Coda: Slow Computing During a Pandemic

The coronavirus pandemic started to sweep across the globe just as this book was going to press. All aspects of daily life changed once delay, and then containment measures, were put in place. Initially, closing down most workplaces and schools and restricting movement seemingly created new scope for people to practise slow computing. Rather than dashing here and there, trying to cope with a crowded diary and too many tasks, those people not on the frontline would be static and confined to the home. Life would become stationary, routines broken, busyness reduced, and work-life balance restored. However, the scope for pursuing slow computing is now in question like never before.

In many ways our lives have become even more digitally-mediated. In our own cases, at very short notice we had to pivot our teaching from face-to-face contact on our university campus into virtual classes. New knowledge and skills had to be acquired about new pedagogies and platforms (Teams, Skype, Zoom, Moodle, etc). Classes and meetings were to be conducted from home. Social interactions with family and friends shifted to video calls, WhatsApp and Facebook. Information was elicited through social media and news sites. Streaming services replaced out-of-home social activities. Our time was still fragmented and interleaved, and rather than our sense of stress being lowered, it was heightened by the sense of isolation and the fear and anxiety expressed through our media channels. We thus tried to follow our own slow computing advice by limiting the use of social media and making sure to do non-digitally mediated activities: exercise, cooking, gardening, reading, playing traditional games.

We're fortunate. For some of our colleagues (and also our students), the new digital realities of working at home have posed

acute challenges. Many were left looking after bored, cooped-up children who needed home schooling, play and reassurance. They've had to cope with family-wide fights over who will use the computer. New skills have been acquired to access and install software and work out how to use new services. Some have quite limited access to broadband internet. Other workers have not been allowed to self-isolate due to the nature of their job, performing essential work. In many cases, this work has intensified due to increased demand or the stress of trying to deliver it in difficult circumstances. At the same time, many of these essential workers are trying to deal with organizing childcare or other care duties when schools and crèches are closed and services limited. And in many jurisdictions they are doing this work with little protection against infection or access to needed health insurance. Others still have found themselves out of work at short notice and scrambling to negotiate government websites to access welfare and unemployment benefits.

In addition, new social and technological arrangements that amplify surveillance and data extraction practices have started to emerge in an effort to halt the spread of the pandemic virus. Led by governments and companies, these technologies have been rolled out for five primary purposes: (1) quarantine enforcement/movement permission (knowing people are where they should be, either enforcing home isolation for those infected or close contacts, or enabling approved movement for those not infected); (2) contact tracing (knowing whose path people have crossed); (3) pattern and flow modelling (knowing the distribution of the disease and its spread and how many people passed through places); (4) social distancing and movement monitoring (knowing if people are adhering to recommended safe distances and to circulation restrictions); and (5) symptom tracking (knowing whether the population are experiencing any symptoms of the disease).[1]

Numerous digital technologies are employed to perform these tasks, including smartphone apps, facial recognition and thermal cameras, biometric wearables, smart helmets, drones, and predictive analytics.[2] For example, citizens in some parts of China have been required to install an app on their phone and then scan QR codes when accessing public spaces (e.g., shopping malls, office buildings, communal residences, metro systems) to verify their infection status

and permission to enter.[3] The Polish government introduced a home quarantine app that requires people in isolation to take a geo-located selfie of themselves within 20 minutes of receiving an SMS or risk a visit from the police.[4] Israel repurposed its advanced digital monitoring tools normally used for counterterrorism to track the movement of phones of all coronavirus carriers in the 14 days prior to testing positive in order to trace close contacts.[5] As of mid-April, 28 countries had produced contact tracing apps that use Bluetooth to detect and store the details of nearby phones and contacts them if someone who had been near them tested positive, and another 11 were planning to launch imminently.[6] Other states have utilised technologies designed to measure biometric information. For example, hand-held thermal cameras have been used in a number of countries, some mounted on drones, to screen movement in public space.[7]

Technology companies have offered, or have actively undertaken, to repurpose their platforms and utilise the data they hold about people as a means to help tackle the virus. Most notably, Apple and Google, who provide operating systems for iOS and Android smartphones, are developing solutions to aid contact tracing.[8] In Germany, Deutsche Telekom are providing aggregated, anonymized information to the government on people's movements; likewise Telecom Italia, Vodafone and WindTre are doing the same in Italy.[9] Unacast, a location-based data broker, is using GPS data harvested from apps installed on smartphones to determine if social distancing is taking place,[10] with several other companies offering similar locational and movement analysis. Experian, a large global data broker and credit scoring company, has announced it will be combing through its 300 million consumer profiles to identify those likely to be most impacted by the pandemic and offering the information to 'essential organizations', including health care providers, federal agencies and NGOs.[11] Some of the most problematic aspects of surveillance capitalism have been repurposed by the state, further legitimating and cementing their practices.

