Since January 2020 Elsevier has created a COVID-19 resource centre with free information in English and Mandarin on the novel coronavirus COVID-19. The COVID-19 resource centre is hosted on Elsevier Connect, the company's public news and information website.

Elsevier hereby grants permission to make all its COVID-19-related research that is available on the COVID-19 resource centre - including this research content - immediately available in PubMed Central and other publicly funded repositories, such as the WHO COVID database with rights for unrestricted research re-use and analyses in any form or by any means with acknowledgement of the original source. These permissions are granted for free by Elsevier for as long as the COVID-19 resource centre remains active.

International Journal of Information Management 55 (2020) 102178

Contents lists available at ScienceDirect

International Journal of Information Management

journal homepage: www.elsevier.com/locate/ijinfomgt

Opinion Paper

Contact tracing apps and values dilemmas: A privacy paradox in a neo-liberal world

Frantz Rowe

University of Nantes, LEMNA and SKEMA Businesss School, Nantes, France

ARTICLE INFO

Keywords:
Contact tracing apps
Privacy paradox
Freedom of movement
Technology of the self
Health

ABSTRACT

Contact tracing apps are presented as a solution, if not the solution, to curb pandemics in the Covid-19 crisis. In France, despite heated public institutional debate on privacy related issues, the app was presented by government as an essential benefit for protecting health and lives, thus avoiding both politicians and citizens to feel morally responsible and looking guilty, and as essential to recover our freedom to move. However we argue that, while detection of cases have still not been reported after 10 days and one million app downloads - a situation comparable to Australia who launched its app a month before -, the adoption of the app generates important risks to our informational privacy, surveillance and habituation to security policies. It also may create discrimination, distrust and generate other health problems such as addiction and others as 5G technology continues to be deployed without prior impact studies. Finally the smartphone app against covid epidemics appears as an extreme case of the privacy paradox where the government plays on the immediate benefits and downplays long-term concerns while inducing a technology of self. Contact tracing apps may become an emblematic case for digital transformation and value changes in the western world.

1. Introduction

«No contact tracing, no lockdown lifting » said Dr Véran, the French government Health Minister, on May 6th at the Senate debate on the "stop-covid" app. The power of this crisp formula seemed clear: the app is a means to the end of reconquering our freedom of movement. Yet it was ambiguous and senators rejected it then before approving it on may 27th. The ambiguity resorts to a debate on values where individual privacy is at risk of being crushed and where surveillance is looming, an important issue in a country who puts liberty first on its motto. In France, as in many countries, the idea of building a mobile app that would inform a smartphone user if she/he crossed the way of contagious individuals has led the French government to add this protection method to the traditional contact tracing method by human investigation that is generally used when an epidemic develops. In general, contact tracing methods enable the State to identify contagious individuals, notably presymptomatic and asymptomatic ones, and isolate them before they spread the pandemic further. With the smartphone app method, they would be informed that they crossed someone who was contagious if they stayed more than 15 min at less than one meter from one another, so not respecting the "social distancing" protection rule. They can be informed up to 15 days after the encounter as the disease may take time to develop. Such contacts happen in many situations, especially in public transportation or with relatives or good friends who may ignore for a moment that they have Covid-19.

The app potentially offers several advantages over the traditional method for contact tracing. The latter rests on traditional snowballing interviews with infected people to identify who they interacted with in the past days. Specifically, tracing cost is much lower if individuals are automatically detected as prospective cases. Most importantly, an app can help identify more quickly and more comprehensively the infected individuals who were in contact with a person if both were carrying their smartphones with the app. It is estimated that on average the method is three days faster than the traditional method assuming that the tracking brigades are not overwhelmed. These advantages are key when an epidemic moves fast and has severe consequences, such as a potentially huge death toll and social and economic crisis (Ferretti et al., 2020). At the time we write France has had nearly 30,000 deaths due to covid-19 and 22 other countries have started develop a similar app. For example Austria and Australia launched their apps a couple of months before but despite the benefits the launch was considered a failure. Beyond technical reasons that may explain this negative outcome, and from which France and other following countries could learn, concerns for privacy may still prevail in France where a culture on data privacy has been built for more than 40 years and prevent this identification and preventative method to be a success.

E-mail address: frantz.rowe@univ-nantes.fr.

https://doi.org/10.1016/j.ijinfomgt.2020.102178
Received 14 June 2020; Accepted 14 June 2020
Available online 30 June 2020
0268-4012/ © 2020 Elsevier Ltd. All rights reserved.

