[11] Sir Michael Briggs, Civil Courts Structure Review, (Interim Report, December 2015) at 6.6ff <https://www.judiciary.uk/wp-content/uploads/2016/01/ccsr-interim-report-dec-15-final1.pdf> accessed 28 November 2019.
[12] ME Katsh and O Rabinovich-Einy, Digital Justice: Technology and the Internet of Disputes (Oxford University Press 2017) 158.
[13] RE Susskind, Online Courts and the Future of Justice (Kindle eBook: Oxford University Press 2019) 28.
[14] Victoria Ramsey, 'Anonymous Litigant in Person Wasted 10 Judges' Time' (Law Society Gazette, 18 November 2019) < https://www.lawgazette.co.uk/practice/anonymous-litigant-in-person-wasted-10-judgestime/5102212.article > accessed 7 December 2019.
[15] JUSTICE, 'What is a Court?' (2016) at ff2.21 < https://justice.org.uk/wp-content/uploads/2016/05/JUSTICE-What-is-a-Court-Report-2016.pdf > accessed 4 December 2019.
[16] John Aitken, 'Lessons From a Trailblazer Model', Tribunals Journal (autumn, 2016) < https://www.judiciary.uk/wp-content/uploads/2017/03/aitken-lessons-from-a-trailblazer-model-autumn-2016.pdf> accessed 4 December 2019.
[17] WE Burger, Delivery of Justice (West Publishing Co 1990) 45.
[18] John Aitken, 'Lessons From a Trailblazer Model', Tribunals Journal (Autumn, 2016).
[19] Kennedys Law, The £1 Billion Plan: The Civil Court of the Future (2017) <https://www.kennedyslaw.com/media/1470/kennedys_theonebillionpoundplan_aug2017.pdf> accessed 4 December 2019.
[20] JH Baker, An Introduction to English Legal History (Oxford University Press 2019) 7.

Legal Information Management, 20 (2020), pp. 103–105

doi:10.1017/S1472669620000249

The 'Personal' in Personal Data: Who is Responsible for Our Data and How Do We Get it Back?

Winner of Best in Category, Justis International Law and Technology Writing Competition 2020 for the Category of Social Media, Data and Privacy, by Janis Wong of the University of St Andrews

In our data-driven society, every piece of technology that connects us to the internet collects our personal data (any information relating to an identified or identifiable natural person), building elaborate profiles on what we are doing, where we are, and even who we are.[1] As data subjects (those about whom personal data are collected), we can no longer hide from data controllers (those who collect and determine what these data are used for). With every data breach and data sharing revelation from Cambridge Analytica[2] to Google's Project Nightingale,[3] our personal data is becoming less personal, where data attached to our identity are no longer in our control and becomes harder for us to identify who is responsible.

THE DATA SUBJECT'S STRUGGLE

Recognising the need to protect privacy as an individual's right, data protection attempts to rebalance power between data subjects and data controllers. The European General Data Protection Regulation (GDPR)[4] grants data

subject rights such as the right of access,[5] right to be forgotten,[6] and right not to be subject to a decision based solely on automated processing.[7] Data controllers must also follow the principles of data protection by design and by default.[8] However, even with the GDPR, data subjects still lack the extra hours and cognitive capacity to exercise these rights.[9] Only 15% of EU citizens feel completely in control of their personal data.[10] Additionally, while there are multiple means for lawful processing of personal data,[11] data controllers have weaponised consent by using privacy policies written in legalese and dark patterns to hide privacy-protecting options, obfuscating how data subjects' data are reused, aggregated, and anonymised to make decisions about them.[12]

EVERYONE IS A DATA CONTROLLER

Responsibility over personal data is further complicated where judgements have expansive interpretations of who could be considered a data controller. A user who administers a Facebook Group or Page,[13] a website operator who has a Facebook 'like' button or other social plugins,[14] and a religious community whose congregation conducted preaching activities and collected personal data[15] are 'joint controllers' who are all liable if one controller breaches requirements on those data. This significantly increases the number of data controllers and people responsible for personal data, where not all joint controllers need to have access to the data for joint controllership to occur. While these judgements introduce more responsibility, they also disperse where data responsibility lies, increasing the ambiguity over who can share, reuse, and repurpose data.

