Who Watches the Watchers?

by Lim Kar Mern

Would you part with valuable data on your movements and driving patterns for a discount off your insurance? Would you be keen to allow your smartphone to capture images of your face to authorise payments via your banking app, e-wallet or an e-commerce platform app? Would you agree to the installation of a CCTV in your children's classroom? For most consumers, ticking "yes" in order to use an app, technology or service, is all too easy. While Alexa, Tesla, Robo-advisors, smart cities are all being touted as the most profound leap in innovation, productivity and technology, the costs to society and businesses remain unclear and less understood.

We can already see some backlash against technology in the news, especially where our personal data is concerned. Simply put, for each innovation and convenience, there are trade-offs for the right to our privacy.

In the wake of changing technologies and at the crux of every discussion on privacy is the need to balance the argument between protecting privacy and monitoring surveillance in the context of developing social values and the global economy. Where do we draw the line?

Privacy as fundamental human right

If we can agree that human rights stem from the very fundamental element of moral agency and the freedom to choose, then just as human rights are rights inherent to all human beings, everyone is entitled to be free from the intrusion of privacy. This was enshrined in the Universal Declaration of Human Rights (UDHR) in 1948 and though the standards and levels of protection may vary across socio-economic and cultural landscapes, the declaration of our rights serves as a constant reminder of the fundamental basics of our relationship with one another.

Up until the information technology age, most people have treated privacy as a space or physical place such as a home where personal affairs can be conducted away from the public eye. It is also seen as the non-disclosure of personal and intimate details about one's private life, like a person's health status or a criminal conviction. The landmark case that sparked the debate on privacy rights in Europe is that of James Malone, in which the European Court of Human Rights found that deliberate phone interceptions were a flagrant disregard of Malone's right to privacy.[1] In Malaysia, the Federal Constitution does not

1 *Malone v Metropolitan Police Commissioner* [1979] Ch 344. Malone was charged for handling stolen goods and he claimed that the phone interceptions from the police were an intrusion of his privacy rights. The European Court of Human Rights agreed and found the interceptions to be a flagrant disregard of his privacy right as provided by Art 8 of the European Convention of Human Rights.

expressly provide for the right to privacy, but the Federal Court in the case of *Sivarasa*[2] did state that the right to personal liberty, as enshrined in Article 5(1) of the Federal Constitution, includes the right to privacy.

The global trends and issues of our digital age may not have been envisaged when the UDHR was first drafted, but privacy rights have never been more important today as authorities and companies continue to collect our personal data at the expense of our consumption, social interaction and freedom of information. Fast forward 34 years later, we realise that governments are still intercepting our data (but this time, through fibre-optic cables that run like veins across the globe) and sharing data and intelligence with other governments in the name of preserving national security and counter-terrorism.[3]

On the explosion of Facebook's data-sharing fest with Cambridge Analytica,[4] law professor Julie Cohen from Georgetown University put it very succinctly that:

> "Privacy is foundational to the capacity of innovation as it shelters the processes of play and experimentation from which innovation emerges."[5]

One may argue that when Facebook is constantly bombarding us with targeted advertisement (with data collected from your use of the social networking platform) and push notifications,[6] it reduces the space we have for being innovative and to an extent that, in itself, becomes an invasion of our privacy — the space we need to be innovative.

Where we are with our personal data

If you own a mobile device, you would have downloaded an app that would only be fully functional if you had consented to its data privacy terms, i.e. allowed it to collect, use, store and process your data.

Germany's Deutsche Post has started offering "e-scan", a test service that involves a machine opening letters, scanning them and emailing it to customers.[7] Wells Fargo[8] provides the option of allowing commercial clients to view bank account balances, make deposits and approve payments from their mobile devices by simply scanning their eyes using the camera on their mobile devices.[9] In order to stay competitive in the increasingly digitised world, and despite the extraterritorial reach of Europe's General Data Protection Regulation (GDPR),[10] businesses continue to innovate, if not thrive, on the ledge of data security.