In this opinion paper we will first present conditions for the app to be effective. We then highlight the value dilemmas. In particular we notice that it provides an original illustration of the privacy paradox (Kokolakis, 2017). The French government and people value privacy, but in the current crisis, they may prefer immediate benefits. Consequently they expose themselves to hacking risks and surveillance related to technology vulnerability and monitoring. We then highlight that this calculus is influenced by the public debate at institutional level and interpret technology and responsibility in a Foucauldian perspective as a technology of self in a neo-liberal world. In the fourth section we then give our opinion which largely overlaps with that of La Quadrature du Net, a French organization similar to Freedom on The Net. We highlight that not only privacy would be harmed, but risks such as potential surveillance and habituation to security policies, discrimination, distrust and generate other health problems in the long-term may develop. We conclude with practical and research implications.

2. Critical conditions for the effectiveness of the app

Numerous conditions are critical to predict that the mobile app method of infected individuals identification will be effective. Notably:

1) Correct information qualifying individuals as infected and contagious requires that population be tested and that tests are not error-prone,
2) High likelihood that when a contagious person meets or crosses another person an infected person both parties have a smartphone,
3) A very high proportion of smartphone users download the app.

That these conditions be all met is very unlikely.

The first condition would require a testing capacity that France did not have before mid-may. With testing capacity clearly below one million per week how can we control at individual level the infection and/or contagious level of a 67 million population? On May 27,th at parliament, Dr Véran presented findings of a recent study indicating that 46 % of pre-systematic individuals contribute to the reproduction of the disease as an argument in favor of the app (Ferretti et al., 2020). But the effectiveness of the app presupposes that the health system and a corresponding IS records who is infected and when infection occurred. We can still cross the way of people who are contagious and have not been tested precisely because a large share of infected individuals are still asymptomatic and ignore it. The second condition can be met if the population is largely equipped with smartphones and if all those in contact in their daily encounters carry their smartphones. This is unlikely even if in France 77 % of the population is equipped with a smartphone (La Quadrature du Net, 2020a). In fact, while when people travel, they take their phone with them in order to face any uncertainty related to traffic jam or delays on public transportation, when at destination, at their office or at their relatives they may keep their phone in a jacket or a bag and visit people or colleagues or go to meetings without them. Thus, people do not always carry their smartphones with them and this makes the traditional method of contact tracing still necessary. The third condition is that a significant share of smartphone owners may want to trade a potentially higher safety for themselves and others for their higher vulnerability to security breaches when they allow Bluetooth and subsequent privacy issues. However wishing to limit these issues, in France, unlike other countries (e.g. Norway), government chose Bluetooth against geolocation by GPS.

Being more cost efficient and, if effective, of interest as a complementary means for isolating contagious people and increasing individual and public health, the app does not come without short-term and long-term risks of privacy and surveillance. Maybe for some this will be a real tradeoff while for others privacy is long gone with the digital and e-commerce (Spiekermann, Grossklags, & Berendt, 2001); they enjoy knowing that their friends and whoever else knows what they do. In sum, for those, private life has gone public with the internet.

Like cell phones, the tracing app offers both positive externalities (any individual is better protected from a health viewpoint when others also have it if they keep their phones with them) and negative externalities (the more others activate Bluetooth in high population density areas such as malls or public transportation, the greater the risk of malevolent action for those who have bad intentions have it on already). However from a public policy viewpoint the value of positive externalities grows exponentially only when a very large share of the population has adopted the app and claim has been made at Parliament on May 27th by Cédric O, Secretary of State that a threshold of 56 % of the population is sufficient, absent of masks, lockdown and tests to curb the pandemics.[1] Contrary to what Dr Véran and Mr O claimed, the conclusions from one of the most advanced epidemiological study taking into account the benefit of a contact tracing smartphone app (Ferretti et al., 2020) neither meant that, without the app, lock-down would continue, nor that other preventative measures should be dropped but that an app similar to what was proposed by the Oxford team would help control the disease. However the team noted that “The app should be one tool among many general preventative population measures such as physical distancing, enhanced hand and respiratory hygiene, and regular decontamination. » (ibidem).

