King's Research Portal

DOI:

[10.1093/idpl/ipz012](https://doi.org/10.1093/idpl/ipz012)

Document Version

Peer reviewed version

[Link to publication record in King's Research Portal](#)

Citation for published version (APA):

Keller, P. (2019). The reconstruction of privacy through law: a strategy of diminishing expectations. *International Data Privacy Law*, 9(3), 132-152. <https://doi.org/10.1093/idpl/ipz012>

Citing this paper

Please note that where the full-text provided on King's Research Portal is the Author Accepted Manuscript or Post-Print version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version for pagination, volume/issue, and date of publication details. And where the final published version is provided on the Research Portal, if citing you are again advised to check the publisher's website for any subsequent corrections.

General rights

Copyright and moral rights for the publications made accessible in the Research Portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognize and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the Research Portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the Research Portal

Take down policy

If you believe that this document breaches copyright please contact librarypure@kcl.ac.uk providing details, and we will remove access to the work immediately and investigate your claim.

The Reconstruction of Privacy through Law: A Strategy of Diminishing Expectations

Perry Keller
Reader in Media and Information Law
Dickson Poon School of Law
King's College London

The reconstruction of privacy through law: A strategy of diminishing expectations

King's College London Law School Research Paper No. 2018-23

Perry Keller

In a time of rapid development in privacy and data protection laws, the state of urban life has much to tell us about their long run effectiveness. Compared to even the recent past, major cities have largely lost the definitive public anonymity and obscurity that has characterised urban life for centuries. Saturated with sensors networked to powerful data analytics, they are at the epicentre of an ongoing revolution in governmental and commercial surveillance. In short, the future radical transparency of all human life is already emerging in our major cities.

This paper addresses a crucial question. Given a hundred years of privacy and then data protection law, how did this happen? In this paper, I argue that the explanation for this long running failure lies substantially in the wider political economy of information law, which

continues to shape and limit the capacities of privacy and data protection law. The prevailing liberal democratic model of information law is structured around two key concerns: protecting the state's powers of ultimate access to information and ensuring that all information remains potentially marketable. The particular vulnerability of personal information to demands for state and market access is, however, much more than a matter of political and economic power imbalances. Information law has developed through a dynamic relationship between governmental and commercial information uses and the continuous application of new technologies that render information more accessible and usable.

Over the long history of privacy and data protection laws, technologies have thus played a uniquely important role in catalysing the erosion of existing personal information protections and creating opportunities for strengthening access rights. The formidable privacy of physical circumstances, which was an ordinary and often unremarkable feature of life, has been gradually eroded away. The contested re-construction of that privacy through law has been, in comparison, porous and compromised.

I explain this claim through three illustrations: First, in the transformation of the concepts of public space and public domain, which are frequently used to justify access to personal information with minimal safeguards; Second, in the conflict within the principles of individual consent and choice, which provide the cornerstone for both personal autonomy and marketability of information; and, Third, in the comparative structural weaknesses of privacy and data protection laws as a field within the wider sphere of information law.

Whether societies find more effective boundaries against further transparency or even change the governance of how personal information is accessed and used in conditions of transparency are primarily political and economic questions. Constructive changes in law and regulation can, however, feed into those wider processes of decision making. In its final part, the paper discusses ways in which important elements of privacy and data protection laws could be used more effectively. This includes current efforts to use diverse forms of collaborative public scrutiny and accountability to challenge information law's embedded preferences towards access and use. Cities, not surprisingly, remain the test bed for success or failure.

Radical transparency and the priorities of information law

Cities have much to tell us about the global transformation towards a radical transparency of human life. Across the globe, major cities are saturated with myriad data gathering sensors embedded in every surface and device, from streets and buildings to vehicles and smartphones. Urban infrastructures and services, which were once entirely separate, are now integrated within overlapping, opaque governmental and commercial information systems that continuously extract and analyse vast arrays of data.¹

Anyone now present in a major city is ever more identifiable and traceable as gaps in surveillance networks narrow and disappear.² The anonymity that characterised urban life for centuries is vanishing.³ Historic distinctions between public and private urban spaces, which have been vitally important to social and legal norms, are also collapsing.⁴ This is, moreover, a highly intrusive form of transparency in which the goal of universal identifiability and traceability is to modulate behaviour, either individually or collectively.⁵

Data analysis, previously well downstream from data extraction, is progressively at the forefront of urban services, determining which individuals or which patterns of behaviour merit which selective response.⁶ Contemporary surveillance thus often includes the simultaneous singling out of particular personal attributes, habits and preferences at the point of data capture.⁷ This rich stream of direct and derived personal information drives a myriad of governmental and commercial decisions, which are variously intended to deter or

¹ M. Batty, 'Data About Cities: Redefining Big, Recasting Small' *CASA Working Paper Series* 203 (2015) < <https://www.ucl.ac.uk/bartlett/casa/case-studies/2015/aug/casa-working-paper-203>> accessed 26 June 2019

² R. Binns, U. Lyngs, M. van Kleek, J. Zhao, T. Libert and N. Shadbolt, 'Third party tracking in the mobile ecosystem', Proceedings of the 10th International ACM Web Science Conference (2018), arXiv:1804.03603 [cs.CY]; Consumer Council of Norway (ForbrukerRadet), 'Every Step You Take - How deceptive design lets Google track users 24/7', 27 November 2018 < <https://fil.forbrukerradet.no/wp-content/uploads/2018/11/27-11-18-every-step-you-take.pdf>> accessed 26 June 2019

³ K. Haggerty and R. Ericson, 'The Surveillant Assemblage', *British Journal of Sociology*, Vol 51, 4, (2000) 605, at 619; M. Froomkin, 'Lessons Learned Too Well: Anonymity in a Time of Surveillance', (2017) 59 *Arizona Law Review*, 95

⁴ M. Graham, M. Zook and A. Boulton, 'Augmented reality in urban places: Contested content and the duplicity of code', (2013) 38 *Transactions of the Institute of British Geographers* 3, 464

⁵ T. Zarsky, 'Privacy and Manipulation in the Digital Age', (2019) *Theoretical Inquiries in Law*, 1, 157; Council of Europe, Committee of Ministers, Declaration on the manipulative capabilities of algorithmic processes, (13 February 2019), Decl(13/02/2019)1

⁶ A. Wilson, 'The future will be data-driven', *Prospect Magazine*, 10 September, 2017

⁷ A. McStay, *Emotional AI: The Rise of Empathic Media*, (Sage 2018)

encourage individuals towards preferred outcomes.⁸ In short, selection for decision has become inseparable from the creation of digital identities.

There are, undoubtedly, many variations in the global shift towards radical transparency. National wealth and politics matter greatly in both capacities and willingness to create ubiquitous data driven surveillance. China's major cities, for example, are at the forefront of systematic governmental and commercial surveillance, having plentiful financial and technical resources as well a policy environment so far comparatively unrestrained by data privacy laws.⁹ Yet even in countries where technical capacities and governmental capabilities are not as well developed as those available in China, the smartphone and other sensor technologies are rapidly increasing identifiability.¹⁰

Within any urban population, degrees of surveillance and access to privacy protections also vary greatly. Those enjoying greater wealth and education are typically better placed to limit the extent of commercial surveillance.¹¹ Indeed, privacy and data protection laws assume high levels of education as well as ample time to consider and arrange privacy protections.¹² For the poor, trading privacy for access to services is often inescapable.¹³ Governmental surveillance, moreover, is often targeted at particular groups or communities, who are frequently less affluent or politically influential.¹⁴ Yet, comparable to local variations in global environmental decline, these important differences do not change the unmistakable trend.

The long running transformation towards radical urban transparency begs a crucial question. Given a hundred years of accumulated privacy and data protection laws, how could this have

⁸ F. Pasquale, 'The Algorithmic Self', (2015) 17 *The Hedgehog Review*, 1

⁹ S. Denyer, 'Beijing bets on facial recognition in a big drive for total surveillance', *The Washington Post*, 7 January 2018; R. Chun, 'China's New Frontiers in Dystopian Tech', *The Atlantic*, April 2018

¹⁰ N. Ni Loideain, 'Cape Town as a Smart and Safe City: Implications for Governance and Data Privacy', (2017) 7 *International Data Protection Law*, 4, 314

¹¹ M. A. Franks, 'Democratic Surveillance', 30 *Harvard Journal of Law and Technology* 425 (2017); A. Hess, 'How Privacy Became a Commodity for the Rich and Powerful', *New York Times*, 19 May 2017.