You may have agreed to use these services knowingly at

2 *Sivarasa v Badan Peguam Malaysia & Anor* [2002] 2 MLJ 413 (FC).
3 Lorenzo Franceschi-Bicchierai, "The 10 Biggest Revelations From Edward Snowden's Leaks" (5 June 2014) <https://mashable.com/2014/06/05/edward-snowden-revelations/> (accessed 21 August 2019).
4 BBC website, n.d., <https://www.bbc.com/news/topics/c81zyn0888lt/facebook-cambridge-analytica-scandal> (accessed 21 August 2019).
5 Julie E Cohen, "What Privacy is For", *Harvard Law Review*, Vol 126 (2013).
6 Amy Gesenhues, "Facebook Ad Revenue Tops $16.6 Billion, Driven by Instagram, Stories" (31 January 2019) <https://martechtoday.com/despite-ongoing-criticism-facebook-generates-16-6-billion-in-ad-revenue-during-q4-up-30-yoy-230261> (accessed 28 August 2019).
7 Kara Fox, "German Post Offices Will Convert Customers' Mail Into Email" (1 February 2019) *CNN* <https://edition.cnn.com/2019/02/01/europe/germany-digitized-mail-grm-intl/index.html> (accessed 28 August 2019).
8 Wells Fargo is a multinational financial services company which provides banking, mortgage, investing, credit card and commercial financial services and has offices in France, Germany, Spain and the UK: <https://www.wellsfargo.com/com/>
9 Alison Arthur and Bethany Frank, "Five Examples of Biometrics in Banking" (8 May 2019) <https://www.alacriti.com/biometrics-in-banking> (accessed 21 August 2019).
10 GDPR regulates business activities relating to the offering of goods or services (even if for free) to data subjects situated in the EU (not restricted to EU citizens) and the monitoring of the behaviour of such data subjects. Thus, data controllers and data processors outside of the EU whose data processing activities relate to such business activities are now also subject to the rules set out in the GDPR.

the expense of your own privacy, but do you know who has access to such data? Where does it get stored, and for how long? Will it be shared with any third-party and, if yes, who are they?

A recent study done at Stanford University and the University of Warsaw has shown that insurance companies can even now rely on Google Street View images of your house and predict a policyholder's risks of a car accident, just by classifying the dwelling according to type (whether it is a detached house, terraced house, block of flats, etc), its age and condition. By applying machine-learning software, the researchers where able to improve an existing insurer's risk model by 2%, better than the existing model which is based on a much larger data set that includes other variables such as age, sex and claim history.[11]

Did you consent for them to use your data in this way?

Such seemingly harmless data is also being collected from our smart devices and with increasing gumption thanks to the Internet of Things. Toronto's smart city (which runs on IoT) would typically have public Wi-Fi,[12] CCTV,[13] multiple sensors installed all around streets collecting data relating to traffic patterns, energy consumption and building use.[14] The Pentagon, on the other hand, has been testing a new technology that would allow smart phones to track even your gait patterns — the way you walk, move your hands or swipe with your fingers — so that it would be easier to track your phone if it gets stolen.[15] Even if phone manufacturers are not willing to integrate such gait technology into their products, the architects of smart cities will.

But what is to fear about parting with our data when we get convenience, efficiency and social connection?

Privacy against 'community interest'

We want to have control over our lives, *to have that private space to innovate*, yet we find ourselves in places where control is often thwarted. China's social credit system[16] brings us facial recognition technology that allows law enforcements to identify people within three seconds (and with a 90% accuracy rate). It allows police officers to name and shame offenders and spot criminals among the crowd.[17] As of today, the range of surveillance that China has deployed ranges from wearing a helmet installed with brainwave-reading technology to detect changes in emotional states of employees[18] — anger, anxiety, sadness — to using facial recognition in toilets to limit the amount of toilet paper dispensed to each individual.[19] What we have in the end is the surveillance of our freedom of thought and the inevitability of moral policing. If brain-wave-

11 Emerging Technology from the arXiv, "How A Google Street View Image of Your House Predicts Your Risk of a Car Accident" (30 April 2019) <https://www.technologyreview.com/s/613432/how-a-google-street-view-image-of-your-house-predicts-your-risk-of-a-car-accident/> (accessed 20 November 2019).

12 David Nield, "Simple Steps to Protect Yourself on Public Wi-Fi" *Wired* (8 May 2018) <https://www.wired.com/story/public-wifi-safety-tips/> (accessed 21 August 2019).