3. A societal choice: values dilemmas, responsibility and neo-liberal thinking

3.1. A privacy paradox: data privacy vs freedom and health

The dilemma(s) we face are about the values that we choose (Rowe, 2018). Most of the time these dilemmas are treated within an organization or a profession (e.g. RFID tags for librarians in various management processes concern efficiency and security vs privacy (Thornley, Ferguson, Weckert, & Gibb, 2011), but they are rarely exposed at the level of a nation with impact on everyone’s life. While privacy is a fundamental human right, freedom to move and safety are also fundamental. The dilemmas here are not only between health and privacy (Harari, 2020), between freedom to move and data security and privacy, but also between who and what to protect. Contact tracing apps may bring higher health safety for others, and particularly for the elderly (since mortality of those infected by covid-19 essentially affects people over 65), and would contribute to allow the economy to restart, as emphasized by Dr Véran, for the risk of overwhelming the health system would diminish. Under the circumstances health professionals would also reduce their own risk of becoming infected. Presented like this, the privacy breaches risk may look minor and the two sides of the dilemma do not weigh equally. Otherwise put the covid crisis may be a nice illustration of the privacy paradox which states that we generally value privacy, but when we have an opportunity we are ready to trade it for something else (Kokolakis, 2017).

This feeling may be even confirmed when one looks at the public debate on privacy issues and the efforts apparently made to surface privacy issues and mitigate corresponding risks. In France, in Germany, in the UK, in Belgium and in most western countries privacy issues related to the design of these « stop-covid » app have seemingly been addressed both at technical level and at institutional level. Technically and from an IS viewpoint, while many countries around the world have developed mobile apps for contact tracing, the design features have fueled heated typical IS debates regarding whether stored data should be decentralized or centralized, which data should be stored and more largely, about data governance. Regarding governance, the French government rejected the idea that the algorithm for identification of an infected contact be developed by Apple or Google or any foreign company. It made it an issue of national sovereignty to try to regain trust of citizens who may otherwise fear that their personal and health

[1] This claim is based on the report to the NHS (Hinch et al., 2020) co-signed by many of the members of the Oxford team who published in Science (Ferretti et al., 2020). However the Science publication is far more cautious.

data may be monetized by tech giants.

Turning to institutional level, France and many other European countries are very sensitive to privacy issues (Miltgen & Peyrat-Guillard, 2014) and privacy is protected by law. For instance, long before the advent of GDPR, the Commission Nationale Informatique et Libertés (CNIL) was set up in 1978 in France, to protect our digital privacy. Furthermore the right to be forgotten was applied in France long before GDPR (2010). Despite the declared State of Urgency/ Emergency the government chose to bring the debate in front of parliament and could not proceed without the legal advice (although not binding) of CNIL who finally gave a favorable recommendation for the stop-covid app on May 26th and for the Information Systems that were set up also for contact tracing when following the traditional method. It did so after considering that: 1) no personal data would be collected from the app without being encrypted and anonymized, 2) the exchange protocol named Robert would not be based on Apple or Google technology but developed by INRIA, the National Research Institute that specializes on computing and automation.

3.2. Who is morally responsible?

The French government and people value privacy, but in the face of human suffering and losses due to health, they may opt for the immediate benefits of the app: freedom to move and not having to feel morally responsible and looking guilty of as politicians rejecting a technique that could save lives. However, this choice is made at the expense of privacy; even if in France geolocation with GPS was rejected for this reason. In fact, bluetooth technology is notoriously fraught with data breaches, and data breach vulnerability considered a risk to data privacy (Culnan & Williams, 2009). The privacy paradox is more multifarious and complex than it seems (Kokolakis, 2017). Privacy itself and related policy is also heavily influenced by political choices related to various stakeholders' interests (Introna & Pouloudi, 1999). Here it is not exactly a calculus between the expected loss of privacy and the immediate gain of information disclosure (Dinev & Hart, 2006; Xu, Luo, Carroll, & Rosson, 2011) that the government think people will make, but a calculus taking into account their need for freedom to move and their feelings about moral responsibility and guilt due to the evolution of the pandemics. For government and parliament representatives themselves the calculus may be a between reducing their risk of looking inactive and bearing similar moral responsibility (with higher social pressure since their decisions are public) if the pandemics is less controlled than in countries where the app has been adopted on the one hand; and being attacked for pursuing a surveillance policy and infringing upon data privacy on the other hand.

