Information Polity 27 (2022) 409–416
DOI 10.3233/IP-229010
IOS Press

Review Essay

Citizens first: A data regulator's perspective on surveillance in three cases[1]

Elizabeth Denham
CBE: Former UK Information Commissioner (2016–21)
E-mail: e@elizabethdenham.org

1. Introduction

In the rapidly expanding digital economy, society faces complex governance challenges that require innovative solutions. Government agencies now process large quantities of data, including huge amounts of personal information, which are necessary to deliver public services. Relevant governmental processes are increasingly governed by rules enshrined in data protection legislation. Further, the public now possesses strong awareness of how our data ought to be collected and handled. Instances of government or corporate overreach frequently attract public scrutiny and media criticism. Seen as the most advanced data governance regime in the world, the European Union's *General Data Protection Regulation* (GDPR) arose in the context of citizens clamouring for strong legal controls and clear ethical standards. Even so, one could argue that even GDPR does not go far enough. Because legislation moves slowly and technology advances quickly, legal protections tend to lag behind the exciting or frightening possibilities opened up by digital innovations. That situation puts data regulators in a tough but not insurmountable predicament.

This essay looks back at several memorable moments from my term at the helm of the UK's Office of the Information Commissioner (ICO) 2016–2021. That period saw major cultural upheavals, from Brexit to COVID-19. And so, the retrospective view already seems a bit blurry. However, major issues that the ICO pursued during that time remain in sharp focus thanks to some of the players involved. Below, three figures drawn from news stories will illustrate cases that affected the UK's regulatory landscape. In remarkably different ways, those three individuals helped set governance mechanisms in motion and changed public expectations for charities, businesses, and law-enforcement agencies. The essay concludes with brief reflections on the future of data processing vis-à-vis personal privacy, taking cues from the 2022 *Beyond Big Data Surveillance* report authored by Professor David Lyon, Director of the Surveillance Studies Centre at Queen's University (Ontario). Hopefully, *Information Polity*'s readership and the broader professional community will benefit from important findings relayed in that landmark document.

[1]This essay derives from a keynote speech delivered to the *Big Data Surveillance Project* meeting in Ottawa, Canada on 18 May 2022.

2. Becoming the UK Information Commissioner

Back in 2016, I faced a difficult choice: whether to accept a second term as the Information and Privacy Commissioner of British Columbia,[2] Canada, or re-locate to the United Kingdom and work as the UK Information Commissioner at the Information Commissioners Office (ICO).[3] A major factor that drew me to the ICO job was that Canada's regulators can only name and shame bad actors. Canadian laws generally lack enforcement measures. Conversely, the ICO has a substantial set of powers and resources enabled by the UK Data Protection Act (1998, 2018). Largely for that reason, the UK became my new home in 2016.

The ICO sets the international gold standard for robust regulation of personal privacy. Even so, I soon found that most of the Office's investigations had taken the long road to nowhere. Rather than add another thin file to the undistinguished list of open investigations, I decided to take a sectoral approach by setting my sights on entire data ecosystems. Despite 2016 being the year of the Brexit referendum and of record-setting data leaks that gained international media attention, my first actions as Commissioner targeted charities. This surprised and angered many in the UK. To set the stage for why charitable organizations merited investigation, let me tell you a little about Mrs. Olive Cooke.

3. The first case: Olive Cooke and the misuse of personal data in charitable fundraising

Olive Cooke was 92 years old in 2015 and a well-known local character in the city of Bristol, England. Even with her advanced age, she continued her work as a poppy seller, which began in the 1930s. For seventy-six years, Cooke had collected funds for the Royal British Legion[4] and made regular donations to more than a dozen other causes. In her final years, she received upwards of 3,000 requests for donations every year, as one *Guardian* headline stated (Morris, 2016). This mass of contacts accumulated because charities that had benefitted from her generosity sold or shared her information to other fundraising bodies. After her passing, some within the Cooke family indicated that she had felt badgered by solicitations. Shortly before my work at the ICO began, Olive ended her own life by throwing herself from the Clifton Suspension Bridge and into the River Avon.