¹² E. Morozov, 'We all have the 'right to disconnect' – but only some of us can afford it', *The Guardian*, 9 February 2017

¹³ M. Madden, M. Gilman, K. Levy, and A. Marwick, 'Privacy, Poverty and Big Data: A Matrix of Vulnerabilities for Poor Americans', (2017) 95 *Washington University Law Review* 53; K. Bridges, *The Poverty of Privacy Rights*, (Stanford University Press, 2017) Chpt 4

¹⁴ J. Hendrix, T. Taniguchi, K. Strom, K. Barrick and N. Johnson, 'The Eyes of Law Enforcement in the New Panopticon: Police- Community Racial Asymmetry and the Use of Surveillance Technology', (2018) 16 *Surveillance & Society* 1, 53

happened? The answer lies in the dynamic nexus between the pursuit of governmental and commercial goals and the application of information and communication technologies. Within that nexus, the demand for more and better connection, convenience and security in individual lives has also been an essential force. Even so, willing populations and embedded information technologies combined with governmental and commercial imperatives to maximise data flows are not sufficient to create cities of perpetual surveillance. This extraordinary transformation could not have begun or now continue without the sustained support of a system of information law that is structured to facilitate governmental and commercial access and use of personal information.

In this paper, I argue that the explanation for this long running failure lies substantially in the wider political economy of information law, which shapes and limits the capacities of laws intended to protect personal information.¹⁵ Information law, in this context, broadly refers to the rights and powers that enable access and use of information, in whatever form, in the face of competing rights, powers or duties. Understood in this way, information law encompasses property rights that protect the control of information as well as statutory, contractual or other duties that create obligations of state secrecy, commercial confidentiality, information privacy, data protection and professional privilege, which also sustain information control. In this sense, information law does not describe a discrete field of law, but is instead a framework useful for critically analysing the relationship of law and information.

As this paper charts in more detail below, the prevailing liberal democratic model of information law is historically structured around two key concerns. First, information law has invariably protected the state's powers of ultimate access to information. Such powers are essential to the state's capacity to protect itself from existential threats and the public from violence and other major harms. Legal protections from the information access powers of state agencies are thus always contingent on that priority. The contentious questions, at least for liberal democracies, concern the conditions that limit the speed and scope of state access.

¹⁵ This argument has affinities with other recent scholarship on political economy and law and their application to the control and use of information. See, for example, J. Cohen, 'Property and the Construction of the Information Economy: A Neo-Polanyian Ontology', in (L. Lievrouw and B. Loader eds) *Routledge Handbook of Digital Media and Communication in Society*, (Routledge, forthcoming 2021); Jathan Sadowski, 'When data is capital: Datafication, accumulation, and extraction', (2019) 6 *Big Data & Society*, 1

Information law's second dominant concern has been to ensure that, as much as possible, information of all kinds is potentially marketable. The rise of liberal market economies, including the more recent development of information economies, could not have occurred without such ready marketability of information. This has meant that legal mechanisms freeing information for acquisition, trade and other uses have needed to be simple, flexible and broadly applicable. Consequently, legal rights that protect personal information, such as privacy and data protection rights, at the same time attempt to provide clarity and efficiency for commercial modes of access and alienation of such information.

The particular vulnerability of personal information to demands for state and market access is not simply a story of powerful organised interests persistently overcoming individual rights. Over the long history of privacy and data protection laws, technologies have played a uniquely important role in catalysing the erosion of existing personal information protections and creating opportunities for strengthening access rights. Seen from that perspective, the political economy of information law is deeply concerned with the adjustment of law to new technologies that render information more accessible and usable for governmental and commercial interests.

As I explain in the following sections, successive technologies adapted to governmental and commercial purposes have enabled the progressive destruction of the natural and social barriers that previously hindered access to personal information. In short, the formidable privacy of circumstances, which was an ordinary and often unremarkable feature of life, has been gradually eroded away in an as yet unfinished process.¹⁶ The contested re-construction of privacy through law has been, in comparison, porous and compromised.

Since the beginnings of the industrial age, new technologies facilitated the governmental and commercial destruction of circumstantial privacy. Communication services, from pre-industrial postal services to telegraph and then telephone services, drew private communications out of protected places and made them vulnerable to interception. In contrast, technologies of observation and disclosure, from the fixing of images by camera to industrial printing, diminished the privacy of circumstances by overcoming barriers to observation, such as physical distance and the weaknesses of human memory. Once images

¹⁶ For a similar description of the historical transition from the privacy of circumstances to constructed privacy, see S. Igo, *The Known Citizen: A History of Privacy in Modern America* (Harvard University Press, 2018), chpt one

could be captured and printed, not only did the importance of these barriers fade, but the volume of recorded personal information began to increase exponentially. It is certainly true that technologies can also create circumstantial privacy, typically through incidental or designed anonymity in new forms of communication. Yet, such is the value of identifiability that over time laws, technologies and other means are invariably found to circumvent these novel forms of privacy.¹⁷

The erosion of circumstantial privacy through the adaptation of new technologies to governmental and commercial purposes has been central to two closely related, but also quite distinct, lines of development: the progressive theorisation of privacy and, second, the steady accretion of laws protecting personal information from unjustifiable access and use. The flourishing of privacy theories has paradoxically enriched public discourse while weakening the conceptual clarity of legislative or judicial efforts to protect personal information.

Among the many influences on theories of privacy over the past century, the effects of new technologies enabling further access, collection and use of personal information have been especially important.¹⁸ Once relatively simple and coherent, ideas of privacy have grown into a contemporary profusion of complementary and conflicting concepts.¹⁹ Broadly described, privacy theories have moved outward from early ideas about personal spheres of information control, often related to private spaces or possessions, to more complex relational and societal descriptions that vary considerably in their relationship with liberalism.²⁰ This diversity in privacy theories now enriches and complicates the relationship between the creation and application of legal protections for personal information and the parallel intellectual discourse of privacy.

¹⁷ See, O. Kerr and B. Schneier, 'Encryption Workarounds', (2018) 106 *Georgetown Law Journal* 989

¹⁸ See, for an early example, S. Warren and L. Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 194. For more recent examples, see, M. Richards, 'The Dangers of Surveillance', (2013) 126 *Harvard Law Review* 1934, at 1962 and D. Citron and D. Gray, 'Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards', (2013) 126 *Harvard Law Review* 262

¹⁹ This progression can be seen in A. Westin, *Privacy and Freedom*, (Atheneum Press, 1967); D. Solove, *Understanding Privacy*, (Harvard University Press, 2008); and, B. Koops, B. Clayton Newell, T. Timan, I. Skorvák, T. Chokrevski, & M. Galic, 'A Typology of Privacy', (2017) 38 *University of Pennsylvania Journal of International Law*, 2, 483. On privacy as a constructed and contested concept, see D. Solove, 'Conceptualizing Privacy', (2002) 90 *California Law Review*, 1087; D. Mulligan C. Koopman, N. Doty, 2016 *Privacy is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy*. (2016) 374 *Philosophical Transactions of the Royal Society*, 2083.

²⁰ C. Fried, *An Anatomy of Values: Problems of Personal and Social Choice* (Cambridge, Mass., 1970), 137; P. Regan, *Legislating Privacy: Technology, Social Values and Public Policy*, (Chapel Hill: The University of North Carolina Press, 1995); J. Cohen, 'What Privacy is For', (2013) 126 *Harvard Law Review*, 1904. B. Roessler (Rössler) and D. Mokrosinska, *The Social Dimensions of Privacy* (Cambridge University Press, 2015)

The complex interdisciplinary evolution of privacy theory is evident in the increasing diverse understandings of autonomy and dignity as core normative and descriptive values in concepts of privacy.²¹ In part, this has been a logical and functional expansion of ideas about personal control over information as a protective barrier against unjustifiable and harmful uses. When autonomy is identified as having that function, the theorisation of privacy becomes bound up in changing information technologies.²² As novel ways to use personal information have created new risks of harm to the individual, including most recently the negative effects of profiling and associated choice modulation, the idea of privacy as autonomy has necessarily expanded outwards and diversified.²³

For some privacy theorists, however, widening our understanding of privacy is not simply a functional extension of ideas about informational autonomy or even dignity to new governmental or commercial applications of technology. It is more importantly a recognition of collective or societal interests in information privacy, which either reject or extend liberalism's core focus on the autonomy of the individual.²⁴ These interests prominently include the question of how ubiquitous surveillance is re-shaping democratic participation and dissent.²⁵ As Cohen has argued, governmental and commercial regimes of surveillance and modulation diminish our capacity for democratic self-government.²⁶ Instead of resistance, Cohen argues that ubiquitous surveillance more often normalises surveillance in the minds of the public and leads to an instilled passivity.²⁷ Other theorists have identified a strong connection between privacy's political importance and the neo-republican concept of domination.²⁸ This connection has been particularly important in moving beyond the simple

²¹ B. Rössler, *The Value of Privacy*, (Polity Press, 2005), at 17 and 140; *Report of the Special Rapporteur on the right to privacy*, J. Cannataci, UN Doc. A/HRC/31/64, (2016), para. 24; J. Whitman, 'The Two Western Cultures of Privacy: Dignity v Liberty' (2004) 113 *Yale Law Journal* 6, 1151; E. Eberle, 'Human Dignity, Privacy and Personality in German and American Constitutional Law', (1997) *Utah Law Review*, 963

²² R. Calo, 'The Boundaries of Privacy Harm', (2011) 86 *Indiana Law Journal*, 3, 1132

