquitous surveillance – whether at work, on transit in shops, bars, or restaurants – becomes harder to resist, and therefore more easily normalized.

Interestingly, and perhaps ironically, local adoption of these types of technologies may have the promise of much better performance. With a controlled environment and a limited and identifiable group of employees, tracking contacts in case of a reported infection is considerably easier and technology may make the process rapid and effective. The likelihood that a technology will be useful is a factor in evaluating whether its impacts on privacy and other values are justifiable. The case for CT apps in the workplace, therefore, may be stronger than the case for them on a national level. Further, it is interesting to consider whether their use in these more limited and local contexts might actually be sufficient to meet more immediate public health concerns of detecting and limiting the spread of disease.

5. CONCLUSION

The lessons to learn from the debates over the development and adoption of contact-tracing and exposure notification apps are starting to become clearer, although a fuller view will no doubt emerge once the pandemic has come to an end. It is interesting to note how the trajectory of technology-based contact-tracing solutions rapidly shifted from the more controversial use of pre-existing data to the development of new, purpose-specific apps. It also quickly focused on the use of existing devices as a platform for these apps, raising (largely unexplored) questions about access to smartphone technology and the digital divide.

Certainly, the role of tech giants is an important issue as the GAEN platform has several normative features and has created some constraints for national governments. Also interesting is the way in which the development of these apps was driven by preoccupations of privacy advocates. While this strong and relatively well-organized group mobilized quickly and raised important concerns, these tended to focus primarily on state surveillance and malicious attacks, and limited the attention paid to broader ethical concerns. Further, the privacy focus altered the functionality of such apps, moving them away from more directly supporting public health contact-tracing activities. A focus on addressing privacy also deflected attention away from issues of the actual usefulness of such technologies.

The global and national level debates over contact-tracing apps has also shifted attention away from the intensely local nature of the most important contacts in peoples' daily lives. As countries entered the 'return to normal' phase, much hyped-contact-tracing apps began to give way to different strategies for monitoring and recording contacts in workplaces, schools, and retail spaces. Because so much attention was consumed by the debates over national contact-tracing apps, these more diffuse responses have attracted relatively little attention from privacy advocates, even though they do raise

some very significant concerns. The city, with both its private and its public spaces, will no doubt become a focal point for considering strategies to track, monitor and contain the spread of the disease. At the same time, the urban e-planning context is complicated by national and global debates, as well as by the complex relationships of residents with both the state and their employers.

ACKNOWLEDGMENT

The author gratefully acknowledges the research assistance of Ryan Mosoff and Thomas Friedlich, as well as the support of the Scotiabank AI & Society Initiative.

REFERENCES

Agence France-Presse. (2020, June 15). Norway suspends virus-tracing app due to privacy concerns. *The Guardian*. Retrieved from https://www.theguardian.com/world/2020/jun/15/norway-suspends-virus-tracing-app-due-to-privacy-concerns

Amendment, P. (Public Health Contact Information) Act 2020, (No. 44, 2020)(Australia).

Amit, M., Kimhi, H., Bader, T., Chen, J., Glassberg, E., & Benov, A. (2020, May 26). Mass-surveillance technologies to fight coronavirus spread: the case of Israel. *Nature Medicine*. Retrieved from https://www.nature.com/articles/s41591-020-0927-z

Bloomberg. (2020, May 20). Surveillance and monitoring invade European post-pandemic workplaces. *Japan Times*. Retrieved July 17, 2020, from https://www.japantimes.co.jp/news/2020/05/20/world/surveillance-monitoring-europe-coronavirus/

Bond, S. (2020, May 8). Your Boss May Soon Track You At Work For Coronavirus Safety. *National Public Radio*. Retrieved July 17, 2020, from https://www.npr.org/2020/05/08/852896051/your-boss-may-soon-track-you-at-work-for-coronavirus-safety

Bouffanais, R., & Lim, S. S. (2020). Cities— Try to predict superspreading hotspots for COVID-19. *Nature*, *583*(7816), 352–355. doi:10.1038/d41586-020-02072-3 PMID:32651472

Busvine, D., & Rinke, A. (2020, April 26). Germany flips to Apple-Google approach on smartphone contact-tracing. *Reuters*. Retrieved July 16, 2020, from https://www.reuters.com/article/us-health-coronavirus-europe-tech/germany-flips-to-apple-google-approach-on-smartphone-contact-tracing-idUSKCN22807J

CDC. (2020, February 11). *Coronavirus Disease 2019 (COVID-19)*. Retrieved July 16, 2020, from https://www.cdc.gov/coronavirus/2019-ncov/daily-life-coping/contact-tracing.html