Just as the UK has more stringent limits on how personal data can be handled than does my home country of Canada, national laws also restrict how charities can interact with the public. For example, 'cold calls' are known as 'nuisance calls' in British parlance. In the UK, such solicitations are unambiguously illegal.

When we dove deeply into practices charities use to encourage giving, my investigators found that many lines had been crossed. By aggressively wealth-screening potential donors, these organizations made public surveillance a routine activity. Terrible business practices had developed in the pursuit of worthy causes. Some of the more flagrant violations had been committed by trusted brands, such as the British Red Cross.[5]

As part of the ICO's sectoral investigation, we convened discussions with well over 100 fundraising entities. Ultimately, 13 organizations received fines (ICO, n.d.). And then came the backlash. Some cast me as an upstart regulator from the far-flung provinces with the damnable audacity to financially wound

[2] www.oipc.bc.ca/.
[3] www.ico.org.uk/.
[4] www.britishlegion.org.uk/.
[5] www.redcross.org.uk/.

my adopted country's benevolent societies. Few critics understood the staggering amount of personal information these organizations collected, retained, and exploited. The number of people whose data has been mistreated numbered in the millions. Their personal identifiers and habits had far too often been gathered without their knowledge or consent; this resulted in "lopsided information" (Lyon, 2022, p. 4) that benefitted organisations at the expense of individuals. In the wake of Olive Cooke's suicide, Britain's Fundraising Regulator[6] received hundreds of complaints (Anon., 2015). Other factors had contributed to Olive's plight, but her death became the symbol of a widespread problem.

ICO fines leveled against 13 charities included an accommodation that recognized the nature of their work. We knocked a zero off the sum that other types of businesses would have paid. Despite this significant reduction, the charitable sector changed as a result of our work. Several years later, ICO audits found much improved behaviour across the sector (ICO, 2018). And we showed that productive cultural shift to the leaders at technology platform companies as well as in the UK's direct-marketing and retail sectors. We argued the business case for handling personal data with respect.

4. The second case: Christopher Wylie and the Facebook-Cambridge Analytica scandal

The next major file that the ICO tackled with a sectoral approach concerns data-driven political campaigns. The major story there is more familiar than that of Olive Cooke. Moving from an elderly poppy seller from Bristol, I present Mr. Christopher Wylie: a pink-haired, Millennial tech wiz and *fashionisto* from the quaint provincial capital of Victoria, British Columbia (where I reside, coincidentally). Mr. Wylie has become the Edward Snowden of the corporate tech sector. In 2017, he entered a board room with a shocking story to tell and his lawyer at his side. The issue of online surveillance lies at the heart of the well-known Facebook-Cambridge Analytica scandal that emerged from that meeting. And I do not think that one goes too far by saying that subsequent news stories launched the value of personal data as a major issue in our time.

Christopher Wylie seemed deeply uncomfortable when disclosing stories about his former employer, the data firm Cambridge Analytica (now defunct). Although seated directly across the table from me, the whistleblower and his lawyer would only provide material evidence via Signal and only after all electronic devices had been removed from the room.

This young computer whiz – oddly shy and outwardly theatrical, fast-talking but soft-spoken – delivered his story in drips and drabs. I struggled to get a handle on just what Cambridge Analytica was up to. One moment, he would detail techniques that allowed Cambridge Analytica to socially sort Facebook profiles according to personality traits. The next, he would draw novelistic character studies of the players involved, overlain with the company's operations in Africa or South America, Asia or Europe. A quick disquisition on Steve Banon's personality would be followed by scads of technological jargon and mathematical logic, all before the company's actual plans for the United States and elsewhere unfolded.

Mr. Wylie could produce only scant evidence for the dramatic tale he relayed. But the ICO managed to confirm a critical mass of facts just before learning that "auditors hired by Facebook" had arrived in the UK "to inspect the servers and systems of Cambridge Analytica" (O'Sullivan, 2018). The ICO ordered Facebook's proxies off premises and seized hardware as well as data from could servers. I cannot say for certain whether Facebook managed to sequester any relevant information. But the ICO came away with 700 terabytes of data, the equivalent of 52 billion printed pages (McLaren, 2019).

