DATA RIGHTS AND POPULATION CONTROL: HUMAN, CONSUMER, OR COMRADE?

A Review Essay by Charles Kriel

'The Cambridge Analytica Files'.
The Guardian. 2018.

The EU General Data Protection Regulation and Recitals.
General Data Protection Regulation (GDPR). 2018.

Black Mirror, Season 3, Episode 1, 'Nosedive'.
21 October 2016. Netflix.

'Inside China's Vast New Experiment in Social Ranking'.
Hvistendahl et al. *Wired*. 14 December 2017.

Keywords—*data, privacy, human rights, consumer rights, DCMS Select Committee, fake news, Facebook, social credit, GDPR, Cambridge Analytica, Federal Trade Commission*

About the Author

Dr Charles Kriel is the author of several books. He is Specialist Advisor to the UK House of Commons Select Committee on Fake News, and hosts the podcast *Ci – Countering Violent Extremism.*[1]

1 Charles Kriel, *CI- Countering Violent Extremism* [podcast] Corsham Institute.

DOI 10.30966/2018.RIGA.4.8

On a rainy London Friday this year, the 23rd of March, seventeen UK officials entered a New Oxford Street building. Across the backs of many were FBI-style jackets emblazoned with a logo reading 'ico.'—the UK Information Commissioner's Office. The woman who led them carried a sheet of paper, presumably the warrant ICO Information Commissioner Elizabeth Denham had sought days before, allowing her to enter the offices of the campaign firm Cambridge Analytica.[2]

According to the *Guardian's* 'Cambridge Analytica Files'[3] lead by investigative reporter Carole Cadwalladr, they weren't the first group of 'auditors' to breach the building that week. Five days before, investigators from the cybersecurity firm Stroz Friedberg entered the Cambridge Analytica offices on behalf of Facebook, Inc., looking for information similar to that sought by Commissioner Denham.[4]

What was at stake was the data of at least 87 million Facebook users, most of them US citizens, and a trail of evidence implicating Cambridge Analytica. This material showed their CEO to be potentially in contempt of Parliament. Facebook too was in potential violation of a 2011 US Federal Trade Commission consent agreement that could see the company fined hundreds of millions of dollars.[5] These discoveries led to an even deeper revelation—the world's super-states were engaged in a struggle with information, all seeking to define the look of data governance. This revelation was to place the constituent foundational principles of the modern US, EU, and Chinese management policies—data management and also population management—in the spotlight.

On 19 March, Britain's Channel 4 TV interviewed Damian Collins, the MP leading the UK's House of Commons Select Committee investigation into fake news,[6] on the propriety of Facebook, a corporation under suspicion, sending private investigators into Cambridge Analytica, a company under investigation, to trawl the evidence.[7]

2 Harriet Agerholm, 'Investigators raid Cambridge Analytica offices after search warrant granted', *Independent*, 23 March 2018. [Accessed 10 May 2018]
3 *Guardian*, 'The Cambridge Analytica Files', a continuing series of articles from 17 March 2018. [Accessed 10 May 2018]
4 Hannah Summers and Nicola Slawson, 'Investigators complete seven-hour Cambridge Analytica HQ search', *Guardian,* US edition, 24 March 2018. [Accessed 10 May 2018]; David Meyer, 'Facebook Sent Auditors to Ensure Cambridge Analytica Wasn't Hiding User Data. The U.K. Said "Get Out" ', *Fortune*, 20 March 2018. [Accessed 10 May 2018]
5 Bloomberg, 'Facebook May Have Breached a 2011 Consent Agreement, FTC Says', *Fortune*, 29 March 2018. [Accessed 10 May 2018]
6 The author is the Specialist Advisor to the House of Commons Select Committee on Fake News. Kriel, Charles, Expert testimony on 'Fake News', UK Parliament, Digital, Culture, Media and Sport Committee, meeting chaired by Damian Collins, 23 January 2018.
7 Channel 4 TV, 'Damian Collins MP on Cambridge Analytica and Facebook: Mark Zuckerberg "should give evidence to MPs" ', presenter Jon Snow, 19 March 2018.