Chesler, C. (2020, May 4). Coronavirus will turn your office into a surveillance state. *Wired UK*. Retrieved from https://www.wired.co.uk/article/coronavirus-work-office-surveillance

Chyi, N. (2020, May 12). The Workplace-Surveillance Technology Boom. *Slate*. Retrieved July 17, 2020, from https://slate.com/technology/2020/05/workplace-surveillance-apps-coronavirus.html

Clarke, L. (2020, May 22). Employers face legal minefield over Covid-19 workplace surveillance tech. *New Statesman*. Retrieved July 17, 2020, from https://tech.newstatesman.com/coronavirus/workplace-surveillance-tech-legal

COVID-19 National Emergency Response Center, Epidemiology & Case Management Team, Korea Centers for Disease Control & Prevention. (2020). Contact Transmission of COVID-19 in South Korea: Novel Investigation Techniques for Tracing Contacts. Osong Public Health and Research Perspectives, 11(1), 60–63. doi:10.24171/j.phrp.2020.11.1.09

DP3T. (2000). Retrieved July 16, 2020 from: https://github.com/DP-3T/documents

Daflos, P. (2020, May 22). Credit cards, loyalty programs quietly used in B.C. contact-tracing. *CTV News*. Retrieved May 27, 2020, from https://bc.ctvnews.ca/credit-cards-loyalty-programs-quietly-used-in-b-c-contact-tracing-1.4951402

Dryden, J. (2020, May 01). Alberta declares COVID-19 outbreak at Amazon warehouse near Calgary. *CBC News*. Retrieved July 17, 2020, from https://www.cbc.ca/news/canada/calgary/calgary-amazon-covid-warehouse-outbreak-1.5553126

European Commission. (2020, June 16). *Coronavirus: Member States agree on an interoperability solution.* Retrieved July 16, 2020, from https://ec.europa.eu/commission/presscorner/detail/en/ip_20_1043

Foer, F. (2020 July/August). Big Tech's Pandemic Power Grab. *The Atlantic*. Retrieved July 16, 2020, from https://www.theatlantic.com/magazine/archive/2020/07/big-tech-pandemic-power-grab/612238/

France, C. (2020, May 4). Cameras to monitor masks and distancing in France. *BBC News*. Retrieved from https://www.bbc.com/news/world-europe-52529981

Gan, N., & Culver, D. (2020, April 16). China is fighting the coronavirus with a digital QR code. Here's how it works. *CNN*. Retrieved July 17, 2020, from https://www.cnn.com/2020/04/15/asia/china-coronavirus-qr-code-intl-hnk/index.html

Gasser, U., Ienca, M., Scheibner, J., Sleigh, J., & Vayena, E. (2020). Digital tools against COVID-19: Taxonomy, ethical challenges, and navigation aid. *The Lancet Digital Health*, *0*(0), e425–e434. Advance online publication. doi:10.1016/S2589-7500(20)30137-0

Government of Ireland. (2020). *Privacy and how we use your data*. Retrieved July 16, 2020 from: https://covidtracker.gov.ie/privacy-and-data/

Government of Ontario. (2020). *A Framework for Reopening Our Province: Stage 3*. Retrieved on July 16, 2020 from https://www.hawkesbury.ca/images/2020/mof-framework-reopening-province-stage-3-en-2020-07-13.pdf

Government of Scotland. (2020). *Coronavirus (COVID-19): tourism and hospitality sector guidance*. Retrieved July 16, 2020, from https://www.gov.scot/publications/coronavirus-covid-19-tourism-and-hospitality-sector-guidance/pages/collecting-customer-contact-details

Gov.uk. (2020). *Maintaining records of staff, customers and visitors to support NHS Test and Trace*. Retrieved July 16, 2020 from https://www.gov.uk/guidance/maintaining-records-of-staff-customers-and-visitors-to-support-nhs-test-and-trace

Guy, J. (2020, June 29). Singapore rolls out contact-tracing device for people without smartphones. *CNN*. Retrieved July 16, 2020, from https://www.cnn.com/2020/06/29/asia/tracetogether-tokens-singapore-scli-intl/index.html

Hawkins, D., & Wan, W. (2020, March 8). Health agencies' funding cuts challenge coronavirus response. *Washington Post*. Retrieved from https://www.washingtonpost.com/health/health-agencies-funding-cuts-challenge-coronavirus-response/2020/03/08/73953314-5f0a-11ea-b014-4fafa866bb81_story.html