3.3. A technology of the self in a neo-liberal world

However, even if taking account stakeholders' interest we may still at this stage conclude that the two sides of the dilemma do not weigh equally. So why this fuss about privacy? Isn't it over with the dilemma? My own opinion and that of many other digital specialists in France is that, while the "stop-covid" app has been released in France like many other apps in the world pursuing the same contact tracing goal, and whatever the design choices they embed – centralized as in France and the UK or decentralized as in Germany, independent from Apple and Google as in the UK and in France or not, using GPS or bluetooth – these apps are more dangerous than they seem and the values dilemmas persist. Not only is privacy endangered and we move towards a surveillance society, but long term health risk are also significant if the app is widely accepted. To control the pandemics with this app people would voluntarily request to be tested and would self quarantine. By making the choice of voluntary rather than compulsory adoption of the app the government reinforces self-discipline in the population. Because it is necessary to carry smartphones close to our body to make the detection process and calculation of distance more effective, we argue that this contact tracing app can be interpreted as a technology of the self in a neo-liberal thinking, included in governmentality (Foucault, 1993; Lemke, 2001), a biopower self-disciplining our bodily behavior and reinforcing self-discipline in a Foucauldian sense (Leclercq-Vandelannoitte, 2014), but also creating long-term risks including for society and for our health.

4. An opinion informed by a LA Quadrature du Net and longer-term concerns

My humble opinion is very similar to that of La Quadrature du Net (LQdN), an independent association that generally defends privacy and fights against trends towards the advent of a surveillance society, but also goes further in that it considers other long term negative consequences such as health and exclusion/discrimination consequences related to more intense smartphone use.

In its opinion LQdN approves the position of CNIL who expressly demanded that government demonstrate the practical utility of stop-covid, while regretting that, given its illusory benefits, CNIL did not purely and simply asked the French government « to stop this dangerous and useless project and gets lost in the false debate about deceptive warrants to delineate the use of the app » (La Quadrature du Net, 2020b). On april 14th LQdN sent to parliament its own arguments against post-covid. The main argument is that we can very cautiously agree to limit our freedoms ONLY when there are strong proven benefits, which is not currently the case and will not be, because, as we explained above, stop-covid effectiveness is very uncertain essentially due to a) too low predicted app and smartphone use[2] and b) too low data quality related to false positives (i.e. being informed that someone we crossed was contagious when this person was not (to reduce this risk people will have to enter a QR code in the app) or when the person (e.g. a doctor) was already informed prior to the encounter and protected herself and false negatives (e.g. not identifying the risk in the absence of sufficient disease testing capacity and due to not detecting beyond one meter as in France). From an ethical viewpoint CNIL considered that collected data will be fitting the definition of data minimisation regarding data privacy. Data minimisation means that data collection should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. However, given our previous remark, we would argue that data minimisation is not met for multiple reasons: there will be multiple false positive/negative (relevance), the scope of data collection is too large and too loosely defined (purpose)[3], the analysis and future use of biometric data are not

[2] Detection of cases have still not been reported after four days its launch on june 2nd and one million app downloads - a situation comparable to Australia who launched its app a month before France. In Australia with 6 million downloads only one case was detected!

[3] Scope at best is unclear and not well delineated. On the one hand there are three applications in charge of fighting the pandemics at national level in France: 1) « Stop-covid » on the smartphone that notifies a potential risk to the user. 2) « SI-DEP » (Système d'Informations de DEPistage) that records all the results of labs who test COVID-19 and whose purpose is to make sure that all positive cases are taken care of. 3) « Contact-COVID » whose purpose is to identify the contacts of a covid-19 case and to make sure that each and everyone has been called, informed, tested and coached. Stop-covid is not related to the other two apps (no triangulation). On the other hand, concerns remain at the portfolio of applications level : 1) any « Contact-Covid » and « SI-DEP » even if anonymized can be hacked. In short the privacy risk of stop-covid itself may not be considered important, but this risk should be assessed for any contact tracing application like contact-covid. In this respect little is known about how contact-covid is operated. 2) It remains that increased surveillance, habituation to security policy, health issues related to more permanent carrying of smartphone and addiction are serious risks specifically related to stop-covid with little predicted effectiveness if we examine the conditions for its success. Source : https://solidarites-sante.gouv.fr/soins-et-maladies/maladies/maladies-infectieuses/coronavirus/tout-savoir-sur-le-covid-19/article/contact-covid-et-si-dep-les-outils-numeriques-du-depistage-covid-19.

properly addressed (adequation)[4] . With regards to health safety LQdN adds that the stop-covid app may even prove counter-effective either with people feeling safe when they are not and stop behaving cautiously[5] or with people hiding their symptoms in fear that they be discriminated.