On the same day, Commissioner Denham kicked Facebook's auditors out. 'At the request of the U.K. Information Commissioner's Office, which has announced it is pursuing a warrant to conduct its own on-site investigation, the Stroz Friedberg auditors stood down', Facebook said.[8]

The arrogance of Facebook in sending in their own investigation team ahead of the authorities was noted in the press. 'Its culture melds a ruthless pursuit of profit with a Panglossian and narcissistic belief in its own virtue. Mr Zuckerberg controls the firm's voting rights. Clearly, he gets too little criticism', read the *Economist's* breathless assessment.[9] But this wasn't the only surprise questioned by press and public.

Although the ICO first issued a demand for access to Cambridge Analytica's offices and data on 7 March, and a demand for a warrant on 19 March, the application wasn't granted until 23 March. In the four long days between, several shipping crates were removed from the building, followed by a suspended CEO Alexander Nix.[10] Shadow digital minister Liam Byrne called the delay 'ludicrous'.[11]

Within three weeks, Mark Zuckerberg would testify twice before Congressional committees. His company lost more than $100 bn in market capitalisation (it would later recover somewhat).[12] And the US Federal Trade Commission (FTC) would confirm an investigation into whether Facebook violated a 2011 consent decree regarding the privacy of not just 87 million users, but possibly of *every* Facebook user.

In addition to these FTC, Congressional, and Parliamentary investigations, Norway, the Netherlands, Belgium, Spain, Portugal, Italy, Greece,[13] Australia,[14] India, Kenya, and Nigeria[15] were in pursuit as well.

8 Meyer, 'Facebook Sent Auditors'.
9 *Economist*, 'Facebook faces a reputational meltdown' (entitled 'Epic Fail' in the print edition), 22 March 2018. [Accessed 10 May 2018]
10 Hilary Osborne and Dan Sabbagh, 'Cambridge Analytica: search of London HQ delayed by wait for warrant', *Guardian,* 22 March 2018. [Accessed 10 May 2018]; Paul Sandle and Costas Pitas, 'Cambridge Analytica London search warrant delayed by court', *Reuters*, 22 March 2018. [Accessed 10 May 2018]
11 *BBC News*, 'Cambridge Analytica chief recalled by MPs', 22 March 2018. [Accessed 10 May 2018]
12 Business Standard, 'Facebook loses $100-bn m-cap in 10 days as US FTC announces privacy probe', 26 March 2018. [Accessed 10 May 2018]
13 Már Másson Maack, 'Facebook reported in 7 countries for breaking European privacy law', *The Next Web*, 6 April 2018. [Accessed 10 May 2018]
14 Rishi Iyengar, 'Australia launches investigation into Facebook over data scandal', *CNNMoney*, 5 April 2018. [Accessed 10 May 2018]
15 Karen Attiah, 'It's not just America: Zuckerberg has to answer for Facebook's actions around the world', *Washington Post*, 10 April 2018. [Accessed 10 May 2018]

DOI 10.30966/2018.RIGA.4.8

What also began to emerge was the existence of a fundamental schism in the way data, and Facebook, are treated in the US and the EU, and further used to control populations in more autocratic countries such as the Philippines and Myanmar.[16] Not to mention China, where, although Facebook has been banned since 2009,[17] data surveillance is potentially one of the Chinese Communist Party's most promising tools for self-preservation.

At the Senate Committee hearing on 10 April, senators slung phrases like 'consumer rights', 'freedom and liberties', and 'Terms and Conditions' at the Facebook founder. Meanwhile, Zuckerberg shielded himself with promises of stateside implementation of much of the EU's sweeping General Data Protection Regulation, and that Artificial Intelligence would fix it.[18] Despite that, the interrogation was generally congenial, with few sharp elbows. Senator Dan Sullivan (R–Alaska) even offered compliments, 'Quite a story—dorm room to the global behemoth you are. Only in America, would you agree? You couldn't do this in China.'

Zuckerberg's reply: 'There are some strong Chinese Internet companies.'

***

> In fact they're a little bit similar, in that [China and America] both come at data protection very much from a sectoral standpoint whereas in the EU we're really looking at a pan European Data Protection Regulation which is very much from a human rights standpoint.

Erin Anzelmo is a privacy advocate who spent ten years in Brussels working on Internet policy. She's being interviewed on the podcast *Ci – Countering Violent Extremism*,[19] discussing the difference between data privacy approaches in the US and China.[20] 'In China and America it is very much piecemeal by industry, by sector, cut across many different forms of legislation as well as often from a *consumer rights angle*.'