[6] www.fundraisingregulator.org.uk/.

Information Commissioners and law-enforcement agencies around the world requested access to the Cambridge Analytica data that the ICO obtained by court order, wanting to launch investigations in their own jurisdictions.

News broadcasts beamed around the world showed ICO investigators arriving at Cambridge Analytica offices, decked-out in enforcement jackets. The spectacle recalls innumerable scenes of FBI or ATF teams busting down doors on television and in movies. A 2018 article in the *Guardian* stated that our "somewhat dusty regulator" had become "something of an armed militia" in that watershed moment (Cadwalladr, 2018). The same article quoted me in its bold-type headline: "data crimes are real crimes." I stand behind that phrase today, more firmly than ever before.

Readers may appreciate an obscure epilogue to the familiar story. One evening, I received a visitor at my door. He identified himself only as John K., a counter-terrorism agent with MI5 (*Hansard*, 20 Jan. 2022 col 572). True to his Kafkaesque moniker, K. sported a militaristic haircut over broad shoulders cloaked in business-casual attire. In a calm but muscular tone, he reported on a threat against my security. This potential threat apparently devolved from the fact that, as part of the ICO's Brexit investigations, we investigated whether client data held by a set of insurance companies had been used by the Leave.EU campaign. The insurance companies in question are owned by Arron Banks, a major political donor and co-founder of Leave.EU. The UK's Electoral Commission and National Crime Agency also took an interest in his political activities (Powers, 2018) in the years before Banks unsuccessfully appealed against the right of the ICO to conduct audits.[7]

Mr. K diligently swept my home for recording devices. He helped ensure that my license-plate number was not available through public records, that my home address did not appear online. K. convinced me to shut down my social media accounts completely: Facebook, LinkedIn, et cetera. He walked me through various encryption tools and recommended using different emails for different functions. He then provided a precis of my online presence accompanied by reports on the Internet behaviours of my inner circle. Shades of Kafka here, even if the anonymous and unflappable K. had cast my digital footprint only to expose me to my own vulnerabilities. His actions constitute appropriate surveillance, done with proper authority and for the purpose of protecting me from those without such clearances or scruples.

At the time of my encounter with John K., leading conversations about privacy and population-level surveillance centred around profiling, micro-targeting, and the spread of disinformation on social-media platforms. Marketing strategies to which many become inured had crept into political campaigning, unleashing serious public backlash. This was the moment when such conversations became common fare around innumerable kitchen tables. We have since seen transformational advances that, for good and for ill, make personal information more comprehensive than ever before.

5. The third case: Edward Bridges and facial recognition technology

Today, debates about surveillance often concern law enforcement's use of live Facial Recognition Technology (FRT). It is still unclear where this defining civic shift will settle – if it ever does. To help give shape to nebulous societal issues surrounding surveillance, let me present to you Mr. Edward Bridges, who initiated legal actions against the South Wales Police in 2020.

[7]The General Regulatory Chamber on Information Rights dismissed a series of appeals, and the Tribunal's decision (EA/2019/0054-0059) can be read in full online, here: www.panopticonblog.com/wp-content/uploads/sites/2/2020/03/Leave.eu-Eldon-PECR-appeal.pdf.

Edward Bridges: a Welsh national and resident of Cardiff; late thirties; father of two; quite well spoken; a public-affairs professional and, formerly, Liberal Democrat local councillor. In the UK and beyond, Bridges has helped animate the issue of live FRT in our civic-cum-digital society. A BBC news story about Bridges' opposition to state surveillance details a timeline of events and highlights the theme of public consent, or lack thereof. Its headline describes the man as having "taken on South Wales Police" (Anon., 2020). For me, that verbiage ("take on" the police) seems to distort this man's merely passive role in an instigating incident that constitutes overreach by law enforcement. One might say instead that the South Wales Police struck first in "taking on" a private citizen suspected of no crime.