²³ J. Cohen, 'What Privacy is For', 126 *Harvard Law Review*. 1904; R. Calo, 'Artificial Intelligence Policy: A Roadmap', (2018) 51 *UC Davis Law Review*, 399, 420

²⁴ See, for example, M. Hu, 'Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test', (2017) 92 *Washington Law Review* 1819, at 1903

²⁵ On the impact of surveillance, see, J. Penney, 'Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study', (2017) 6 *Internet Policy Review*, 2, 1

²⁶ J. Cohen, n 23 above

²⁷ J. Cohen, 'Privacy, Visibility, Transparency, and Exposure', (2008) 75 *University of Chicago Law Review* 181

²⁸ J. Hoye and J. Monaghan, 'Surveillance, Freedom and the Republic', European (2015) 9 *Journal of Political Theory*, 1, 25. But see also, T. Stahl, 'Indiscriminate Mass Surveillance and the Public Sphere', (2016) 18 *Ethics and Information Technology*, 1, 33

oppressiveness of surveillance to identify data driven modulations of personal decision making as a form of domination that is also a specific privacy concern.²⁹

Alongside the evolution of theories of privacy, the second development arising out of the erosion of circumstantial privacy through the application of new technologies has been the steady accretion of laws protecting personal information. That accretion has grown through recurring interventions intended, among other things, to allay concerns about privacy and security in the face of novel technologies and services. The judicial and legislative creation of privacy torts in American law, encouraged in part by the scholarly proposals of Warren and Brandeis and later those of Prosser, is an early example of this process of accretion.³⁰

To continue the argument I summarised above, the evolution of laws and regulatory measures that protect personal information can be usefully described as a partial re-construction of privacy through law. In a limited sense, this could also be described as the incremental re-construction of an eroding social good. That description, however, does not properly take into account the structural priorities of information law to ensure that personal information remains subject to the state's powers of ultimate access or that any new legal protections do not foreclose the potential marketability of personal information. In this inhospitable environment, privacy and later data protection laws have been unavoidably defensive in their mode of development and conservative in their nature, never fully re-creating the privacy of circumstances they aim to replace. Quite the reverse, these deep structural compromises have instead paved the way for the growing radical transparency of contemporary urban life.

A defensive and cautious history

The contested and partial re-construction of privacy through law has grown in increasing density and complexity over the past century. This can be illustrated in three overlapping phases in the growth of legal protections for personal information in liberal democracies over the past century, which are summarised in this section. This illustrative model does not to claim that the liberal democratic world has moved in lock step in this path of legal development. There are undoubtedly messy variations and divergent paths, which this

²⁹ A. Roberts, 'Why Privacy and Domination?', (2018) 4 *European Data Protection Law Review*, 1, 5

³⁰ S. Warren and L. Brandeis, n 18 above; W. Prosser, 'Privacy', (1960) 48 *California Law Review*, 383

comparative account describes. I only assert that there are also broad consistencies in the European and American models.

The first of these phases in the modern re-construction of privacy began when ideas of privacy were initially formalised into law as a distinct concept. Historically, physical or social circumstances that afforded the protection of personal information from unwanted access always required law to maintain their effectiveness. Exclusive rights to forms of property capable of protecting privacy or confidentiality from observation or access, such as buildings or luggage, for example, have been critical to the protection of personal information since such rights first emerged in ancient law. In the development of the common law, these included criminal offences regarding burglary, robbery and larceny as well as private law remedies for trespass to land, goods and the person.³¹ Contemporary laws against unauthorised computer access and misuse provide a similar property based protection of information privacy.³²

Property rights were, however, much less effective in ensuring the protection of confidential or personal information sent through new public or commercial communication services, notably including national post, telegraph, telephone and, most recently, internet services. The need to protect these long distance communication systems, which were at high risk of unauthorised disclosure by employees or interception by other parties, lead to successive legal prohibitions against third party access as each service developed.³³

The adaptation of new communication and publication technologies to governmental and commercial purposes also spurred interest in the notion of private law rights to privacy, which would give individuals the means to prevent unwarranted access, disclosure or other unjustifiable proximate uses of their personal information. In European civil law, private law

³¹ M. Tugendhat, Chapter 10: 'Private and Family Life, Home and Correspondence', *Liberty Intact – Human Rights in English Law*, (Oxford University Press, 2016)

³² See, for example, Computer Misuse Act 1990, C.18 (U.K.) and Computer Fraud and Abuse Act (18 U.S.C. § 1030) (U.S.A.)

³³ In Britain, for example, the Proclamation of May 25th, 1663 forbid the opening of any letters or packets by anyone, except by the immediate warrant of the Principal Secretary of State, Report of the Committee of Privy Councillors appointed to inquire into the interception of communications, (Birkett Committee) 1957, Cmnd 283. Stealing letters, packets or bags of mail was later made a specific offence under the Post Office Offences and Isle of Man Postage Act 1767, 7 Geo 3 c.50, Section II. In the United States, the confidentiality of postal correspondence was established in law by the Post Office Act of 1792. That principle was adopted in subsequent federal legislation concerning other communications services. See, for example, the Omnibus Crime Control and Safe Streets Act of 1968, Title 18 U. S. C. § 2511(I)(a)

rights protecting personal information advanced cautiously in the face of conceptual and textual gaps. Without a specific civil code right to information privacy, there was instead an early focus on proprietary interests in personality rights, such as a person's name, image and likeness.³⁴ Doctrinal opposition to compensation for non-pecuniary harms was eventually overcome to enable the application of personality rights to prevent and compensate unauthorised third party uses of personal information.³⁵ As mentioned above, the earlier accumulation of various privacy oriented torts in American law took decisive shape under Prosser's categorisation of four specific privacy torts.³⁶ Other common law countries, such as Britain and Canada resisted these innovations, relying instead on duties of secrecy and equitable rights of confidentiality to address information privacy concerns until the more recent intervention of fundamental rights law.³⁷

Over the past half century, as liberal democratic legal systems were re-shaped through the constitutionalisation of fundamental rights, the re-construction of privacy through law entered a new phase. In Europe, this process gathered pace quite slowly as key national and European courts gradually asserted their authority over human rights instruments newly created after the Second World War. In 1983, for example, the Federal Constitutional Court of Germany broke critical ground when it recognised that core constitutional rights to human dignity and free development of personality contained a right of 'informational self-determination'.³⁸ This juridical concept remains a cornerstone for German laws protecting personal information, enabling new forms of redress for harms arising out of consequential uses.³⁹

Delayed procedurally and doctrinally, the interpretation of the European Convention on Human Rights (ECHR) followed Germany in a broadly parallel fashion through case law innovations of the European Court of Human Rights (ECtHR).⁴⁰ The ECHR Article 8 right to

³⁴ G. Bruggemeier, 'Protection of Personality Rights in the Law of Delict/Torts in Europe: Mapping out Paradigms', *Personality Rights in European Tort Law*, in (G. Bruggemeier, A. Columbi Ciacchi and P. O'Callaghan, ed's), (Cambridge University Press, 2010), 5

³⁵ German Civil Code (Bürgerliches Gesetzbuch), Section 823 – Liability in Damages

³⁶ W. Prosser, n 30 above

³⁷ A. Goodhart, 'Restatement of the Law of Torts, Vol. IV: A Comparison between American and English Law', (1943) 91 *University of Pennsylvania Law Review* 487; *Kaye v Robertson* [1991] FSR 62

³⁸ 65 BVerfGE 1, 41-52 (1983), (the Census case); E. Eberle, 'Observations on the Development of Human Dignity and Personality in German Constitutional Law', (2012) 33 *Liverpool Law Review* (33) 201

³⁹ A. Rouvroy and Y. Pouillet, 'The Right to Informational Self-Determination and the Value of Self-development, Reassessing the Importance of Privacy for Democracy', in S. Gutwirth, Y. Pouillet, P. De Hert, C. Terwangne, S. Nouwt (eds) *Reinventing Data Protection?*. (Springer, Dordrecht, 2009) 45.

⁴⁰ *Niemietz v Germany*, [1992] 16 EHRR 97

respect for private and family life, home and correspondence only developed its full significance for the re-construction of privacy through law in Europe when the Court began to apply Article 8 protections for personal information to private as well as governmental parties.⁴¹ As discussed in more detail below, that doctrinal change enabled the Court to set governing principles for both governmental and commercial surveillance, overcoming historical and conceptual barriers to the more effective protection of privacy in domestic law.⁴² European fundamental rights protections for personal information were later both strengthened and complicated by the EU Charter of Fundamental Rights (CFR), whose drafters included not only a restatement of the ECHR right to privacy but also a novel fundamental right to the protection of personal data.⁴³

In the United States, Fourth Amendment rights against unreasonable search and seizures, which form the backbone of U.S. constitutional protections for personal information, have been part of the federal Constitution since 1792. It was, however, only in the past century as law enforcement agencies adopted new technologies of surveillance and communications interception that the U.S. Supreme Court developed doctrinal principles that moved beyond the Fourth Amendment's originating concept of physical trespass.⁴⁴ The U.S. Constitution, moreover, only provides protections against actions of the state, which has severely limited the scope of its privacy protections under the Fourth Amendment or indeed under other constitutional provisions.⁴⁵ Unlike the ECtHR, Supreme Court has not recognised a principle of positive obligation on the state to create protections against private parties.⁴⁶

These striking transatlantic differences are, nonetheless, often outweighed by common structures and similar principles. As archetypical civil and political rights provisions, Article 8 of the ECHR and the Fourth Amendment to the U.S. Constitution are, for example, primarily directed at specific instances of harm affecting individuals rather than cumulative harmful effects on societal interests. In the privacy sphere, this focus on the individual has

⁴¹ *X and Y v. The Netherlands*, (1985) 8 EHRR 235; *Hannover v. Germany*, [2005] 40 EHRR 1, para 57

⁴² N. Moreham, 'Compensating for Loss of Dignity and Autonomy in the Misuse of Private Information Tort' in (J. Varuhas and N. Moreham eds) *Remedies for Breach of Privacy* (Hart Publishing, 2018).