Howell, C. T., Hoffman, C., & Millendorf, S. M. (2020, May 15). *Reopening and worried you are infecting your employees as they come back to work? The new face of employee workplace surveillance and monitoring in the age of COVID-19*. Foley & Lardner LLP. Retrieved July 17, 2020, from https://www.foley.com/en/insights/publications/2020/05/reopening-employee-workplace-surveillance-covid-19

Jones, R. P. (2020, April 21). OPH to develop digital contact-tracing app. *CBC News*. Retrieved July 16, 2020, from https://www.cbc.ca/news/canada/ottawa/oph-contact-tracing-app-1.5539250

Kahn, J. (Ed.). (2020). *Digital Contact-tracing for Pandemic Response*. Johns Hopkins University Press., doi:10.1353/book.75831

Kharpal, A. (2020, March 26). Use of surveillance to fight coronavirus raises concerns about government power after pandemic ends. *CNBC*. Retrieved July 16, 2020, from https://www.cnbc.com/2020/03/27/coronavirus-surveillance-used-by-governments-to-fight-pandemic-privacy-concerns.html

Kiss, S. J., & Mosco, V. (2006). Negotiating Electronic Surveillance in the Workplace: A Study of Collective Agreements in Canada. *Canadian Journal of Communication*, *30*(4). Advance online publication. doi:10.22230/cjc.2005v30n4a1671

Kitchin, R. (2020). Civil liberties or public health, or civil liberties and public health? Using surveillance technologies to tackle the spread of COVID-19. *Space and Polity*, *0*(0), 1–20. doi:10.1080/13562576.2020.1770587

Kleinman, R. A., & Merkel, C. (2020). Digital contact-tracing for COVID-19. *Canadian Medical Association Journal*, *192*(24), E653–E656. doi:10.1503/cmaj.200922 PMID:32461324

Knight, W. (2020, May 17). Tech Could Be Used to Track Employees—in the Name of Health. *Wired*. Retrieved from https://www.wired.com/story/tech-used-track-employees-name-health/

Lieber, D. (2020, June 9). Israel Halts Controversial Coronavirus Surveillance. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/israel-halts-controversial-coronavirus-surveillance-11591734875

MacDonald, S. (2020, July 13). *Technology Theatre*. CIGI. Retrieved July 14, 2020, from https://www.cigionline.org/articles/technology-theatre

Maddocks. (2020, April 25). *COVIDSafe Application Privacy Impact Assessment*. Retrieved July 17, 2020, from https://www.health.gov.au/resources/publications/covidsafe-application-privacy-impact-assessment

Millar, J. (2020, April 15). Five ways a COVID-19 contact-tracing app could make things worse. *Policy Options*. Retrieved from https://policyoptions.irpp.org/magazines/april-2020/five-ways-a-covid-19-contact-tracing-app-could-make-things-worse/

Molteni, M. (2020, May 7). Why Meatpacking Plants Have Become Covid-19 Hot Spots. *Wired*. Retrieved from https://www.wired.com/story/why-meatpacking-plants-have-become-covid-19-hot-spots/

Nack, C. (2020, June 26). Europe's meat industry is a coronavirus hot spot. *DW*. Retrieved July 17, 2020, from https://www.dw.com/en/europes-meat-industry-is-a-coronavirus-hot-spot/a-53961438

New Zealand Ministry of Health. (2020). *Questions and Answers on NZ COVID Trace*. Retrieved July 16, 2020 from: https://www.health.govt.nz/our-work/diseases-and-conditions/covid-19-novel-coronavirus/covid-19-novel-coronavirus-resources-and-tools/nz-covid-tracer-app/questions-and-answers-nz-covid-tracer

Newton, C. (2020, April 28). How Big Tech is dictating the terms of the coronavirus response to national governments. *The Verge*. Retrieved July 16, 2020, from https://www.theverge.com/interface/2020/4/28/21238633/apple-germany-contact-tracing-exposure-notification-nhs-shin-bet-australia

OIPC. (2020). *ABTraceTogether Privacy Impact Assessment Review Report*. Retrieved July 16, 2020 from: https://www.oipc.ab.ca/media/1089098/Report_ABTraceTogether_PIA_Review_Jun2020.pdf

Osman, L. (2020, May 22). Trudeau says Ottawa will help fund coronavirus contact-tracing across Canada. *Canadian Press*. Retrieved July 16, 2020, from https://globalnews.ca/news/6973077/coronavirus-justin-trudeau-contact-tracing-testing/