13 Fachrul Kurniawan, "Urban Distribution CCTV for Smart City Using Decision Tree Methods" (August 2017) <https://www.researchgate.net/publication/320148770_Urban_Distribution_CCTV_for_Smart_City_Using_Decision_Tree_Methods> (accessed 21 August 2019).

14 Oon Yeoh, "Future Proof: Cities Are Getting Smarter" *New Straits Times* (1 September 2019) <https://www.nst.com.my/lifestyle/sunday-vibes/2019/09/517680/future-proof-cities-are-getting-smarter> (accessed 21 August 2019).

15 Richard Bradbury, Jeff Sandhu and Arvindh Yuvaraj, "The Pentagon Wants Smartphones to Track How You Strut" BFM: The Business Station podcast (28 February 2019) <https://www.bfm.my/podcast/enterprise/enterprise-biz-bytes/ent-bb-pentagon-smartphones-track-strut> (accessed 28 August 2019).

16 Originating from the grid-style social management policing strategy in select locations of mainland China from 2001 and 2002, the system was eventually used to provide authorities with greater situational awareness on communities as well as tracking monitoring of individuals.

17 Zhou Jiaquan, "Drones, Facial Recognition and A Social Credit System: 10 Ways China Watches its Citizens" (4 August 2018) <https://www.scmp.com/news/china/society/article/2157883/drones-facial-recognition-and-social-credit-system-10-ways-china> (accessed 1 September 2019).

18 Tara Francis Chan, "China is Monitoring Employees' Brain Waves and Emotions — and the Technology Boosted One Company's Profits by $315 Million" *Business Insider US* (1 May 2018) <https://www.businessinsider.my/china-emotional-surveillance-technology-2018-4/> (accessed 28 August 2019). The technology facilitates managing efficiency at the production line.

19 Thuy Ong, "KFC in China Tests Letting People Pay by Smiling" *The Verge* (4 September 2017) <https://www.theverge.com/2017/9/4/16251304/kfc-china-alipay-ant-financial-smile-to-pay> (accessed 21 August 2019).

reading technology is coupled with AI, there would be no such thing as civil protest, political dissidence or diversity simply because these thoughts would be uncovered and stopped before they even arise in the mind. If we put facial recognition, brain-wave technology and AI together, your thoughts would be constantly monitored and pre-empted, just by clawing through massive data sets collected from various sources and making an inference based on your daily actions.[20]

What is more shocking is that 80% of 2,209 Chinese citizens interviewed believe that the social credit system is a positive thing as a means of improving the quality of life and fostering honest and law-abiding behaviour in society.[21]

The technology of drones, for example, was first famously used by the military and law enforcement as surveillance vehicles and weapons. Drones can certainly be useful for agricultural production[22] and putting out wild fires[23] but lately, Icelandic drones come with flapping wings and they are trained to behave exactly like a bird (not to immortalise your pet budgie, unfortunately) but to be sold to the military and law enforcement.[24] These silent "birds" not only go undetected in the presence of other animals, they are also fitted with cameras and GPS to map exactly where we are and record with proximity what we are doing.[25]

The argument is that with more drones, fewer soldiers will be killed in air strikes but as is the case with war and arms, "when the rich wage war, it's the poor who die".[26]

Ever-shifting goalpost

The war analogy can be applied today in the catch-22 we have with privacy and technology. The goalpost of balancing the protection of privacy and enforcing surveillance gets pushed every time a new wave of technology is invented and consumed by the masses. Because we leave so much digital footprint behind, the impending fear is that if ever the rich Big Tech like Apple and Google is used to architect a smart city, we would be the poor realising that the grave we have been digging is to bury our own privacy. Apple or Google would have already

20 For further reading: Karen Hao, "Inside Amazon's Plan for Alexa to Run Your Entire Life" *MIT Technology Review* (5 November 2019) <https://www.technologyreview.com/s/614676/amazon-alexa-will-run-your-life-data-privacy/> (accessed 8 November 2019).

21 Genia Kostka, "What Do People in China Think About 'Social Credit' Monitoring?" *The Washington Post* (21 March 2019) <https://www.washingtonpost.com/politics/2019/03/21/what-do-people-china-think-about-social-credit-monitoring/>

22 Andrew Nixon, "Best Drones for Agriculture 2019: The Ultimate Buyer's Guide" (11 June 2019) <https://bestdroneforthejob.com/drone-buying-guides/agriculture-drone-buyers-guide/> (accessed 20 September 2019).