⁴³ Charter of Fundamental Rights of the European Union, (2000/C 364/01), Articles 7 and 8; Charter of Fundamental Rights of the European Union, OJ 2010 C 83/389; C-362/14, *Maximillian Schrems v Data Protection Commissioner*, ECLI:EU:C:2015:650, para 38

⁴⁴ Most notably, in *Katz v. United States*, 389 U.S. 347 (1967)

⁴⁵ See, for example, *Lawrence v. Texas*, 539 U.S. 558 (2003)

⁴⁶ J. Mathews, 'State Action Doctrine and the Logic of Constitutional Containment', *University of Illinois Law Review*, Vol. 2017, No. 2, p. 655, 2017

given rise to a similar methods of determining the proper scope of the protective right, including the widely used juridical notion of a ‘reasonable expectation of privacy’.⁴⁷

The application of constitutionalised fundamental rights to the protection of personal information had hardly begun to produce mature legal principles when the re-construction of privacy through law entered its newest phase. Even by the early 1960’s, potential harms arising out of computerised database processing by governments and businesses, including such risks as data errors, unauthorised disclosures and innovations in fraud, were becoming a matter of public concern.⁴⁸ Governments in Europe and North America began to investigate the possibilities for regulating computerised processing of ‘personal information’, which was soon to be known in European law as ‘personal data’.⁴⁹ There are good reasons to see these early steps in data protection law as the beginning of a major divergence between Europe and the United States in the regulation of personal information processing and, indeed, the regulation of internet content more generally.⁵⁰

There are, plainly, many distinctively different elements in the European and American models for data protection / data privacy.⁵¹ In Europe, the public sector Hesse Data Protection Act of 1970 was the first legislation specifically directed at data processing. The German federal law that followed in 1977 covered both public and private sector data processing while also being firmly grounded in national fundamental rights law.⁵² In that same decade, the Council of Europe began its own first initiatives in this field, leading in 1981 to the first pan-European legal instrument governing data protection, an optional treaty on data protection frequently known as Convention 108.⁵³ The European Union, however, soon took the lead in establishing a mandatory data protection regime for its member states,

⁴⁷ See, for example, *Benedik v. Slovenia*, Application no. 62357/14 (ECtHR 24 April 2018) and *Carpenter v. United States*, 585 U.S. (2018) U.S. Supreme Court

⁴⁸ See, for example, V. Packard, *The Naked Society*, (David Mackay Publications, 1964)

⁴⁹ Council of Europe, Committee of Ministers Resolution (73) 22 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Private Sector (26 September 1973); Council of Europe, Committee of Ministers Resolution (74) 29 on the Protection of the Privacy of Individuals vis-a-vis Electronic Data Banks in the Public Sector (20 September 1974); *Council of Europe Convention 108*: Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data 1981, ETS 108 (Convention 108)

⁵⁰ K. O’Hara and W. Hall, ‘Four Internets: The Geopolitics of Digital Governance’, CIGI Paper No. 206, December, 2018.

⁵¹ P. Schwartz and K-N. Peifer, ‘Transatlantic Data Privacy’, (2017) 106 *Georgetown Law Journal*, 115

⁵² H. Burkert, ‘Privacy—data Protection: A German/ European Perspective,’ in (C. Engel and K. Keller ed’s) *Governance of Global Networks in the Light of Differing Local Values*, (Baden-Baden, *Nomos*, 2000), 60.

⁵³ Convention 108, n 49 above

which the EU has since promoted as a global model for the fair and lawful processing of personal information.⁵⁴ European data protection law, which is now centred on the EU General Data Protection Regulation (GDPR),⁵⁵ is strikingly comprehensive and unified, although increasingly complicated by parallel and subsidiary legislation, such as the Law Enforcement Directive and the proposed ePrivacy Regulation.⁵⁶ Often described as ‘user centric’, the GDPR is constructed around the protection of individual autonomy and dignity regarding the use of his or her personal information.

In comparison, data privacy legislation in the United States is undoubtedly an untidy patchwork. While initial American government concerns regarding data processing harms paralleled European developments,⁵⁷ the U.S. federal government quickly adopted a definitively sectoral approach to the regulation of data processing. Early initiatives concerned the processing of personal information in both private and public sectors, which for example lead to limits on personal information processing by credit reporting businesses under the Fair Credit Reporting Act of 1970 and by government departments and agencies under the Privacy Act of 1974.⁵⁸ These were, however, purely legislative and policy based measures. As noted above, the U.S. Constitution does not create rights directly enforceable against private parties and there is, moreover, no primary right of access to government held information, including the personal information of any applicant.⁵⁹ As a matter of statutory law, the 1974 Privacy Act creates access rights to personal information held by government entities, but fewer secondary rights than the GDPR.⁶⁰

⁵⁴ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ 1995 L 281/31 (Data Protection Directive); G. Greenleaf, ‘European’ Data Privacy Standards Implemented in Laws Outside Europe’, (2017) 149 *Privacy Laws & Business International Report* 21-23

⁵⁵ Regulation (EU) 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), OJ 2016 L 119/1

⁵⁶ Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, *OJ L 119, 4.5.2016*, (Law Enforcement Directive), and Proposal for a Regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC, COM/2017/010 final - 2017/03 (COD), (ePrivacy Regulation)

⁵⁷ P. Regan, *n 20 above*, chpt 7, Congress, Privacy and Policy Decisions, 174

⁵⁸ Fair Credit Reporting Act of 1970, 15 U.S.C. § 1681; U.S. Privacy Act of 1974, 5 U.S.C. § 552a

⁵⁹ *Houchins v. KQED*, 438 U.S. 1 (1978); *McBurney v. Young*, 569 U.S. 221 (2013)

⁶⁰ Privacy Act of 1974, 5 U.S.C. § 552a

Federal and state laws creating data privacy obligations for commercial or other private service providers are typically based on a consumer protection model.⁶¹ This is prominently reflected in the central role of the U.S. Federal Trade Commission, which is empowered to pursue sanctions against companies that engage in deceptive or unfair practices.⁶² The FTC's market based preference for reasonable notice and freely given consent is broadly shared across other American consumer focused privacy legislation.⁶³ Notice and consent is, for example, a key element in prominent state laws, such as the California Consumer Privacy Act of 2018 (CalCPA) and the Illinois Biometric Information Privacy Act of 2008.⁶⁴

Despite this sectoral approach to data privacy, which lacks consistently shared principles or comprehensive grounding in constitutional rights, American and European data protection laws and policies have significant similarities. These begin with shared concerns about the need to address accelerating intrusions into the privacy of the mind. While many of the historic barriers to access and use of personal information are long gone, data analytics are providing novel ways to reveal an individual's preferences, moods and intentions.⁶⁵ Current public debates about privacy harms are consequently often flow across the liberal democratic world, which is reflected in a shared range of ideas about the meaning of privacy in relation to data analytics and new judicial approaches to questions of surveillance and harm.⁶⁶

It is also apparent that the legal protection of personal information in liberal democracies has become increasingly regulatory and technical in nature. As discussed further below, European data protection laws, which are borne out of the EU's regulatory management of economic relations between member states, have become more paternalistic in character, requiring more intensive regulatory oversight. The European regulatory model for data

⁶¹ J. Brill, 'The Intersection of Privacy and Consumer Protection' in Selinger, Polonetsky and Tene (ed's) *The Cambridge Handbook of Consumer Privacy*, (Cambridge University Press, 2018)

⁶² Section 5(a) of the FTC Act, 15 U.S.C. § 45(a); See, for example, FTC consent order, In the Matter of FACEBOOK, INC.,) a corporation, File No 092 3184 (2011)

⁶³ C. Hoofnagle, 'The Federal Trade Commission's Inner Privacy Struggle', in (E. Selinger, J. Polonetsky and O.Tene, eds), *The Cambridge Handbook of Consumer Privacy* (Cambridge University Press 2018) Chpt 9; See, for example, *Children's Online Privacy Protection Act* of 1998 (*COPPA*) 15 U.S.C. §§ 6501