16 Ibid.
17 Sherisse Pham and Charles Riley, 'Banned! 11 things you won't find in China', *CNN Tech*, 17 March 2018. [Accessed 18 May 2018]
18 *C-SPAN*, 'Facebook CEO Mark Zuckerberg Senate Hearing on Data Protection', 10 April 2018. [Accessed 10 May 2018]
19 Erin Anzelmo, interview by Charles Kriel, 'State surveillance, privacy and online radicalisation', Corsham Institute podcast *Ci - Countering Violent Extremism*, 3 March 2018. [Accessed 10 May 2018]
20 The author is the host and producer of *Ci – Countering Violent Extremism.*

According to Anzelmo, the Chinese General Data Protection law is made up of two pieces of legislation: One is a legally binding document, drafted in 2012, that strengthens online information protection. The other is the Guideline for Personal Information Protection, classed somewhere below legislation, but still a part of China's data protection package. Although not legally binding, it guides industry and the private sector on subject access to, and handling and transfer of, sensitive personal data. 'These two comprise the majority of data protection law in China. And thirdly there's recently in 2017 adopted [sic] the China Cybersecurity Law which also touches on the handling of personal information.'

So isn't there some irony in these data protection laws having been passed in China, yet, as outlined in *Wired's* recent article 'You Are a Number' by Mara Hvistendahl, the Chinese government is working with Chinese companies to monitor and score citizens on their trustworthiness to the Chinese Communist Party?

'True. Some could call this window dressing', says Anzelmo. 'It is very different from what's happening in America with the vast amount of data harvesting, profiling and surveillance.'

***

America's approach to privacy began with the Fourth Amendment to the Constitution, ratified in 1791 as part of the Bill of Rights.[21] The Amendment was a response to the British Writ of Assistance, and largely protected the individual against unreasonable search and seizure by the State.[22]

The US Privacy Act of 1974 'governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies'.[23] While it seeks to protect the citizen from undue publication of personal data held in government systems of record, as well as giving individuals a means of accessing and amending these records—comprehensively listed by the Department of Justice[24]—the Act does nothing to protect personal data held by non-government entities, and is limited to the federal government's processing of information. [25]

21 Anzelmo, 'State surveillance'.
22 Cornell Law School, Legal Information Institute (LII), *Fourth Amendment: An Overview,* last edited June 2017. [Accessed 10 May 2018]
23 United States Department of Justice, Office of Privacy and Civil Liberties, *Privacy Act of 1974,* Updated 27 July 2015. [Accessed 10 May 2018]
24 US Department of Justice, Office of Privacy and Civil Liberties, *DOJ Systems of Records*, Updated 12 April 2018. [Accessed 10 May 2018]
25 Anzelmo, 'State surveillance'.

DOI 10.30966/2018.RIGA.4.8

The US began to address individual data privacy with regard to non-federal entities with acts like the Health Insurance Portability and Accountability Act (HIPAA), the Children's Internet Protection Act (CIPA), and the Children's Online Privacy Protection Act (COPPA), the latter of which prohibits the collection of online data from anyone under the age of thirteen. In practice, this prohibits children from creating accounts on Facebook, or obtaining an Apple ID.[26]

What is common amongst these Acts is they are trade-driven, and focused on rendering the data rights of consumers. 'The U.S. Agency primarily responsible for data protection is of course the Federal Trade Commission, the FTC. In the United States we see that privacy is very much about consumer protection. It's certainly not being regarded as a human right in comparison to what's happening in the European Union,' Anzelmo says, referring to the General Data Protection Regulation, implemented in 2018, harmonising data privacy laws across Europe.[27]

If any organisation represents an existential threat to Zuckerberg's company, it is the FTC. There's no small irony in the world's monopoly social network—which shares a duopoly in global digital advertising with Google[28]—putting the Federal Trade Commission on the front page of the world's newspapers. The FTC was established by Woodrow Wilson 104 years ago precisely to augment and enforce the Clayton Antitrust Act of 1914 with the Federal Trade Commission Act. The FTC Act represented one of Wilson's major moves against America's trusts, unfair competition, and consumer exploitation.[29]

> [T]he Commission is empowered, among other things, to (a) prevent unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce; (b) seek monetary redress and other relief for conduct injurious to consumers; (c) prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices; (d) gather and compile information and conduct investigations relating to the organization, business, practices,