Interestingly, not only short-term benefits are illusory, but negative long term risks abound, not only for privacy. LQdN (La Quadrature du Net, 2020a) notes three types of risks for our freedom:

- People could be discriminated if the app was to be compulsory or if social pressure towards adoption becomes too high; a particular case of discrimination being access to blood testing being conditioned by its adoption (On this first type of risk CNIL felt that government had taken appropriate measures hence its final favorable recommendation);
- Increased surveillance will be facilitated if the app is adopted by a large share of the population; and anonymity is simply impossible as it runs counter to the very objective of the app which is to inform targeted persons. Hence the need for pseudonyms which can not be very effective against malevolent action (Bonnetain et al., 2020) and individual surveillance.
- Habituation to security policies that curtail our freedoms and social acceptability of digital surveillance based on the blind belief of technology as solutions to social problems.

I do not wish to paint a bleak picture of the situation but the very last argument can be completed in two ways. First, the haste to develop contact tracing apps evokes pure technological solutionism that runs completely against all socio-technical lessons from IS and other socio-technical disciplines. It is not hard to guess that the tech industry and government are not innocent in this state of affairs. As La Quadrature du Net (2020a) notes this is sad because there are much more important actions for government to undertake including to fight pandemics and its consequences.

Second, such smartphones tracing apps would inevitably reinforce the ubiquitous use of smartphones in the population who is not educated to the complexity of the dark side of IT (D'Arcy, Gupta, Tarafdar, & Turel, 2014), pushing them to carry them permanently on the body. Why inevitably? Even if the app is not massively adopted, this announcement sends the signal that in order to combat risks the government and society must be digitally oriented and this exerts pressure towards adoption and use. What will happen when technologies that are also highly contentious like 5 G come without impact studies? It is notorious that adolescents are already prone to some forms of problematic smartphone dependency (Gentina & Rowe, 2020). Do we want them to turn into real addicts and not let them be able to discern what could be suitable for them in their daily life and inevitably beyond? More importantly adolescents are unaware about privacy issues and such apps reinforce the message that personal data do not belong to you, that tracking trips is not problematic and legitimizes that this can be done by any government.

5. Implications for research and practice

As academics in our multiple activities we have an important role to play to contribute to better public project decisions like these who are critical both on the short-term and on the long-term. Our first role is to raise awareness on the situation by offering an hopefully different yet interesting interpretation. Then, it is to act more directly to contribute to relevant efforts by teaching and research in a way which is suited to the evolving situation.

Contact tracing apps may become an emblematic case for digital transformation and value changes in the western world. We see the contact tracing as an original if not extreme case of the privacy paradox (Kokolakis, 2017) because in studies of the informational privacy paradox a) smartphones apps, or b) location data have rarely been studied ((Egelman, Felt, & Wagner, 2012) and (Zafeiropoulou, Millard, Webber, & O'Hara, 2013) being exceptions) and because here the dilemma is not at the level of an executive, an organization or a profession, but at the level of all countries who are launching such apps and potentially to the world! In such context no active personal information disclosure is used contrary to the vast majority of the privacy paradox literature; only metadata about our location and having been in contact or not with an infected person is monitored. What is activated through self-discipline are the opening of Bluetooth and the consent to be tested and to self-quarantine if the person crossed someone infected. However it is voluntary and at all the stages of the process citizens are made responsible for their health and public safety, an important issue in governmentality: if this stop-covid preventative method for avoiding to spread the disease is not effective government won't be to blame, people will be responsible. Our interpretation is that, consciously or not, the government plays on the immediate benefits and downplays long-term risks in the equation considered by the privacy paradox while inducing self-discipline. As a consequence this case is also an opportunity to research changing bodily behavior of stop-covid adopters (Chughtai, 2020; Leclercq-Vandelannoitte, 2014) and assess risks if the app lives long enough.