⁶⁴ California Consumer Privacy Act of 2018, California Civil Code, §1798; Illinois Biometric Information Privacy Act of 2008, 740 ILCS 14 et seq

⁶⁵ A. McStay, n 7 above

⁶⁶ See, for example, A. Mantelero, 'AI and Big Data: A Blueprint for a Human Rights, Social and Ethical Impact Assessment', (2018) 34 *Computer Law & Security Review*, 4 754, and M. Whittaker et al, *AI Now Report 2018*, AI Now Institute, New York University; Compare, Joined Cases C-203/15 and C-698/15 *Tele2 Sverige AB v Post- och Telestyrelsen and Secretary of State for Home Department v Tom Watson* [2016] ECR I-970 and *Carpenter v. United States*, n 47 above

protection is also enmeshed within the structure and interpretation of European fundamental rights law. This has occurred not only through the formal transformation of data protection legislation into the basis for Article 8 of the CFR, but is also evident in the case law of both the CJEU and the ECtHR, in which data protection legislation is frequently used to contextualise claims to information privacy.⁶⁷ In the United States, a regulatory approach to the protection of personal information is similarly embedded in key sectoral and state laws, such as the federal Health Insurance Portability and Accountability Act of 1996 and the more recent California Consumer Privacy Act.⁶⁸ While the U.S. Constitution lacks a general privacy right and does not carry positive obligations similar to the ECHR, there is nonetheless a similarly formative relationship between U.S. constitutional rights and federal or state legislation protecting personal information from unjustified access or use. First Amendment freedom of speech rights are, for example, a constant constraint on privacy laws or regulations that prohibit public disclosures of information,⁶⁹ while the Fourth Amendment has had a mutually defining relationship with law enforcement legislation for many decades.⁷⁰

The most significant convergent elements in European and American privacy and data protection laws, however, lie in their shared commitment to the conflicting goals of protecting personal information while also ensuring essential government access and efficient data markets.⁷¹ That joint commitment is evident in the 1980 OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, in which the economically advanced liberal democracies of the time pledged that national standards for the protection of personal information should not disrupt data flows.⁷² In this vein, the Guidelines sought to sustain the liberalisation of trans-border commercial flows of data, while also respecting the

⁶⁷ While Article 8 CFR was constructed out of the core features of the pre-existing Data Protection Directive, less explicitly, but in parallel, the ECtHR has relied on Convention 108, n 49 above, in its interpretation of Article 8 ECHR. See for example, *Benedik v Slovenia*, n 47 above

⁶⁸ Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); California Consumer Privacy Act, n 64 above

⁶⁹ *Sorrell v. IMS Health Inc.*, 564 U.S. 552 (2011)

⁷⁰ D. Gray, L. Donohue, T. Maclin, D Citron, M. Cloud, W. Cuddihy, N. Garland, Norman. M. Hu, R. Hutchins, L. Milligan, and G. Thomas, 'Brief of Scholars on the History and Original Meaning of the Fourth Amendment as Amici Curiae in Support of Petitioner in *Carpenter v. United States* (2017) Southwestern Law School Research Paper No. 2017-10 < <https://www.scotusblog.com/wp-content/uploads/2017/08/16-402-tsac-ScholarsOfTheHistoryAnd-OriginalMeaning.pdf>> accessed 26 June 2019

⁷¹ General Data Protection Regulation, n 55 above, Article 1(1), Recital 166. See also, European Commission, Communication on Building a Data Economy COM(2017) 9 final (January 2017); California Consumer Privacy Act, n 64 above; C. Hoofnagle n 63 above

⁷² Organisation for Economic Cooperation and Development (OECD), Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, Annex to the Recommendation of the Council - 1980

special status of national intelligence and law enforcement agencies. Despite recurring transatlantic confrontations over data flows since the OECD agreement, these baseline commitments have remained constant. They reflect the historic priorities of liberal democratic information law to safeguard the state's powers of ultimate access to information and the potential marketability of information.

In the following sections, I explain this claim through three illustrations: First, in the transformation of the concepts of public space and public domain, which are frequently used to justify access to personal information with minimal safeguards; Second, in the conflict within the principles of individual consent and choice, which provide the cornerstone for both personal autonomy and marketability of information; and, Third, in the comparative structural weaknesses of privacy and data protection laws as a field within the wider sphere of information law.

Information in public spaces and the public domain

The notions of 'public space' and 'public domain', especially when placed in urban environments, provide a key example of the evolution of information law concepts towards greater accessibility, shedding their historic ambiguities in favour of clarity in the rules of access. Two centuries ago, the crowded public spaces of cities offered many degrees of privacy along with their opportunities for public display and association. Being unknown in the crowd gave individuals the protection of anonymity and, even when recognised, the limitations of human observation and memory meant that participation in everyday public activities was quickly forgotten. Information was, moreover, not easily shared widely nor easily verified once shared.

In the contemporary city, obscurity in public has disappeared as identities are captured through a myriad of networked sensors.⁷³ CCTV cameras enabled for automatic vehicle number plate recognition and, increasingly, automatic facial or other biometric recognition of

⁷³ M. Brincker, 'Privacy in Public and the Contextual Conditions of Agency', in (T. Timan, B. Koops and B. Newell, eds.), in (T. Timan, B. Koops and B. Newell, eds.), *Privacy in Public Space: Conceptual and Regulatory Challenges*, (Edward Elgar, 2017), 64

individuals progressively ensure no one is lost in the crowd.⁷⁴ In the long transition towards instantaneous public identifiability, each technical erosion of circumstantial privacy has renewed the question of when personal information should be deemed publicly available in nature and therefore open to non-consensual collection and use. The legal concepts of public space and public domain are, consequently, becoming ever more technically defined.

Since the industrial revolution, one of the important functions of information law has been to ensure, as information becomes ever more abundant, accessible and usable, that the legal conceptualisation of information pursues the simplicity and clarity needed to enable access to new information resources. The reasons for that default towards access are usually simple enough. The governmental and commercial benefits of new information and communication technologies cannot be captured if the accessibility of information they enable is deemed unjustifiably intrusive per se. The state, for example, may reasonably argue that it cannot provide more effective public security without using the information access such new technologies enable, especially given the risks to the public created by the increasing scale and sophistication those same technologies bring to malign acts.⁷⁵

As a consequence, the legal repair of circumstantial privacy eroded by new technologies will never fully replace the privacy lost. The general default preference of information law towards access operates to privilege the observability and accessibility that new technologies make possible, while discounting the significance of the privacy of circumstances destroyed in the same moment. In this process, the background concepts of public space and public domain are dynamic and aggressive, flowing into spaces newly laid bare by surveillance enabling technologies. Any balancing between privacy and conflicting interests, consequently, takes place in a shifting context in which the historic background privacy has already been substantially conceded.

It is, however, only through the doctrinal mechanics of constitutionalised fundamental rights that notions of public space and public domain developed their now frequently decisive role in determining the limits of privacy. Out of previously fragmented public and private law

⁷⁴ C. Garvie, A. Bedoya, J. Frankle, 'The Pertual Line-Up – Unregulated Police Face Recognition in America', Georgetown Law Center on Privacy and Technology Report, (2016) 9; J. Lynch, 'Face Off – Law Enforcement Use of Face Recognition Technology', Electronic Frontier Foundation Report, (2018) 2

⁷⁵ O. Kerr, 'An Equilibrium-Adjustment Theory of the Fourth Amendment', (2011) 125 *Harvard Law Review*, 476

considerations affecting the legal protection of personal information, courts in much of the liberal democratic world have used fundamental rights to set principles applicable across diverse situations, determining the relative scope and weight of conflicting rights and interests in the information law sphere.

In European human rights law, public space and public domain are frequently determinative in two respects in the application of the ECHR Article 8 right to privacy. First, the preliminary question of whether an individual claiming infringement of the right enjoys a ‘reasonable expectation of privacy’ in the circumstances of the case may turn on the extent to which he or she disclosed personal information in a public space or otherwise voluntarily shared that information with others.⁷⁶ In her work, Kirsty Hughes shows that the external construction of ‘reasonable expectations of privacy’ is similarly essential when determining which matters are of legitimate public interest or who should be deemed a ‘public figure’.⁷⁷ Second, public space and public domain disclosures are also likely to be weighty factors in deciding consequent questions of necessity and proportionality.⁷⁸

The European Court of Human Rights has repeatedly asserted that individuals enjoy a reasonable expectation of privacy regarding personal matters even when in public places.⁷⁹ As the important *Von Hannover* cases illustrate, the recording and use of a person’s image obtained in public can be a vital privacy concern.⁸⁰ What is less often noted is the unstated principle, evident from ECHR case-law, that personal information collected in public spaces is not protected by Article 8 where there is a reasonable justification for its collection not outweighed by the sensitive nature of the information or the intrusiveness of the circumstances.⁸¹ Those justifications include the recording and analysis of images necessary

⁷⁶ *Benedik v. Slovenia*, n 47 above; See also, *Copland v. The United Kingdom*, ECtHR 45 EHRR 858

⁷⁷ Kirsty Hughes, ‘The Public Figure Doctrine and the Right to Privacy’, (2019) 78 *Cambridge Law Journal*, 70, 85.