According to the BBC article, in December of 2017, FRT captured Mr. Bridges' movements in Cardiff while he completed a bit of Christmas shopping. Months later, FRT captured his image again, this time at a peaceful protest in opposition to the arms trade. He then contacted the UK's National Council for Civil Liberties[8] (also known as Liberty), pointing out that the South Wales Police had parked their highly conspicuous van – with the words "automatic facial recognition" printed on the side – very near to the protestors. Guess which direction the cameras pointed that day. This manoeuvre, Bridges argued, sought to dissuade discontented citizens from assembling lawfully in a public place.

Edward very publicly objects to, in his words, "oppressive mass surveillance being deployed on our streets" (Anon., 2020). Further, he declaims that Britain, on paper, allows only for "policing by consent": meaning "police need to have the consent of the public in what they do." When law-enforcement agencies defy that principle, they risk losing the trust of the public, which is, according to Bridges, "not in anyone's interest" (2020). This chap hardly sounds like the bomb-planting radicals or violent religious extremists who normally help justify expansions of government's capacity to monitor, profile, and track individuals and even entire populations.

Au contraire, Mr. Bridges is a dramatic figure in the world of data rights partly for seeming so ordinary. It all began with a rather buttoned-down family man doing a bit of Christmas shopping.

Bridges took his local police constable to court, lost, then won a compromised sort of victory on an appeal filed in High Court (EWCA Civ 1058). He supported his legal costs partly through an online crowd-funding campaign (Anon., 2020). Those of us dedicated to raising awareness about the dangers of FRT should thank Bridges: for standing up in the first place and for his crowd-funding efforts, which may have drawn extra attention to the issue of state surveillance in the months before his lawsuit became a major news story.

While Bridges' case moved through the court system, with ICO interventions, we also investigated several police forces trialing FRT tools. We looked closely at how law-enforcement used the technology; investigating where searches and data came from, the technology's accuracy, and the types of gatherings the Police had targeted. Like Edward, we were worried that FRT had a chilling effect on democratic activity. That is a grave enough concern in countries with political rights enshrined. Frightening to imagine: what uses might totalitarian regimes find for equivalent or improved technologies? Adding an FRT layer effectively weaponizes the UK's 6 million CCTV cameras. When law enforcement captures and retains citizens' biometrics and location-based data as they go about their daily business, I must ask (in concert with Mr. Edward Bridges) whether police are simply going about *their* proper business. FRT enables a culture shift from policing after an event to anticipating criminality in every instance: capture-and-release policing on a mass scale.

The ICO drafted a formal opinion for when FRT is appropriate (ICO, 2019). We set a clear threshold for turning the technology on: substantial, evidence-based threats about a particular action, at a certain time, in a known location. Effectively, we created a first-of-its-kind framework for a code of practice.

[8] www.libertyhumanrights.org.uk/.

Our file also included commercial uses of FRT, notably those deployed by the company Clearview AI.[9] Clearview scrapes the Internet to match faces and biometrics with publicly available intelligence. It then sells its information and technology to government agencies. The company was chased out of the UK, following a £7.5 m fine issued by the Information Commissioner's Office (ICO, 2022). Even so, Clearview finds safe harbour in other jurisdictions. I worry deeply about the situation in countries without strong privacy laws and where commissioners do not have practical enforcement powers. If a law does not legislate measures for redress and enforcement, it is merely a symbolic gesture toward democratic rights. We need material consequences, like financial sanctions or stop-processing orders, to make the word of law actionable. Equally, we need the voices of courageous citizens, like Edward Bridges, to animate societal issues and raise public awareness.

6. On the importance of personal narratives

Only personal identifications can bring mere narratives to life. Olive Cooke was no ordinary fundraiser; she was a nonagenarian poppy-seller for the Royal British Legion, who had lost an enlisted father and an enlisted husband to World Wars One and Two, respectively. The remarkably different figures of Misters Wylie, Banks, and K. appear in a story not just about user data and its misuse. Rather, the well-known scandal concerned people's personality traits and political manipulation that targeted them directly. Books and movies about Wylie's whistleblowing and Cambridge Analytica's activities have been created[10] partly because the company's work has potent and lasting effects, partly because of the vivid characters at the heart of the story.