FROM MY DATA TO OUR DATA TO YOUR DATA

Beyond the individual, initiatives such as Decode encourages public institutions to be more responsible with its citizens' data.[16] However, governments continue to watch over its people through social credit scoring,[17] criminal sentencing,[18] and partnerships with privately-owned, pervasive technologies.[19] In the age of surveillance capitalism,[20] where personal experiences are translated into free raw material for behavioural data, our personal and derived data are collectively used against us. Although data protection and information rights enable some forms of transparency and accountability, our data are still often used without our knowledge and without legal recourse as decisions are made using unexplainable black-box algorithms.[21]

RECLAIMING OUR PERSONAL DATA

In order to better understand how our personal data is being used and abused, we need to look beyond data protection on an individual level. Instead, privacy should represent an ecosystem that requires legal and socio-technical collaboration between lawyers, technologists, policy makers, and most importantly, us as data subjects.

Firstly, stronger regulation beyond data protection is required to fully realise the responsibility data controllers have over our personal data. While the European Data Protection Board established guidelines to clarify the GDPR,[22] further regulatory guidance has only been provided by academics and has yet to be codified.[23] Regulators should do more to prevent 'ethics washing', whereby data companies use ethics boards and policies to limit regulation.[24] Competition law in particular may help us escape the grasp of digital behemoths. Looking beyond fines, Margrethe Vestager, the EU's competition commissioner, plans to regulate industries such as artificial intelligence and gig economy companies to return the ethos of 'consumer is king' back to data subjects.[25] Other mechanisms include using legal data trusts to empower data subjects by facilitating access to pre-authorised, aggregated data and remove key obstacles to the realisation of the potential underlying large datasets.[26]

Secondly, although many of the challenges described are driven by the business models of data controllers, technology should be considered part of, and not excluded from, solutions that help data subjects better understand how our data are processed and managed. Tools such as Databox,[27] Jumbo Privacy,[28] and DoNotPay[29] are already beginning to challenge the data protection practices of big Tech companies, providing alternatives to existing services and mechanisms for control.

Finally, in considering how personal data should be best protected, data protection must be considered beyond the individual. Data protection should look beyond privacy as control and be expanded to include the ability to participate and engage with other individuals and groups, crowdsourcing information and solutions to personal data challenges. Philosophical discussions surrounding group privacy can be put into practice. Developing a data protection public sphere and commons, regulators, lawyers, and technologists can support data subjects in minimising the risks involved in the public use of anonymised personal data[30] and establish the necessity for collective rights[31] before and after data are collected. The protection of data subjects with regard to the processing of personal data can only be achieved where legal frameworks and technological mechanisms include input from data subjects to respect their data protection requirements.

The responsibility over our personal data should not burden data subjects. As data protection matures, this responsibility should be shared with all stakeholders that benefit from the personal data, not only with those about whom personal data are collected. It is only with legal and technical collaboration that data subjects can be collectively protected, governing the data protection landscape for the benefit of our current and our future selves.

Footnotes

[1] Surya Mattu and Kashmir Hill, 'The House that Spied on Me' *Wired* (2 February 2018) <https://gizmodo.com/the-house-that-spied-on-me-1822429852> accessed 30 November 2019.

[2] Carole Cadwalladr and Emma Graham-Harrison, 'Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach' *The Guardian* (17 March 2018) <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election> accessed 30 November 2019.

[3] Anonymous, 'I'm the Google whistleblower. The Medical Data of Millions of Americans is at Risk' *The Guardian* (14 November 2019) <https://www.theguardian.com/commentisfree/2019/nov/14/im-the-google-whistleblower-the-medical-data-of-millions-of-americans-is-at-risk> accessed 30 November 2019.

[4] Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L119/1.

[5] ibid art 15.

[6] ibid art 17.

[7] ibid art 22.

[8] ibid rec 108.

[9] Rachel Coldicutt, 'Better than ethics' (*doteveryone*, 28 November 2019) <https://www.doteveryone.org.uk/2019/11/better-than-ethics/> accessed 30 November 2019.