⁷⁸ See, for example, *Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*, Application no. 72562/10, (ECtHR 22 February 2018); See, also, *Egeland and Hanseid v. Norway*, (2010) 50 E.H.R.R. 2

⁷⁹ See, for example, *Peck v. The United Kingdom*, (2003) 36 EHRR 41; *Hannover v. Germany*, (Application no. 59320/00, 24 June 2004) ECtHR, para 57

⁸⁰ *Von Hannover v. Germany*, *ibid*; *Von Hannover v. Germany* (no. 2), (2012) 55 E.H.R.R. 15

⁸¹ See, for example, *Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*, n 78 above, para 78. Compare this general rule with non-intrusive photos (of a baby) taken in a private place – *Reklos and Davourlis v. Greece*, [2009] ECHR 200, and intrusive photos taken in a public place – *Egeland and Hanseid v. Norway*, n 78 above

to safeguard the security of the workplace, protect the public from crime, or inform the public of current events.⁸²

That principle has, moreover, adjusted according to changing times. As the definitional boundaries of public space and public domain expand through the progressive erosion of circumstantial privacy, the baseline for factor balancing moves towards ever greater access to personal information. In this process, judicial applications of the Article 8 right to privacy are carried forward, focused on rational trade-offs between the benefits and costs of new technologies, but without reference to what privacy in such circumstances once meant. Plainly, building legal safeguards as human existence becomes increasingly transparent is an essential task. The problem lies in failing to acknowledge that that end destination is already significantly conceded by the process.

Victories in the courts vindicating Convention privacy rights should therefore be seen as occurring on this constantly shifting ground. This is readily apparent in challenges to state access to personal information for national security and criminal law enforcement purposes, which occupy a special place within the rules of European human rights law. The ECHR recognises the legitimate interests of states in national security, territorial integrity, public safety and for the prevention of disorder or crime, which are also recognised in similar terms in Council of Europe Convention 108 on data protection.⁸³ Given the importance of these governmental purposes and the frequent necessity for operational secrecy, ECHR Article 8 case-law permits states considerable latitude in shielding intelligence gathering and criminal investigations from direct public scrutiny.⁸⁴ State parties cannot, however, interfere with ECHR Article 8 privacy rights when acting for such purposes without showing lawfulness, necessity and proportionality.⁸⁵

In this area of law, the legal status of automated recording of information that potentially identifies individuals is developing rapidly. For several decades, government deployed

⁸² *Bărbulescu v. Romania*, [2017] ECHR 754); *Peck v. United Kingdom*, n 79 above; *Axel Springer Ag v. Germany*, (2012) 55 EHRR 6

⁸³ Convention 108, N 49 above, Article 9

⁸⁴ *Weber and Saravia v Germany*, (2008) 46 EHRR SE5

⁸⁵ *Roman Zakharov v Russia* (2015) ECHR 1065, para 231
; European Court of Human Rights, Factsheet: Mass Surveillance, February 2019)
https://www.echr.coe.int/Documents/FS_Mass_surveillance_ENG.pdf > accessed 26 June 2019

CCTV in streets and other public spaces has operated on the basis that images disclosed in such places may be recorded and used for legitimate purposes by the state.⁸⁶ Until recently, that position has gone relatively unchallenged, giving the application of new, more intrusive technologies the benefit of public space and public domain justifications.⁸⁷

These technologies are, however, a world away from the film loaded CCTV of the past. By combining automatic recognition of vehicle number plates or automatic recognition of facial and other biometric information over time and locations, networked street cameras and sensors offer highly specific identifiability, which potentially discloses detailed composite information regarding occupations, health and relationships.⁸⁸

Undoubtedly, there is increasing judicial recognition of the risk of individual harms and general chilling effects of government collection and analysis of enormous volumes of seemingly anodyne and inconsequential personal information. The ECtHR Grand Chamber, for example, decided a decade ago that indefinite bulk retention of sensitive personal information by police forces, including DNA records, without more specific and proportionate justifications is a violation of the Convention right to privacy.⁸⁹ The Court has similarly pursued the goal of tightening public and internal processes for approval and supervision of information interception and access by state authorities.⁹⁰ Yet, these minimum safeguards do not challenge the lawfulness of the state's coercive powers of ultimate access to personal information, provided that access is necessary and proportionate.

As restraints on state access, however, principles of necessity and proportionality are increasingly implicated in the applications of complex data analytics in areas cloaked by state secrecy, which provide limited purchase for judicial oversight and rule setting. Within the argumentation of necessity and proportionality, the pivotally important public space and

⁸⁶ See, for example, Home Office, Surveillance Camera Code of Practice, (June 2013)

<<https://www.gov.uk/government/publications/surveillance-camera-code-of-practice>> accessed 26 June 2019

⁸⁷ Surveillance Camera Commissioner, Annual Report 2017/18 <

<https://www.gov.uk/government/collections/surveillance-camera-commissioner-annual-reports>> accessed 26 June 2019; Technology and Law Public Policy Commission, *Algorithm use in the Criminal Justice System*, Law Society of England and Wales, June 2019, 39

⁸⁸ A. Babuta, 'Big Data and Policing: An Assessment of Law Enforcement Requirements, Expectations and Priorities', Royal United Services Institute for Defence and Security Studies, 2017

⁸⁹ *S. and Marper v the United Kingdom* (2009) 48 EHRR 50

⁹⁰ *Roman Zakharov v Russia* n 85 above; *Szabó and Vissy v. Hungary* [2016] ECHR 579 ; *Centrum För Rättvisa v. Sweden*, Application no. 35252/08 (ECtHR 19 June 2018); *Big Brother Watch and Others v. The United Kingdom*, Applications nos. 58170/13, 62322/14 and 24960/15 (ECtHR, 13 September 2018), para 307

public domain justifications for increased access to personal information have, for example, become virtually inseparable concepts. As communications connection and device location data are harvested simultaneously for commercial purposes, providing rich data flows potentially useful for state surveillance purposes, the potentially expansive boundaries of public space / public domain are vitally important, but also ever more esoteric.

The application of the EU Charter of Fundamental Rights by the CJEU has strengthened but also complicated judicial oversight of state surveillance at the European level. It is complicated, first, by the introduction of a separate fundamental right to the protection of personal data, which is modelled on the core principles of the EU data protection regulatory regime. This sits alongside the Charter right to privacy with considerable overlaps in areas of potential application. Second, the Charter is more limited than the ECHR in its applicability to state powers of access for national security and criminal law enforcement purposes.

As a general matter, the EU has limited legislative or judicial competence in matters of national security, which are reserved to member states.⁹¹ The CJEU has, nonetheless, established that the EU enjoys competence over national security related issues that arise in the application of EU law.⁹² This includes, for example, European Commission Decisions approving transfers of European personal data to countries not subject to EU data protection law.⁹³ As a result, the surveillance work of intelligence agencies of these countries, including the United States, is subject to indirect review by the CJEU while similar national security work carried out by EU member states is not.

Using this still significant sphere of legislative and judicial competence, the CJEU has decided several cases concerning the conditions for lawful state access to personal information held by communication providers.⁹⁴ Like the ECtHR, the Court has attempted to create safeguards for the protection of personal information in the face of rapid technological change. In doing so, the CJEU has needed to re-consider established distinctions between bulk collection versus access to personal information as well as distinctions between

⁹¹ Article 4(2) TEU.

⁹² Opinion of the Advocate General Saugmandsgaard Øe in the case C-203/15, *Tele2 Sverige*, ECLI:EU:C:2016:57, paras 73-80

⁹³ *Maximillian Schrems v Data Protection Commissioner*, n 43 above.

⁹⁴ Joined Cases C-293/12 and 594/12, *Digital Rights Ireland and Seitlinger and others*, [2014] E.C.R. I-238 ; *Maximillian Schrems v Data Protection Commissioner*, n 43 above; *Tele2 and Watson*, n 66 above.

communications content data versus communications traffic data (sometimes known as metadata).

Taking a broad view, the Court has pointed out that traffic and location data retained over long periods of time is, in relation to the right to privacy, no less sensitive than the actual content of communications as it is “liable to allow very precise conclusions to be drawn concerning the private lives of the persons whose data has been retained”⁹⁵ This, in essence, rejects traditional distinctions that would treat traffic and location data as less private in nature because they are akin to the observable addresses on a posted letter.

Like other courts, the CJEU can only address the parts of the personal information jigsaw that come before it. While the Court has taken a holistic approach to the significance of communications traffic and location data, that conclusion sits awkwardly with the Court’s more traditional distinctions between private and public spaces in other personal information settings.⁹⁶ Such inconsistencies are not merely an unavoidable product of the randomness of litigation, they reflect a deeper problem. The legitimacy of the state’s surveillance purposes logically flows forward to new surveillance enabling technologies and courts follow after, attempting to adapt or create suitable safeguards. Establishing safeguards does not, however, prevent the ongoing shift towards radical transparency.