26 Wikibooks contributors, 'Information Security in Education/Security Regulations', *Wikibooks,* 19 March 2018.
27 *EU GDPR Information Portal.* [Accessed 10 May 2018]
28 Financial Times, <https://www.ft.com/content/cf362186-d840-11e7-a039-c64b1c09b482> PAYWALL.
29 Federal Trade Commission, *About the FTC,* n.d. [Accessed 10 May 2018]

> and management of entities engaged in commerce; and (e) make reports and legislative recommendations to Congress and the public.[30]

Zuckerberg sailed through his early Spring 'grilling' by senators on Capitol Hill, deflecting poorly informed questions from politicians who seemed never to have used his platform. At one point, Senator Brian Schatz, a Democrat from Hawaii, asked, 'Let's say I'm emailing about "Black Panther" within WhatsApp [...] do I get a "Black Panther" banner ad?'[31]

But because of the FTC and their consumer-protection approach, Facebook is a long way from home safe and back in the dugout. A regular feature of Zuckerberg's testimony was mention of the FTC's 2011 consent decree with the social network. At the time, Facebook was charged with eight counts of deceiving consumers about their privacy. Said Jon Leibowitz, then Chairman of the FTC, 'Facebook is obligated to keep the promises about privacy that it makes to its hundreds of millions of users. Facebook's innovation does not have to come at the expense of consumer privacy. The FTC action will ensure it will not.'[32]

A consent decree is a settlement resolving a legal dispute between two parties. In this case, the FTC laid out eight charges against Facebook. Avoiding prosecution, the company agreed on a settlement to abide by certain rules going forward, without actually admitting guilt.

From a consumer protections perspective, the charges were damning:

- In December 2009, Facebook changed its website so certain information that users may have designated as private—such as their Friends List—was made public. They didn't warn users that this change was coming, or get their approval in advance.
- Facebook represented that the third-party apps users installed would have access only to such user information that they needed to operate. In fact, the apps could access nearly all of users' personal data—data the apps didn't need.
- Facebook told users they could restrict sharing of data to limited

30 Federal Trade Commission, *Federal Trade Commission Act, n.d.* [Accessed 10 May 2018]
31 Amelia Tait, 'Five clueless questions United States senators asked Mark Zuckerberg', *New Statesman*, 11 April 2018. [Accessed 10 May 2018]
32 Federal Trade Commission, 'Facebook Settles FTC Charges That It Deceived Consumers By Failing To Keep Privacy Promises', 29 November 2011. [Accessed 10 May 2018]

DOI 10.30966/2018.RIGA.4.8

audiences—for example with 'Friends Only'. In fact, selecting 'Friends Only' did not prevent their information from being shared with third-party applications used by their friends.

- Facebook had a 'Verified Apps' programme & claimed it certified the security of participating apps. It didn't.
- Facebook promised users that it would not share their personal information with advertisers. It did.
- Facebook claimed that when users deactivated or deleted their accounts, their photos and videos would be inaccessible. But Facebook allowed access to the content, even after users had deactivated or deleted their accounts.
- Facebook claimed that it complied with the US–EU Safe Harbor Framework that governs data transfer between the US and the European Union. It didn't.[33]

In the consent decree, Facebook agreed to implement a 'comprehensive privacy program', obtaining third-party audits of their own actions every two years for the following twenty years, ensuring 'that the privacy of *consumers*' information [was] protected'. They also agreed to protect consumers' data from access by third parties.[34]

In fact, the entire Cambridge Analytica / Facebook affair rests on the violation of this last requirement. David Vladeck, ex-Director of the Bureau of Consumer Protections at the commission, said on *Harvard Law Review's* blog: 'Facebook's apparent violations […] of the decree is [sic] troubling. The decree makes clear that robust opt-in consent is required before any sharing that exceeds the restrictions imposed by a user's setting.' Vladeck worked specifically on the FTC's case against Facebook. He goes on to say they broke the consent decree 'when Kogan deceived 270,000 users into thinking that their information would be used solely for research, and then managed to gain access to 50 million[35] of their friends, who had no clue (and probably still don't) that their data was harvested as well.'[36]

The punishment is severe. The penalty for violation of the consent decree is US $40,000 per user per violation. At 87 million people, that is potentially trillions

33 Ibid.
34 Ibid.
35 This number has since been revised to 87 million by Facebook themselves; Issie Lapowski, 'Facebook Exposed 87 Million Users to Cambridge Analytica', *Wired,* 4 April 2018. [Accessed 10 May 2018]
36 David C. Vladeck, 'Facebook, Cambridge Analytica, and the Regulator's Dilemma: Clueless or Venal?', *Harvard Law Review,* Blog. [Accessed 10 May 2018]

of dollars—a fraction of which could bring Facebook down.