Unfortunately for the reasons we explained in the first section of this paper, this tactic is not even going to be effective from a public health viewpoint. For our academic community, fighting solutionism in this context requires developing awareness of ethical concerns and calls for future research on the ethics of digital governance (Markus, 2016) (e.g. on conditions where data sharing would be really useful (and there are plenty such as the project of health data hub which is about the sharing of health data to help discover new treatments for all sorts of deadly and rare disease). It also suggests insisting on every occasion on our socio-technical identity as a discipline and introducing some moral philosophy or ethics into IS curricula (Markus, Marabelli, & Zhu, 2019). As suggested above there is a need to study institutions (government, parliament, justice) and industry actors positions and interests and not to focus only on the smartphone app. Beyond data governance of this app, various socio-technical systems should be studied, included the traditional contact tracing systems such as contact-covid and how it is enacted with stakeholders. Beyond the opposition between the market (Big tech companies) and the State, community governance ought to be considered.

While there is a tradition of research tracks on privacy in most IS conferences, it is important that related problems be not treated only technically (e.g. How to respect confidentiality or anonymity when one collects personal data?) but to truly address both a) values dilemmas including by providing some philosophical background with a critical theoretical stance when possible (Introna & Pouloudi, 1999) and b) risks and negative consequences related to the design (e.g. Solove, 2006; Thornley et al., 2011). Most importantly ethical concerns should not be last or a supplement to the design but integrated from the beginning with equal power to those in charge of enforcing it to those with a more technical profile, regardless of whether "privacy by design" has been claimed as is the case with the INRIA team who is responsible

[4] Strangely the law says nothing for instance about thermal cameras that have already been installed at CDG airport. Normally those who have high temperature should then have their temperature confirmed and be tested if necessary. If positive this information will be added to SI-DEP. It does not say much about the myriad of sub-contactors who work on such a centralized system albeit the three apps are separate and who could also lead to data leaks. Source : https://www.legifrance.gouv.fr/eli/loi/2020/5/11/PRMX2010645L/jo/texte.

[5] This argument has also been used by the French government for masks. However people are not stupid: it is not because they put their seat belt on that they speed up.

for the app development. Regarding adoption decisions, equal importance should be given to risks (Gibb, Thornley, Ferguson, & Weckert, 2011; Introna & Pouloudi, 1999) and ethics (Mingers & Walsham, 2010) as it is to strategic alignment, profitability, ease of use and usefulness.

Finally, we fear that youngsters will get used to no privacy even more than now and will let surveillance generalize by industry itself with no precaution. Intelligent agent and smartphone providers are already jumping on the opportunity (Brewster, 2020). Future generations must protect data privacy which took French and Europeans 40 years to build! However it is our task to also educate them to defend their privacy and be critical when receiving appealing commercial offers and invited to participate to local and national governments projects.

6. Conclusion

As IS specialists our temptation, and sometimes our trap, is to contribute to the main ongoing and visible debate about what design feature is best and there are always pros and cons for any application and needs in our changing world. But we should also step back and interrogate these apparent needs and strive to see the ethical or moral dilemmas that are often hidden or not really addressed because opponents voices are unheard; covered by those disproportionally richer, vocal and influential and whose interest is to present technology as the solution to our problems. The world we build with technologies incorporates irreversible trends that are part of the digital transformation. We can not make choices for others but we can inform society when we see the dangers and make more conscious choices when we face dilemmas such as the apparent one between privacy and health (Harari, 2020). Opting systematically for the latest technology does not necessarily means progress but could mean being under influence. Although hardly hit by covid-19 Belgium decided all the more courageously to only use the traditional contact tracing method.

As INRIA researchers team note (Bonnetain et al., 2020), the first article of CNIL has not aged a bit: “IT must serve each citizen [.. .]. It must undermine neither human identity, nor human rights, nor private life, nor individual or public freedoms ».

Acknowledgment

I am grateful to Maguelone Destang, Tamara Dinev, Ojelanki Ngwenyama and Jean-Loup Richet who made some good comments on previous version of this paper.

References

Bonnetain, X., Canteaut, A., Cortier, V., Gaudry, P., Hirschi, L., Kremer, S., et al. (2020). *Le traçage anonyme, dangereux oxymore : Analyse de risques à destination des non-spécialistes.* Working paperhttps://risques-tracage.fr/.

Brewster, T. (2020). *Exclusive: Warning over Chines mobile giant Xiaomi recording millions of people's private web and phone use.* April 30th 2020, (Accessed June 1st)Forbeshttps://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/#6dc4c3a01b2a).

Chughtai, H. (2020). Taking the human body seriously. *European Journal of Information Systems*. https://doi.org/10.1080/0960085X.2020.1746202.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: Lessons from the Choicepoint and TJX data breaches. *MIS Quarterly, 33*(4), 673–687.