PEPP-T. (2020). Retrieved July 16, 2020 from: https://www.pepp-pt.org/

Ravindranath, M. (2020, June 26). Coronavirus opens door to company surveillance of workers. *Politico*. Retrieved July 17, 2020, from https://www.politico.com/news/2020/06/26/workplace-apps-tracking-coronavirus-could-test-privacy-boundaries-340525

Sabbagh, D., & Hern, A. (2020, June 18). UK abandons contact-tracing app for Apple and Google model. *The Guardian*. Retrieved July 16, 2020, from https://www.theguardian.com/world/2020/jun/18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models

Scassa, T. (2020, May 13). *One app per province? How Canada's federalism complicates digital contact-tracing*. Heinrich Böll Stiftung. Retrieved May 15, 2020, from https://us.boell.org/en/2020/05/13/one-app-province-how-canadas-federalism-complicates-digital-contact-tracing

Scassa, T., Millar, J., & Bronson, K. (2020). Privacy, Ethics, and Contact-tracing Apps. In *Vulnerable: The Law and Policy of COVID-19*. University of Ottawa Press. https://ruor.uottawa.ca/handle/10393/40726

Scheck, T., & Hing, G. (2020, April 28). *Public Health Labs Suffered Budget Cuts Prior To The Coronavirus Pandemic*. National Public Radio. Retrieved July 16, 2020, from https://www.npr.org/2020/04/28/845484900/public-health-labs-suffered-budget-cuts-prior-to-the-coronavirus-pandemic

Setboonsarang, C., & Kuhakan, J. (2020, May 17). Thailand opens malls after nearly two months amid coronavirus outbreak. *The Guardian*. Retrieved July 17, 2020, from https://www.theguardian.pe.ca/news/world/thailand-opens-malls-after-nearly-two-months-amid-coronavirus-outbreak-450711/

Simmons-Duffin, S. (2020, May 7). States Nearly Doubled Plans For Contact Tracers Since NPR Surveyed Them 10 Days Ago. *National Public Radio*. Retrieved July 16, 2020, from https://www.npr.org/sections/health-shots/2020/04/28/846736937/we-asked-all-50-states-about-their-contact-tracing-capacity-heres-what-we-learne

Singer, N. (2020, May 11). Employers Rush to Adopt Virus Screening. The Tools May Not Help Much. *The New York Times*. Retrieved from https://www.nytimes.com/2020/05/11/technology/coronavirus-worker-testing-privacy.html

Taylor, J. (2020, May 6). Covidsafe app is not working properly on iPhones, authorities admit. *The Guardian*. Retrieved from https://www.theguardian.com/world/2020/may/06/covidsafe-app-is-not-working-properly-on-iphones-authorities-admit

Thomson, S. (2020, June 5). Opt in or opt out? Officials face difficult ethical decision over COVID-19 contact-tracing apps. *National Post*. Retrieved July 17, 2020, from https://nationalpost.com/news/opt-in-or-opt-out-officials-face-difficult-ethical-decision-over-covid-19-contact-tracing-apps

Towers-Clark, C. (2020, June 17). Is Contact-tracing A Public Or Private Concern? *Forbes*. Retrieved July 17, 2020, from https://www.forbes.com/sites/charlestowersclark/2020/06/17/is-contact-tracing-a-public-or-private-concern/

van Kolfschooten, H., & de Ruijter, A. (2020). COVID-19 and privacy in the European Union: A legal perspective on contact-tracing. *Contemporary Security Policy*, *41*(3), 478–491. doi:10.1080/13523260.2020.1771509

Vaudenay, S. (2020). *Centralized or Decentralized? The Contact-tracing Dilemma* (No. 531). Retrieved from https://eprint.iacr.org/2020/531

Warnica, R. (2020, June 23). *Public Health Ontario suffered exodus of senior leaders and budget cuts before the COVID-19 pandemic struck*. National Post. Retrieved July 16, 2007, from https://nationalpost.com/news/canada/covid-19-public-health-ontario-budget-cuts

ENDNOTES

[1] Apple/Google, Privacy Preserving Contact-tracing, https://www.apple.com/covid19/contacttracing.

[2] Apple, Exposure Notification Addendum, https://developer.apple.com/contact/request/download/Exposure_Notification_Addendum.pdf.

Teresa Scassa (PhD) is the Canada Research Chair in Information Law at the University of Ottawa, where she is also a professor at the Faculty of Law. She is the author or co-author of several books on intellectual property and technology law subjects. She is a past member of the External Advisory Committee of the Office of the Privacy Commissioner of Canada, and of the Canadian Government Advisory Committee on Open Government. She is a member of the GEOTHINK research partnership, and has written widely in the areas of intellectual property law, law and technology, privacy, and open government.