If the senators' performance in the hearing can be taken as any indication of US political will, the chances of this happening are slim.

***

Throughout his testimony, Zuckerberg alluded to the EU General Data Protection Regulation (GDPR).[37] 'We believe that everyone around the world deserves good privacy controls,' he said. 'We've had a lot of these controls in place for years. The GDPR requires us to do a few more things, and we're going to extend that to the world.'[38]

A few more things indeed.

Recital 1 of the GDPR opens boldly, stating, 'The protection of natural persons in relation to the processing of personal data is a fundamental right.'[39]

In other words, data protection is a *human* right, with profound implications.

For example, for 'natural persons'—that is, any citizen of any country, anywhere in the world—the processing of 'sensitive personal data' in Europe, if accompanied by risk, is illegal.[40]

Risk occurs 'where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data; where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures; where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;

37 Intersoft Consulting, *General Data Protection Regulation*, 2018. [Accessed 10 May 2018]
38 Bloomberg Government Transcripts, 'Transcript of Zuckerberg's appearance before House Committee,' *Washington Post*, 11 April 2018. [Accessed 10 May 2018]
39 Intersoft Consulting, 'Recital 1 - Data protection as a fundamental right', 2018. [Accessed 10 May 2018]
40 Matthias Dehmer and Frank Emmert-Streib, *Frontiers in Data Science*. (Boca Raton, FL: CRC Press, 2018) p. 14.

DOI 10.30966/2018.RIGA.4.8

where personal data of vulnerable natural persons, in particular of children, are processed; or where processing involves a large amount of personal data and affects a large number of data subjects.'[41] A broad church of digital information, by any estimation.

These definitions—of 'risk', 'sensitive personal data', 'natural citizens', etc.—are vital to the changes brought on by the GDPR. Facebook, for example, is almost wholly made up of 'natural citizens' and their 'sensitive personal data'. At a minimum, and even where legal, processing natural citizens' data in Europe has been highly regulated since 25 May of this year, when the GDPR updated the already-in-place Data Protection Directive 95/46/EC, harmonising data privacy law across Europe.[42]

Just how much Facebook data is processed in Europe? Almost all of it.

In this instance, and particularly in light of Zuckerberg's promise to deliver GDPR-like controls to US consumers, Facebook should be thought of as two entities: Facebook Menlo Park, and Facebook Ireland. 239 million Facebook users in the United States and Canada are served from Menlo Park, California, and thus escape the jurisdiction of any real data protection authority—only the consumer protection authority of the FTC.[43]

Facebook Ireland processes the rest—1.9 billion users, or 89% of Facebook's user base. And as their data is processed within the EU, as 'natural citizens', their data processing is subject to the GDPR.[44]

But then, those users around the world were, until 25 May, also subject to the Data Protection Directive 95/46/EC, with similar rules. So what has changed? According to the *Washington Post*, the EU's privacy standards have been upgraded, and are now the toughest in the world.[45]

First, the GDPR extends the geopolitical territory it covers. If data from any EU citizen is processed, it no longer matters where that happens. The entity doing the processing will still be subject to EU law. 'Non-EU businesses processing the data of EU citizens will also have to appoint a representative in the EU',

41 Intersoft Consulting, 'Recital 75 - Risks to the rights and freedoms of natural persons', 2018. [Accessed 10 May 2018]
42 EU GDPR Portal, 'EU GDPR Information Portal', 2018. [Accessed 10 May 2018]
43 Michael Veale, 'Ignore Mark Zuckerberg', *Slate,* 12 April 2018. [Accessed 10 May 2018]
44 Ibid.
45 Rick Noack, 'One key question for Zuckerberg: Will Americans become second-class Web citizens?', *Washington Post,* 10 April 2018. [Accessed 10 May 2018]

according to the GDPR portal EUGDPR.org.[46]