D'Arcy, J., Gupta, A., Tarafdar, M., & Turel, O. (2014). Reflecting on the 'Dark Side' of information technology use. *Communications of the Association for Information Systems, 35*(1), 109–118.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for e-commerce transactions. *Information Systems Research, 17*(1), 61–80.

Egelman, S., Felt, A. P., & Wagner, D. (2012). Choice architecture and smartphone privacy: There's a price for that. *Proceedings of the 11th Annual Workshop on the Economics of Information Security*.

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.

Foucault, M. (1993). About the beginning of the hermeneutics of the Self' (Transcription of two lectures in Darthmouth on Nov. 17 and 24, 1980), ed. by Mark Blasius. *Political Theory, 21*(2), 198–227.

Gentina, E., & Rowe, F. (2020). Effects of materialism on problematic smartphone dependency among adolescents: The role of gender and gratifications. *International Journal of Information Management*. https://doi.org/10.1016/j.ijinfomgt.2020.102134.

Gibb, F., Thornley, C., Ferguson, S., & Weckert, J. (2011). The application of RFIDs in libraries: An assessment of technological, management and professional issues. *International Journal of Information Management, 31*(3), 244–251.

Harari, Y. N. (2020). *The world after coronavirus.* Financial Times March 20th.

Hinch, R., Probert, W., Nurtay, A., Kendall, M., Wymant, C., Hall, M., et al. (2020). *Effective configurations of a digital contact tracing app: A report to NHSX*.

Introna, L., & Pouloudi, A. (1999). Privacy in the information age: Stakeholders, Interests and Values. *Journal of Business Ethics, 22*(1), 27–38.

Kokolakis, S. (2017). Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security, 64*(C), 122–134.

La Quadrature du Net (2020a) https://www.laquadrature.net/2020/04/14/nos-arguments-pour-rejeter-stopcovid/.

La Quadrature du Net (2020b) https://www.laquadrature.net/2020/04/27/la-cnil-sarrete-a-mi-chemin-contre-stopcovid/.

Leclercq-Vandelannoitte, A. (2014). Interrelationships of identity and technology in IT assimilation. *European Journal of Information Systems, 23*(1), 51–68.

Lemke, T. (2001). "'The birth of bio-politics'" – Michel Foucault's lecture at the Collège de France on neo-liberal governmentality. *Economy and Society, 30*(2), 190–200.

Markus, M. L. (2016). Obstacles on the road to corporate data responsibility. In C. R. Sugimoto, H. R. Ekbia, & M. Mattioli (Eds.). *Big data is not a monolith: Policies, practices and problems* (pp. 143–161). Cambridge, MA: The MIT Press.

Markus, M. L., Marabelli, M., & Zhu, X. (2019). POETs and quants: Ethics education for data scientists and managers. *3rd RICK Workshop of Information and Organization*.

Miltgen, C. L., & Peyrat-Guillard, D. (2014). Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems, 23*(2), 103–125. https://doi.org/10.1057/ejis.2013.17.

Mingers, J., & Walsham, G. (2010). Towards ethical information systems: The contribution of discourse ethics. *MIS Quarterly, 34*(4), 833–854.

Rowe, F. (2018). Being critical is good, but better with philosophy! From digital transformation and values to the future of IS research. *European Journal of Information Systems, 27*(3), 380–393.

Solove, D. J. (2006). A taxonomy of privacy. *University of Pennsylvania Law Review, 154*(3), 477–560.

Spiekermann, S., Grossklags, J., & Berendt, B. (2001). E-privacy in 2nd generation E-commerce: Privacy preferences versus actual behavior. *Proceedings of the 3rd ACM Conference on Electronic Commerce*.

Thornley, C., Ferguson, S., Weckert, J., & Gibb, F. (2011). Do RFIDs (radio frequency identifier devices) provide new ethical dilemmas for librarians and information professionals? *International Journal for Information Management, 31*(6), 546–555.

Xu, H., Luo, X. R., Carroll, J. M., & Rosson, M. B. (2011). The personalization privacy paradox: An exploratory study of decision making process for location-aware marketing. *Decision Support Systems, 51*(1), 42–52.

Zafeiropoulou, A. M., Millard, D. E., Webber, C., & O'Hara, K. (2013). Unpicking the privacy paradox: Can structuration theory help to explain location-based privacy decisions? *Proceedings of the 5th Annual ACMWeb Science Conference*.