In the lineage of animating figures at the forefront of privacy, Edward Bridges represents the everyman who navigates but cannot accept daily life in the Surveillance-Industrial Complex. The tale of his encounters with FRT seem heightened by the stark contrast between his mild-mannered, peace-promoting activities and the overbearing police tools brought to bear upon them, needlessly and illegally.

The compelling and courageous individuals presented in this essay defy the phrase 'ordinary citizen'. Similarly, we must not think of live FRT as just another policing tool or tech solution. As a cultural force, surveillance's confluence with computing power breaks the informational riverbanks. Meanwhile, my regulatory and legislative colleagues scramble to keep society from falling into the rising tide.

Increasing public awareness is effecting real-time change. In response to ICO guidance, London's metropolitan police no longer automatically apply FRT to passers through at King's Cross tube station. San Francisco has outright banned facial-recognition technologies within city limits. The executive branch of the EU seems set to ban live FRT on the continent. And, in the spring of 2022, Canadian commissioners urged their House of Commons Standing Committee on Access to Information, Privacy and Ethics to explore limiting law enforcement's capacity to deploy FRT and recommended a ban on its "generalized" application (O'Kane, 2022). Some police forces have argued that they merely trial FRT applications. But when technology is tested indiscriminately on large populations of private citizens, such activity constitutes implementation.

7. Conclusion

I have shared the stories of three influential citizens: Mrs. Cooke, Mr. Wylie, and Mr. Bridges. Although

[9] www.clearview.ai/.

[10] For an example of a film, see 2019's *Brexit: The Uncivil War*. That same year, Random House published a book by Wylie himself, titled *Mindf*ck: Cambridge Analytica and the Plot to Break America*.

these people come from very different walks of life, they each drove social change and data rights forward. Individuals initiate change by making their personal encounters with surveillance a public matter. Doing so, citizens become advocates, journalists, and symbols of widespread social concern. Media stories, research projects, and policy reforms come afterward. There is a painful irony at work here, when reining in surveillance and bolstering privacy protections requires individuals to publicize personal harms that result from corporate or state violations.

While technology advances and citizens become increasingly vulnerable to surveillance and manipulation, privacy professionals must think big and act boldly. But our highly changeable data climate makes it difficult for us to gain a clear view of the problems we collectively face. Thankfully, the Beyond Big Data Surveillance project's 2022 report, authored by Professor David Lyon, gives a starting point for the innovative solutions we urgently need (Lyon, 2022: 15–16). He and his colleagues make three key recommendations. First, nation states must establish digital rights and data justice for their citizens. The principle of personal privacy cannot, alone, stand up to the technological developments afoot. Second, meaningful progress will only come from collaborative efforts across civil society, government, and academia. Diverse players must contribute to resisting developments that inappropriately blur the lines between commercial and state actors. Third, we need to grow public awareness. In my view, individual members of the public are best poised to raise that awareness. Their intimate stories have the power of relatability. First-hand accounts can most effectively expose the measurable impacts of our ever-more intimate surveyors.

All the Cookes and Wylies and Bridges out there are potent symbols of the little guy in a Big Data world. Bad data cultures, based on secrecy and exploitation, will only be punctured by courageous flesh-and-blood people. Without them, no digital rights, no data justice.

Elizabeth Denham has worked as an effective regulator of information and privacy rights across multiple jurisdictions. She frequently appears as a speaker and advocate at conferences, for universities, and on media platforms. Her accolades include an award as a Commander of the British Empire for her services in protecting information rights. Ongoing projects address children's rights online, through the 5Rights Foundation, and international data policy issues as an advisor to the law firm Baker McKenzie. Email: e@elizabethdenham.org

References

Anon. (2015, July 16). *Olive Cooke inquest: Poppy seller suffered depression*. BBC. https://www.bbc.com/news/uk-england-bristol-33550581.