The GDPR's increase in penalties is also significant. While before fines varied from country to country, and hovered in the hundreds of thousands, GDPR penalties have teeth—up to 4% of global turnover in the preceding year or €20 million, whichever is greater. Even the GDPR's tiered approach is enough to hit the bottom line of any company, as they can be fined 2% merely for not having their records in order.[47]

Companies are now also forbidden from relying on documents filled with 'long illegible terms and conditions full of legalese' to protect themselves when obtaining consent from users.[48]

There are substantial changes to rights of access, the right to be forgotten, data portability, design of systems for retention of the least data necessary ('privacy by design'), and the harmonisation of procedures around the appointment of Data Protection Officers.[49]

Significantly for Facebook, there are also changes to the notification period when a data breach has occurred. Companies now have three days to inform a 'natural citizen' when their data has been compromised.[50]

In the case of the 87 million records harvested by Dr Alexander Kogan for Cambridge Analytica and SCL, Facebook didn't get around to notifying victims for three years.[51]

Editor's note: On 11 July 2018, reports came in that Facebook is indeed to be fined the maximum £500,000 for failing to provide the protections required under data protection laws. In the first quarter of 2018, Facebook took in that amount in revenues every five and half minutes, but this cap was set in 1988 by the Data Protection Act. Under the new GDPR regime, the maximum fine would be '€20m (£17m) or 4% of global turnover—in Facebook's case, $1.9bn (£1.4bn)'.[52]

46 EU GDPR Portal, 'Key Changes with the General Data Protection Regulation', 27 April 2016 [Accessed 10 May 2018]
47 Ibid.
48 Ibid.
49 Ibid.
50 Ibid.
51 Aja Romano, 'The Facebook data breach wasn't a hack. It was a wake-up call', *Vox,* 20 March 2018. [Accessed 10 May 2018]
52 Alex Hern and David Pegg, 'The Cambridge Analytica Files: Facebook fined for data breaches in Cambridge Analytica scandal', *Guardian*, 11 July 2018. [Accessed 13 July 2018]

DOI 10.30966/2018.RIGA.4.8

***

China's approach to online data protection arrived in the global consciousness like a 2017 October Surprise, outlined in an aghast *Wired UK* article. 'Big data meets Big Brother' read the headline.

What was being announced to a relatively unsuspecting West was China's Social Credit System. Despite the innocuous name—sounding something like a social welfare system as envisaged by Equifax—the Social Credit System as told by *Wired* lands more in the territory of *Black Mirror* meets *The Man in the High Castle*.

The first episode of Charlie Booker's television series *Black Mirror*[53] (named for the state of reflection of an unpowered digital screen) is called 'Nosedive'. In a Max Richter-scored pastel future, dressed in clothes seemingly designed by a nostalgic *haute couture* Easter Bunny, citizens spend every waking moment glued to a smartphone, viewing their world through smart contact lenses. Attached to that view is a social media score in constant flux, regulated by the opinions of 'friends' in the black mirror.

In 'Nosedive', Lacie (played by Bryce Dallas Howard) is a sugary, cheerful 4.2 keen to buy a new home in a development for 4.5s and up. Hoping to raise her score, she attacks every human interaction with relentless positivity. Lacie even seeks out her childhood best friend Naomi—an impressive 4.8—in hopes that proximity and approval will up her score. Naomi acts thrilled, inviting Lacie to be her bridesmaid.

A comedy of errors leads Lacie to the wedding: she accidentally spills coffee on a stranger, lowering her score to 4.183; she misses her flight and only 4.2s or higher are allowed on the next one; an expletive-laden outburst at the airport drops her to a 3.1, forcing her into a hooptie rental that runs out of gas. Hitchhiking to a missed rehearsal dinner, bedraggled and desperate, her rating hits 2.6.

Aware of the new score, Naomi bans Lacie who nonetheless crashes the wedding, humiliates herself with a pathetic speech, is removed and remanded, and lands on a solid 0.0. Freed of her inhibitions and relentless observation, she seems to find love over an exchange of ridiculous insults with a handsome fellow-incarceree, both now freed to say whatever they like to the Other. My particular favourite was Lacie's 'What sort of cartoon character did your Mom

53 *Black Mirror,* season 3, episode 1, 'Nosedive', aired 21 October 2016, on Netflix. [Accessed 11 May 2018]

have to fuck to brew you up?'[54]

Whenever I've mentioned China's Social Credit Score,[55] I've been met with, 'Oh, just like *Black Mirror*.'