In the United States, courts have travelled a parallel path, despite substantial textual and doctrinal differences with European fundamental rights. Most importantly, the protections of the Fourth Amendment to the U.S. Constitution encompass similar questions regarding the legitimacy of state access to personal information for national security and law enforcement purposes.⁹⁷

Current federal government authority for such access rests on laws that originate in earlier legislation protecting the security of telephone and other electronic communications.⁹⁸ This

⁹⁵ *Tele2 and Watson*, n 66 above, para 99

⁹⁶ Case C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, (11 December 2014) ECR I-0000, ECLI:EU:C:2014:2428

⁹⁷ D. Gray et al, n 70 above

⁹⁸ *Electronic Communications Privacy Act of 1986 (ECPA)*, 18 U.S.C. § 2510-22; A. Desai, ‘Wiretapping before the Wires: The Post Office and the Birth of Communications Privacy’, (2007) 60 *Stanford Law Review*, 2, 553; O. Kerr, ‘The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution’, (2004) 102 *Michigan Law Review* 801

federal legislation has given legal authority to a continually widening array of surveillance capabilities enabled by digital technologies. The Fourth Amendment's prohibition on unreasonable search and seizures raises the question of whether specific government surveillance methods are sufficiently intrusive to require the safeguard of a prior judicially approved warrant issued on the basis of reasonable cause. In that question of constitutional standards, concepts of public spaces and public domain have played a key role.⁹⁹

The protection against unreasonable searches or seizures is grounded in the Fourth Amendment's spatial and proprietary language, which refers to 'persons, houses, papers and effects'. In its 1967 decision in *Katz v. United States*, the U.S. Supreme Court moved beyond more literal interpretations of this phrase, famously declaring that 'the Fourth Amendment protects people, not places'.¹⁰⁰ Nonetheless, public place remains a key determinant in the reasonable expectation of privacy test introduced in *Katz*,¹⁰¹ which supplements but does not replace a property-based understanding of the Fourth Amendment.¹⁰² Quite apart from the presumption against an expectation of privacy in public places, the Fourth Amendment 'third party doctrine' applies a similar presumption to information voluntarily shared and thus entering the public domain.¹⁰³

More recently, the U.S. Supreme Court reached an apparent watershed in applying these categorical assumptions to new forms of electronic surveillance. In 2018, the Court, by a narrow majority, decided in *Carpenter v. United States* that law enforcement agencies seeking access to accumulated mobile phone location data must comply with Fourth Amendment judicial warrant and reasonable cause requirements.¹⁰⁴ Consistent with European courts, the majority expressed concern about the deeply revealing nature of such stored location data, noting that, 'time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.''¹⁰⁵ As the mobile phone location data at issue in *Carpenter* recorded much more than the appellant's movements across

⁹⁹ J. Reidenberg, 'Privacy in Public' (2014) 69 *University of Miami Law Review* 141.

¹⁰⁰ *Katz v. United States*, n 44 above

¹⁰¹ *United States v. Knotts*, 460 U.S. 276, 281 (1983)

¹⁰² *Katz v. United States*, n 44 above; *Florida v. Jardines*, 569 U.S. 1 (2013)

¹⁰³ *United States v. Miller*, 425 U.S. 435 (1976); *Smith v. Maryland*, 442 U.S. 735 (1979); O. Kerr, 'The Case for the Third-Party Doctrine', (2009) 107 *Michigan Law Review*, 561, 563-64

¹⁰⁴ *Carpenter v. United States*, n 47 above

¹⁰⁵ *Ibid*

obviously public places, the Court's decision was concerned more generally with the depth, breadth, and comprehensive reach of these records as well as the inescapable and automatic nature of their collection.

On that basis, the majority rejected the application of the third party doctrine, finding that the location data was not shared with the relevant service providers to the extent that there was a voluntary assumption of the risk of further disclosure. *Carpenter* is, consequently, a significant challenge to assumptions about what it means for personal information to be in the public domain. That also carries implicit challenges to restrictive concepts regarding reasonable expectations of privacy in public spaces where identities and activities have been revealed through communication or information services.

Yet, other key similarities with Europe should be observed. *Carpenter*, like all Supreme Court Fourth Amendment decisions, does not question the legitimacy of the state's ultimate access to information. It concerns the conditions of access, which are vitally important to the protection of personal information, but do not slow the ongoing dynamic relationship between state access and the erosion of circumstantial privacy. Like their European counterparts, U.S. courts are building safeguards while continuing to adapt aggressive notions of public space and public domain to novel exposures of personal life.

Autonomy and agency overwhelmed

Opportunities for individual consent and choice arise throughout the patchwork of laws and regulations that protect personal information. In the overlapping fields of privacy and data protection, which form the contemporary core of that patchwork, consent is a widely used condition for justifiable access or use. Choices, on the other hand, arise subsequent to either lawful or unlawful access and use, and include individual choices as to whether to exercise various secondary rights, such as correction and deletion rights, or to pursue potential remedies.¹⁰⁶ Consent and choice are thus essential to the design of these laws and their potential effectiveness. They are also, however, mechanisms for achieving the often conflicting purposes of personal autonomy and marketability in the control of personal

¹⁰⁶ See, for example, GDPR, n 55 above, Chapter 3; See also CalCPA, n 64 above, Section 1798.105 and 1798.120

information. This section looks at consent and choice as gateways to the marketability of personal information in the context of ever increasing informational complexity.

In liberal democratic information law, consent and choice provide direct applications of the concept of autonomy, while also demonstrating liberalism's preference for individual agency over paternalism.¹⁰⁷ In that vein, consent and choice are enabling devices intended to empower individuals to make appropriate decisions for themselves regarding potential benefits and harms. Yet, consent and choice in the protection of personal information also reflect the transactional importance of agency to the marketability of information.

The transactional dimension is most obvious in the case of consent. Many business models for online consumer services are, for example, based on the exchange of personal information for access to services through the mechanisms of consent.¹⁰⁸ Personal autonomy and agency are therefore often essential to the alienability of personal information in privacy and data protection laws, even though not recognised as a property right. Choice in relation to the exercise of secondary rights and remedies extends the potential for a transactional exchange. When offered sufficiently satisfying and convenient options by service providers, consumers will choose not to invoke those rights or remedies.

The mechanisms of individual consent and choice have, however, been gradually overwhelmed by the dynamic complexity of how personal information is now produced and used. That complexity includes the vastness of contemporary information flows, the extraordinary technical opacity of information processing, the resulting layered intricacies of relevant laws and regulations as well as the diversity of public discourse about privacy. Indeed, even the idea of 'personal information' has itself become increasingly complex and uncertain as an increasing range of data points, such as locations, purchases and app uses, are used to identify unique individuals.¹⁰⁹ In these circumstances, ideas of personal autonomy and agency often have no meaningful application. More specifically, overwhelming

¹⁰⁷ J. Cohen, 'Turning Privacy Inside Out' (2019) 20 *Theoretical Inquiries in Law*, 1

¹⁰⁸ C. Hoofnagle and J. Whittington, 'Free: Accounting for the Costs of the Internet's Most Popular Price', (2014) 61 *UCLA Law Review* 606

¹⁰⁹ N. Purtova, 'The law of everything. Broad concept of personal data and future of EU data protection law', (2018) 10 *Law, Innovation and Technology* 1, 40; S. Wachter and B Mittelstadt 'A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI' (2019) *Columbia Business Law Review*, 1

complexity has pushed the transactional nature of consent and choice further in favour of governmental and commercial service providers.

The problems of consent as an a gateway to lawful access or use of personal information are well known and need not be discussed in detail here. The informed consent model is widely known to work poorly in complex, digitised information environments, even when options are presented in good faith.¹¹⁰ An individual's capacity to absorb information and make reasoned decisions assumed by the informed consent model is therefore frequently overpowered by the volume and complexity of the decisions needed to manage information protections effectively.¹¹¹

The drafters of the GDPR were certainly aware of the problems of securing informed, meaningful consent.¹¹² There is, consequently, a deliberate push within the GDPR towards alternative bases for lawful processing, such as necessity for the 'performance of a task carried out in the public interest' or the 'legitimate interests pursued by the controller'.¹¹³ That push towards controller responsibility standards does not, however, avoid the underlying problem of new technologies and services whose novel benefits cannot be delivered without yet more access and use of personal information. These standards require a balancing of benefits and harms in a dynamic that accepts the need for at least some degree of access and use to enable more efficient and effective services.