[10] Bart Custers, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani, and Simone van der Hof, 'Conclusions' in Bart Custers, Alan M. Sears, Francien Dechesne, Ilina Georgieva, Tommaso Tani, and Simone van der Hof (eds), *EU Personal Data Protection in Policy and Practice* (T.M.C. Asser Press 2019).

[11] General Data Protection Regulation, art 6.

[12] Christine Utz, Martin Degeling, Sascha Fahl, Florian Schaub, and Thorsten Holz. '(Un)informed Consent: Studying GDPR Consent Notices in the Field.' (2019) ACM SIGSAC Conference on Computer and Communications Security (CCS '19) < https://doi.org/10.1145/3319535.3354212> accessed 30 November 2019.

[13] Case C-210/16 *Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v Wirtschaftsakademie Schleswig-Holstein GmbH* ECLI:EU:C:2018:388.

[14] Case C-40/17 *Fashion ID GmbH & Co. KG v Verbraucherzentrale NRW eV* ECLI:EU:C:2019:629.

[15] Case C-25/17 *Tietosuojavaltuutettu v Jehovan todistajat — uskonnollinen yhdyskunta* ECLI:EU:C:2018:551.

[16] Decode European Commission, 'Reclaiming the Smart City: Personal Data, Trust, and the New Commons' (July 2018) <https://media.nesta.org.uk/documents/DECODE-2018_report-smart-cities.pdf> accessed 30 November 2019.

[17] VICE News, 'China's "Social Credit System" Has Caused More Than Just Public Shaming (HBO)' (12 December 2018) <https://www.youtube.com/watch?v=Dkw15LkZ_Kw&> accessed 30 November 2019.

[18] Julia Angwin, Jeff Larson, Surya Mattu, and Lauren Kirchner, 'Machine Bias' *Propublica* (23 May 2016) <https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing> accessed 30 November 2019.

[19] Sam Biddle, 'Amazon's Ring Planned Neighborhood "Watch Lists" Built on Facial Recognition' (*The Intercept*, 27 November 2019) <https://theintercept.com/2019/11/26/amazon-ring-home-security-facial-recognition/> accessed 30 November 2019.

[20] Shoshana Zuboff, 'Big Other: Surveillance Capitalism and the Prospects of an Information Civilization' (2015) Journal of Information Technology 30, 75–89 < https://doi.org/10.1057/jit.2015.5.> accessed 30 November 2019.

[21] Frank Pasquale, *The Black Box Society: The Secret Algorithms That Control Money and Information* (Harvard University Press 2015).

[22] European Data Protection Board, 'Guidelines' (25 May 2018) <https://edpb.europa.eu/our-work-tools/our-documents/publication-type/guidelines_en> accessed 30 November 2019.

[23] Jef Ausloos, René Mahieu, and Michael Veale, 'Getting Data Subject Rights Right' (25 November 2019) <osf.io/preprints/lawarxiv/e2thg> accessed 30 November 2019.

[24] James Vincent, 'The Problem with AI Ethics' *The Verge* (3 April 2019) <https://www.theverge.com/2019/4/3/18293410/ai-artificial-intelligence-ethics-boards-charters-problem-big-tech> accessed 30 November 2019.

[25] Adam Satariano and Matina Stevis-Gridneff, 'Big Tech's Toughest Opponent Says She's Just Getting Started' *New York Times* (19 November 2019) <https://www.nytimes.com/2019/11/19/technology/tech-regulator-europe.html> accessed 30 November 2019.

[26] Sylvie Delacroix and Neil D Lawrence, 'Bottom-up Data Trusts: Disturbing the 'one size fits all' Approach to Data Governance' (2019) *International Data Privacy Law* <https://doi.org/10.1093/idpl/ipz014> accessed 30 November 2019.

[27] Databox <https://www.databoxproject.uk/> accessed 30 November 2019.

[28] Jumbo Privacy <https://www.jumboprivacy.com/> accessed 30 November 2019.

[29] DoNotPay <https://donotpay.com/> accessed 30 November 2019.

[30] Luciano Floridi, 'Group Privacy: A Defence and an Interpretation' in Linnet Taylor, Luciano Floridi, and Bart van der Sloot (eds), *Group Privacy: New Challenges of Data Technologies* (Springer International Publishing 2016).

[31] Joseph Raz, *The Morality of Freedom* (Oxford University Press 1986).