Social Credit Score is not just like *Black Mirror*. To the civil society-trained mind, it is a dystopian near-future reality, prepped for China-wide launch by 2020, with real possibilities of expanding beyond the country's borders.

The concept was first mooted on 14 June 2014 by the State Council of China in a document titled 'Planning Outline for the Construction of a Social Credit System', calling for 'the establishment of a nationwide tracking system to rate the reputations of individuals, businesses, and even government officials', according to Hvistendahl in 'You Are a Number'.[56]

The aim of the Social Credit Score, slated for nationwide implementation by 2020, is that each citizen's data should be tracked across all possible digital services and then consolidated into a file that will follow them throughout their lives, both online and offline. This aggregation of files is searchable and identifiable—by both fingerprints and biometric data.

The system is based on a scaled series of rewards and demerits. Everyone starts at 600, with a maximum possible score of 900. The number fluctuates according to trackable behaviours—'what you buy at the shops and online; where you are at any given time; who your friends are and how you interact with them; how many hours you spend watching content or playing video games; and what bills and taxes you pay'.[57]

While the Chinese Communist Party (CCP) has implemented piecemeal legislation giving citizens' rights and placing limits on companies collecting personal data—the General Data Protection Law, the Guideline for Personal Information Protection, and the Cyber Security Law—it is simultaneously working with the Asian continent's equivalents of Facebook, Google, and Amazon to cement power and insure their dominance for decades to come.[58]

54 Natalie Zutter, 'Trying Too Hard: Black Mirror, "Nosedive" ', *Tor*, 24 October 2016. [Accessed 11 May 2018]
55 This journal's editor is the one exception.
56 Mara Hvistendahl, 'Inside China's Vast new Experiment in Social Ranking', *Wired*, 14 December 2017. [Accessed 11 May 2018]
57 Rachel Botsman, 'Big data meets Big Brother as China moves to rate its citizens', *Wired*, 21 October 2017, updated 21 November 2017. [Accessed 11 May 2018]
58 Anzelmo, 'State surveillance'.

DOI 10.30966/2018.RIGA.4.8

In regional experiments across the country, Alibaba, China Rapid Finance, and Sesame Credit, to name just three, use platforms like AliPay, WeChat, Didi Chuxing, and even Baihe—China's largest dating app, to collect information and pass it on to a ranking algorithm. Charged with calculating the score, Alibaba subjects citizens to a 'complex algorithm', taking five factors into account when determining their score: credit history (do you pay your bills), fulfilment capacity (could you pay your bills), personal characteristics (phone numbers, etc., for personal identification), behaviour and preference, and interpersonal relationships. While the first three categories would surprise no European scanning their Experian statement, the last two rely on social media relationships, adding an alarming surveillance factor.

'Someone who plays video games for ten hours a day, for example, would be considered an idle person. Someone who frequently buys diapers would be considered as probably a parent, who on balance is more likely to have a sense of responsibility', Li Yingyun, Technology Director of Sesame Credit, told *Wired*. '[T]he system not only investigates behaviour—it shapes it. It 'nudges' citizens away from purchases and behaviours the government does not like', according to the magazine.

As users' scores rise and fall, they find their ability to negotiate society either enhanced or inhibited. With the standard starting score of 600, a citizen can take out a Just Spend loan of £500 to use with Alibaba. At 650, rental cars no longer require deposits, hotel check-ins become faster, and VIP airport lounges open their doors. Ant Financial offers nearly £6,000 loans with scores of 666. And a score of 750 opens the fast-track to a pan-European Schengen visa. These are not just life enhancements, but also opportunities to display individual status. According to *Wired*, more than 100,000 people have boasted about their high scores on China's Twitter equivalent, Weibo. This is important to not only the individual, but to their families for generations to come, because a higher score results in greater prominence for a potential partner's profile on dating app Baihe.[59]

But this is also the Chinese Communist Party harnessing data to automate its processes for the consolidation and maintenance of power. Along with rewards come punishments. Like 'a big data gamified version of the Communist Party's surveillance methods', Social Credit doles out demerits for the smallest violation, taking *nudge* to a new level.[60]