Beyond society-wide surveillance to combat the pandemic, some companies have rushed to implement their own versions of these technological solutions, for example scanning the temperature of workers or deploying their own contact tracing systems. These are likely to become more common as restrictions are lifted, and their

use might become a mandatory condition of entering workplaces. In addition, many have adopted remote work surveillance systems so they can monitor the activity and productivity of their employees working at home, including recording keystrokes, how many emails are sent and their contents, and what employees are printing, or seeking constant status updates or that work is always undertaken while a video call is live.[12] These companies argue that they are trying to ensure that their workers are not taking unfair advantage of flexible work arrangements, or are not leaking confidential information. They take no account of workers trying to cope with the change in workplace environment which may not be conducive to work due to increased care duties, living in a shared space, or having poor or no broadband. Or workers have to learn new systems and procedures at short notice, or do not necessarily have the technical competence to perform any IT services needed to set up and maintain home-based work.

Some citizens will no doubt embrace surveillance technologies regardless of potential deleterious effects in the hope they will help to limit the spread of the virus and thereby save lives. Others might argue that companies should be able to know if their employees are performing the work they are paid to do. An underlying problem, however, stems from the track record of digital technology providers and governments in handling, protecting and extracting value from data. It seems logical to expect that data on movements, contacts or health will have value beyond the current public health crisis and they will be repurposed in some way that is not necessarily beneficial to citizens.[13] There are legitimate concerns as to whether public health and workplace surveillance systems will be turned off after the crisis or whether they will become a normal part of a new surveillance regime, as was the case with systems adopted after 9/11. Without embracing data sovereignty, privacy, civil liberties, workers' rights, citizenship and democracy are under renewed threat.[14]

In this regard it is significant that civil liberties organizations have set out ethical principles designed to protect privacy and rights, while acknowledging the potential utility of digital tools to tackle the virus. The key argument is that we should strive to ensure both civil liberties *and* public health, rather than simply trading the former for the latter. For example, the Electronic Frontier Foundation,[15]

American Civil Liberties Union,[16] the Ada Lovelace Institute,[17] and the European Data Protection Board[18] have demanded that:

- data collection and use must be based on science and need;
- the tech must be transparent in aims, intent, and workings;
- the tech and wider initiative must have an expiration date;
- a privacy-by-design approach with anonymization, strong encryption and access controls should be utilized;
- tools should be opt-in with consent sought, with very clear explanations of the benefits of opting in, operation and lifespan;
- the specification and user requirements, a data protection/privacy impact assessment, and the source code for state-sanctioned coronavirus surveillance should be published;
- data cannot be shared beyond the initiative or repurposed or monetized;
- no effort should be made to re-identify anonymous data;
- the tech and wider initiative must have proper oversight of use, be accountable for actions, have a firm legislative basis, and possess due process to challenge mis-use.

In other words, the tools must only be used when deemed necessary by public health experts for the purpose of containing and delaying the spread of the virus and their use should be discontinued once the crisis is over. We would add that we must also be vigilant to any potential control creep; that is, the risk that apps designed to limit movement based on health status will continue to be used and their criteria extended.

The temporal and organizational aspects of tackling the coronavirus pandemic raise other questions about the ethics of digital care. How do we ensure wellbeing and protect our civil rights while responding rapidly to an emerging crisis? How can we find a balance between the interests of public health and the economy and our own self-care? We don't have ready answers to these questions; formulating individual and collective interventions for slow computing within such a context is not straightforward. We are all now dealing with radically different circumstances. But an obvious conclusion to draw about the crisis response hitherto is that employers and employees need to define and deliver an ethics of digital care. For sure, some managers will have pursued admirable

practices: facilitating flexibility and accommodating workers with respect to workload, hours, and deliverables. Others might have been trying to maintain a business-as-usual stance, thereby elevating stress levels on employees or colleagues.

At the same time, the ethics of digital care concerns those people struggling with non-reciprocal care duties, experiencing the ill-effects of social isolation, or becoming obsessed with media stories that elevate anxiety and place a strain on mental health. New pressures have been placed on women, particularly working mothers, who find their duties increasing and societal supports shrinking. And for the working poor, the ethics of digital care are given new meaning when they find themselves negotiating online government sites to access support, or working essential frontline jobs in retail, public transit, care, cleaning and so on with less protection while also subjected to regimes of digitally-mediated oversight. Practicing slow computing in such situations is not easy when one is bound within digital chains and societal expectation.

No matter what society emerges on the other side of this crisis, digital technologies are still going to be a fundamental part of our everyday lives. Indeed, the crisis might lead to elevated levels of remote working, virtual meetings, digitally-mediated interactions, and online consumption; after all, the response has demonstrated that these can adequately supplement or replace some existing work and social practices. As such, smartphones, personal computers, smart city systems, social media, streaming services, online consumption, games, e-governance, and so on, will continue to saturate and configure our time and extract and utilise our data. Enhanced surveillance and dataveillance practices might remain in place, meaning that it will become ever more necessary to try and protect oneself from data extraction, ensure privacy, and push back against new pernicious powers. More than ever, an ethics of our digital future is required; at issue is a duty of care to imagine and create a society that enables us to practice slow computing during a fast response to a crisis and subsequent recovery. Individual and collective slow computing will remain necessary if we are to experience the joy of computing and enjoy balanced digital lives.