Anon. (2020, August 11). Facial recognition: what led Ed Bridges to take on South Wales Police? BBC. https://www.bbc.com/news/uk-wales-53742099.

Cadwalladr, C. (2018, July 15). Elizabeth Denham: 'data crimes are real crimes'. *The Guardian*. https://www.theguardian.com/uk-news/2018/jul/15/elizabeth-denham-data-protection-information-commissioner-facebook-cambridge-analytica.

Edward Bridges and the Chief Constable of the South Wales Police and The Secretary of the Home Department and The Information Commissioner, et al., June 23–25, 2020. Court of Appeal (Civil Division). Neutral Citation No.: EWCA Civ 1058. https://www.judiciary.uk/wp-content/uploads/2020/08/R-Bridges-v-CC-South-Wales-ors-Judgment.pdf.

Hansard HC Deb vol 707 col 572 (20 January 2022: Lawfare and UK Court System). https://hansard.parliament.uk/commons/2022-01-20/debates/4F7649B7-2085-4B51-9E8C-32992CFF7726/LawfareAndUKCourtSystem.

Haynes, T. (Director). (2019). *Brexit: the uncivil war*. House Productions.

Information Commissioner's Office (ICO). (2018, April). *Findings from ICO information risk reviews at eight charities.* https://ico.org.uk/media/action-weve-taken/audits-and-advisory-visits/2259675/charities-audit-201808.pdf.

Information Commissioner's Office (ICO). (2019, October 31). *The use of live facial recognition technology by law enforcement in public places.* https://ico.org.uk/media/about-the-ico/documents/2616184/live-frt-law-enforcement-opinion-20191031.pdf.

Information Commissioner's Office (ICO). (2022, May 23). ICO fines facial recognition database company Clearview AI Inc more than £7.5 m and orders UK data to be deleted. https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/.

Information Commissioner's Office (ICO). (n.d.). Charity fundraising practices. https://ico.org.uk/your-data-matters/charity-fundraising-practices/.

Leave.EU Group Limited, Eldon Insurance Services Limited and *The Information Commissioner*, December 9–11, 2019. First-Tier Tribunal, General Regulatory Chamber: Information Rights. Appeal No.: EA/2019/0054-0059. https://panopticonblog.com/wp-content/uploads/sites/2/2020/03/Leave.eu-Eldon-PECR-appeal.pdf.

Lyon, D. (2022, May 18). *Surveillance, freedom and fairness: a report for all Canadian citizens*. Surveillance Studies Centre. https://www.sscqueens.org/news/beyond-big-data-surveillance-report-released.

McLaren, L. (2019, April 18). Is Elizabeth Denham the only person powerful enough to take on Facebook? *The Walrus*. https://thewalrus.ca/is-elizabeth-denham-the-only-person-powerful-enough-to-take-on-facebook/.

Morris, M. (2016, January 20). Poppy seller who killed herself got 3,000 charity requests for donations a year. *The Guardian*. https://www.theguardian.com/society/2016/jan/20/poppy-seller-who-killed-herself-got-up-to-3000-charity-mailings-a-year.

O'Kane, Josh. (2022, May 2). Use of facial-recognition technology by law enforcement must be limited, say privacy watchdogs. *The Globe and Mail*. https://www.theglobeandmail.com/politics/article-canadas-privacy-commissioners-come-together-to-ask-for-guardrails/.

O'Sullivan, D. (2018, March 20). *Facebook's Cambridge Analytica auditors stand down at UK request*. CNN. https://money.cnn.com/2018/03/19/technology/cambridge-analytica-audit/index.html.

Power, Sam. (2018, November 7). Arron Banks investigated over £8 m given to the Brexit campaign – what can this even buy you? *The Conversation*. https://theconversation.com/arron-banks-investigated-over-8m-given-to-the-brexit-campaign-what-can-this-even-buy-you-106391.

Wylie, Christopher. (2019). *Mindf*ck: Cambridge Analytica and the plot to break America*. Random House.