23 Charlie Lapastora, "Drones the Latest Critical Tool to Fight Wildfires" *Fox News* (25 June 2019) <https://www.foxnews.com/tech/drones-fighting-forest-fires> (accessed 20 September 2019).

24 Sten Løck, "An Icelandic Inventor Has Achieved the Holy Grail of Airborne Technology With a Drone That Flies Like a Bird" *Business Insider* (29 May 2018) <https://www.businessinsider.com/bird-drone-could-revolutionize-surveillance-2018-5?IR=T> (accessed 13 August 2019). These bird-like drones are made for the use of the military and law enforcement.

25 Mark Bowden, "How the Predator Drone Changed the Character of War" (November 2013) <https://www.smithsonianmag.com/history/how-the-predator-drone-changed-the-character-of-war-3794671/> (accessed 13 August 2019). It was the Predator drone that located Osama bin Laden in Afghanistan and got him killed in 2011.

26 A quote in *Le Diable Et Le Bon Dieu* (The Devil and the Good Lord), a 1951 play by French philosopher Jean-Paul Sartre.

known that we would consume everything advertised to us, that we would follow all the trends, download all the apps and "smile at our phones"[27] at all the right times and at the right prices. You won't opt out because you simply can't, and because tech companies design these products with the idea that it's all or nothing, you won't have any control or any social space to say "no" either.

In the context then of being accorded protections such as the right to be erased[28] or the right to object,[29] it would seem like our right to privacy is turning into a mere philosophical notion despite such guarantees. Realistically, once we have consented to data being shared with a third party (who may share it with another party and that party may share it with *another* third party in order to provide us with the "best possible service"), how do we expect to exercise our right to be erased if we can't even be certain where our data is? In an economy that trades on big data, the truth is, there is no real certainty as to how our data is being used anymore.

Perhaps there are no easy answers as we have seen that technology will permeate almost every single aspect of our lives, if it hasn't already. What we do know is that as standards of privacy are shifting along the lines of technology, the argument of protecting privacy is moving away from the dichotomy of Eastern or Western ideals as even in the US and Europe, there are stark differences in their standards of protection.[30] What may be unacceptable as justification for surveillance today, may be acceptable tomorrow.[31] Freedom of speech aside, with the rise in brainwave technology, should we start recognising the freedom of cognitive liberty and have that embedded in the UDHR too? How else can we give meaningful consent to the use of our personal data if privacy notices are convoluted and time-consuming?

Perhaps there is nothing we can really do but to wait for another epic whistleblower of our time, the emergence of the next Edward Snowden[32] or Christopher Wylie.[33] In that case, it might be a little too late. **LH-AG**

27 AFP, "Smile-to-pay: Chinese Shoppers Turn to Facial Payment Technology" (4 September 2019) *The Guardian* <https://www.theguardian.com/world/2019/sep/04/smile-to-pay-chinese-shoppers-turn-to-facial-payment-technology> (accessed 27 September 2019)

28 GDPR, Art 17

29 *Ibid*, Art 21

30 PwC US, "Data Breach Notification: 10 Ways GDPR Differs From the US Privacy Model" (December 2016) <https://www.pwc.com/us/en/services/consulting/cybersecurity/library/broader-perspectives/gdpr-differences.html> (accessed 30 September 2019)

31 Rory Carroll, "NSA Surveillance Needed to Prevent ISIS Attack, Claims Former Intelligence Chair" *The Guardian* (US) (22 April 2015) <https://www.theguardian.com/us-news/2015/apr/22/mass-surveillance-needed-isis-attack-mike-rogers> (accessed 30 September 2019)

32 Barbara Starr and Holly Yan, "Man Behind NSA Leaks Says He Did It to Safeguard Privacy, Liberty" *CNN* (23 June 2013) <https://edition.cnn.com/2013/06/10/politics/edward-snowden-profile/index.html> (accessed 22 September 2019)

33 Carole Cadwalladr, "'I Made Steve Bannon's Psychological Warfare Tool': Meet the Data War Whistleblower" (18 March 2018) <https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump> (accessed 22 September 2019)