59 Botsman, 'Big data meets Big Brother'.
60 Ibid.

The infractions can range from cheating in school, through associating with low-score 'losers', to expressing opinions online that are out of step with the CCP. *Wired* inventories a few of the punishing restrictions: on internet speeds; access to restaurants and nightclubs; travel and services; access to housing and public transportation; employment opportunities; loans; social security benefits; schools; and more. 'As the government document states, the social credit system will 'allow the trustworthy to roam everywhere under heaven while making it hard for the discredited to take a single step', says *Wired* writer Rachel Botsman, quoting a State Council General Office policy entitled 'Warning and Punishment Mechanisms for Persons Subject to Enforcement for Trust-Breaking'.[61]

China is at a nearly perfect junction for the creation of a total surveillance and control system. Rapidly advancing technology, online tracking, and CCP ambitions have collided, creating a population-control environment with implications beyond the super-state.

'It's always been something that the party saw as a way of improving its control both over the party and over society itself', says Dr Samantha Hoffman of the International Institute for Strategic Studies. Anzelmo agrees. 'China's approach to data is driven by the Chinese Communist party, its ideology and its desire to stay in power.' [62]

Behind the saturated screens of six hundred million smartphones, China's approach to data privacy for population management reflects like a dark mirror, and with the potential to spill beyond Asian borders. The heads of six major intelligence agencies in the US recently warned citizens to avoid products and services from Chinese tech giants Huawei and ZTE. FBI Director Chris Wray warned 'about the risks of allowing any company or entity that is beholden to foreign governments that don't share our values to gain positions of power inside our telecommunications networks'.[63]

As hyperbolic as that may sound, the threat of a Chinese-manufactured global surveillance system driven by data is real. In the face of such a daunting prospect, one of the few safe zones may well be the EU, ring-fenced and protected through trade regulation, the General Data Protection Regulation, and the principle of data as a human right, with profound implications for both individual and national privacy and security.

61 Ibid.
62Anzelmo, 'State surveillance'.
63 James Vincent, 'Don't use Huawei phones, say heads of FBI, CIA, and NSA', *Verge*, 14 February 2018. [Accessed 11 May 2018]

DEFENCE STRATEGIC COMMUNICATIONS, VOLUME 2

Strategic Communications in International Relations: Practical Traps and Ethical Puzzles
Mervyn Frost, Nicholas Michelsen

'Hacking' Into the West: Russia's 'Anti-Hegemonic' Drive and the Strategic Narrative Offensive
James Rogers, Andriy Tyushka

The Russian Perspective on Information Warfare: Conceptual Roots and Politicisation In Russian Academic, Political, and Public Discourse
Ofer Fridman

Examining the Use of Botnets and their Evolution in Propaganda Dissemination
Nitin Agarwal, Samer Al-khateeb, Rick Galeano, Rebecca Goolsby

Putin, Xi, and Hitler—Propaganda and the Paternity of Pseudo Democracy
Nicholas O'Shaughnessy

The Significance and Limitations of Empathy in Strategic Communications
Claire Yorke

Britain's Public War Stories: Punching Above its Weight or Vanishing Force?
Thomas Colley

A Closer Look at Yemen
A review essay by James P. Farwell

Weaponised Honesty: Communication Strategy and NATO Values
A review essay by John Williams

DEFENCE STRATEGIC COMMUNICATIONS, VOLUME 3

Overwriting the City: Graffiti, Communication, and Urban Contestation in Athens
Anna Marazuela Kim with Tara Flores

Putting the Strategy back into Strategic Communications
David Betz, Vaughan Phillips

Japanese Strategic Communication: Its Significance as a Political Tool
Chiyuki Aoi

'You Can Count On Us': When Malian Diplomacy Stratcommed Uncle Sam and the Role of Identity in Communication
Pablo de Orellana

Strategic Communications, Boko Haram, and Counter-Insurgency
Abdullahi Tasiu Abubakar

Fake News, Fake Wars, Fake Worlds
A review essay by Charles Kriel

Living Post-Truth Lives … But What Comes After?
A review essay by Kevin Marsh

'We Have Met the Enemy and He is Us'
A review essay by David Loyn

To read 'Defence Strategic Communications',
go to www.stratcomcoe.org