Importantly, the GDPR alternatives to consent for lawful processing all lead to individual choice options regarding secondary rights and remedies. The mechanisms for individual choice within the rules of data protection law, however, share many of the information complexity problems of consent. Informed choice about the exercise of secondary rights or remedies requires a good understanding of what personal information is involved as well as the manner and purposes of processing, which frequently also requires technical and legal knowledge. Under the GDPR, consent and choice benefit from a robust principle of

¹¹⁰ F. Cate, 'The Failure of Fair Information Practice Principles', in (J. Winn, ed.) *Consumer Protection in the Age of the Information Economy* (Routledge, 2006); N. Richards and W. Hartzog, 'Taking Trust Seriously In Privacy Law', (2016) 19 *Stanford Technology Law Review* 431

¹¹¹ L. Cranor, 'Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice', (2012) 10 *Journal on Telecommunications and High Technology Law* 273, 274

¹¹² GDPR, n 55 above Articles 6-9, Recitals 32, 33, 42 and 43. See, also, Article 29 Working Party, Guidelines on Consent under Regulation 2016/679, WP/259

¹¹³ GDPR, *ibid*

transparency, which requires that mandatory information provided to data subjects be concise, transparent, intelligible and made available in an easily accessible form.¹¹⁴ While this user friendly notion of transparency has obvious benefits for advantaged individuals, it assumes capacities to understand and address the contextual complexities of personal information access and use that most citizens or consumers do not possess.¹¹⁵

In the United States, the California Consumer Privacy Act of 2018 is similar to the GDPR in enumerating rights of individuals, at least regarding commercial uses of personal information. The CalCPA does not, however, establish barriers to access and collection of personal information. Instead, the Act creates, in effect, choices for consumers to exercise rights to disclosure and deletion by the business that has collected or obtained their personal information as well as onward selling of that information.¹¹⁶ Even more so than the GDPR, the CalCPA leaves open the question of how individual choices regarding the exercise of rights in a complex information environment will lead to changes in commercial information practices. The consent and choice mechanisms of both GDPR and CalCPA also provide little answer to the observed indifference of many citizens and consumers to available information protections.¹¹⁷ While possibly regretting aspects of the societal transformation occurring around them, individuals often do not experience personal information harms sufficient to provoke them to more active agency.¹¹⁸

Beyond the technical complexities of information categorisation and processing, individuals are also expected to cope successfully with the increasing complexity of the laws that protect their personal information. European data protection law, for example, while centred on the GDPR is layered with parallel and subsidiary EU data protection legislation, including complex national implementation legislation. It is then further complicated by the EU's limited legislative competence relating to national security matters and reliance on fundamental rights in the dual ECHR and CFR regimes.

¹¹⁴ GDPR, *ibid*, Article 12. See also, Article 29 Working Party, Guidelines on Transparency under Regulation 2016/679 (WP260 rev.01)

¹¹⁵ On meaningful transparency, see, R. Brauneis and E. Goodman, 'Algorithmic Transparency for the Smart City', (2018) 20 *Yale Journal of Law and Technology*, 103

¹¹⁶ CalCPA, n 64 above, Sections 1798.105, 110, 115 and 120

¹¹⁷ *On voluntary exposure and indifference to privacy*, see, B. Harcourt, *Exposed: Desire and Disobedience in the Digital Age*, Cambridge, MA: Harvard University Press, 2015

¹¹⁸ N. Gerber, P. Gerber, M. Volkamer, 'Explaining the privacy paradox: A Systematic Review of Literature Investigating Privacy Attitudes and Behavior', (2018) 77 *Computers & Security*, 226

That legal complexity goes even further when one considers that European Union data protection law, allowing for gaps in legislative competence, is intended to be a comprehensive regime for the protection of personal information. EU data protection law, consequently, has significant and expanding interfaces with other laws that also govern questions of legitimate access and use of such information. These include laws concerning employment, scientific research, medical treatment and public health as well as arrest and criminal prosecution.¹¹⁹ Across these fields of law, EU data protection rights and duties override or condition their indigenous rules for information access and use. In each field, the question is therefore what does EU data protection law dictate and what does it accept.

The capacities of the GDPR to instil order across these interfaces is, moreover, open to doubt. The GDPR is arguably built around a conception of information processing that is incompatible with advanced machine learning and artificial intelligence.¹²⁰ The requirement that data processing is limited to specified purposes, for example, is difficult to apply to the multi-purpose processing of aggregated data common to large scale research.¹²¹ There is, as well, a concern that the GDPR as a law based regulatory mode of evaluation and decision making is unsuited to the challenges of regulating algorithmic decision making.¹²² Aside from the need to address the potential harmful consequences of data analytics, there is an underlying need for basic transparency and contestability in significant decisions that affect the public. Yet, computational processes of decision making involving advanced machine learning will often be incomprehensible, even if they can be made transparent.¹²³ Hildebrandt argues that the differences between legal and computational reasoning are so fundamentally incommensurable that the relevance of law to algorithmic governance is in doubt.¹²⁴ In her view, data driven decision making is not contestable in the terms essential to the rule of law, which depends on a legal rationality that is based on human reasoning.¹²⁵

¹¹⁹ GDPR, n 55 above, Articles 9, 88 and 89; Law Enforcement Directive, n 56 above, Article 6

¹²⁰ T. Zarsky, 'Incompatible: The GDPR in the Age of Big Data' (2017) 47 *Seton Hall Law Review*, 4(2) 995

¹²¹ S. Esayas, 'The Idea of 'Emergent Properties' in Data Privacy: Towards a Holistic Approach', (2017) 25 *International Journal of Law and Information Technology*, 139

¹²² R. Caplan, J. Donovan, L. Hanson, and J. Matthews, 'Algorithmic Accountability: A Primer', (2018) *Data & Society*; S. Wachter and B Mittelstadt, n 109 above

¹²³ M. Annany and K. Crawford, 'Seeing without knowing: Limitations of the transparency ideal and its application to algorithmic accountability', (2018) 20 *New Media & Society*, (3) 973

¹²⁴ M. Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Philosophy*, 2015; M. Hildebrandt, 'Law as Information in the Era of Data-Driven Agency', (2016) 79 *The Modern Law Review*, 1, 1

¹²⁵ M. Hildebrandt, 'Law as an Affordance: The Devil is in the Vanishing Point(s)', (2017) 4 *Critical Analysis of Law*, 1, 116, at 125

In comparison to the European Union, the patchwork of U.S. federal and state sectoral laws protecting the privacy of personal information has created an increasing confusion of gaps and inconsistent protections.¹²⁶ In the American sectoral approach to data privacy, the problem of complex legal interfaces is different but also acute. What the European Union and the United States do share is a fraught external legal interface governing transborder flows of personal information with each other as well as other national jurisdictions. To what extent the GDPR's alternative strategy of reducing potential inconsistencies in data protection standards through targeted extra-territorial applications is as yet largely untested.¹²⁷

Where legislation is complex and uncertain, it might be hoped that more clarity or coherence could be achieved through some consensus at the level of theory and public discourse. As discussed above, however, contemporary privacy discourse is complex and divergent, reflecting in some ways the contemporary political and social crises of liberal democracy. Without doubt, a broad intellectual discourse that seeks to explain and critique the erosion of circumstantial privacy and its partial re-construction through law is essential. Yet, the normative pluralism of the contemporary theorisation of privacy is also part of the deepening complexity of contemporary legal protections for personal information, in which personal autonomy and agency are intended to flourish.

The breadth and diversity of privacy theories creates two potential problems for privacy and data protection laws. Legal rights may be so closely framed around a historical conception of privacy that they are incapable of addressing new forms of informational harm. The American privacy torts identified by Prosser, for example, have been criticised as being frozen in the past.¹²⁸ Alternatively, more loosely phrased laws too readily absorb new conceptions and applications of privacy. Article 8 of the ECHR is a prominent example, capaciously sheltering all manner of privacies. As the ECtHR has stated, the Convention right to private life is incapable of exhaustive definition, embracing multiple aspects of the

¹²⁶ See, for example, the national importance of the Illinois Biometric Information Privacy Act, n 64 above, and national disputes regarding its scope: A. Schwartz, 'EFF to Illinois Supreme Court: Protect Biometric Privacy' Electronic Frontier Foundation, 5 July 2018

¹²⁷ GDPR, n 55 above, Article 3(2); I. Rubinstein and B. Petkova, 'The International Impact of the General Data Protection Regulation' (April 23, 2018), in (M. Cole and F. Boehm, eds), *Commentary on the General Data Protection Regulation*, Edward Elgar 2019, forthcoming)

¹²⁸ N. Richards and D. Solove, 'Prosser's Privacy Law: A Mixed Legacy' (2010) 98 *California Law Review*, 1924

person's social identity and physical, psychological or moral integrity as well as access or use of personal information.¹²⁹

The GDPR offers a different but equally perplexing way to address the growing dissonance between evolving legal protections for personal information and theories of privacy. In contrast to the 1995 EU Data Protection Directive, which repeatedly referred to the ECHR Article 8 right to privacy, the GDPR distances itself from that right.¹³⁰ In Recital 1, it states instead that the protection of personal data is a fundamental right in accordance with CFR Article 8. The GDPR is accordingly at one remove from debates over the proper scope of privacy in relation to consequential and novel harms involving misuses of personal information,¹³¹ although tied to the still uncertain meaning and scope of CFR Article 8 in relation to the fundamental right to privacy.¹³²

The distinctive Charter right to data protection was unusually framed around the key features of the EU Data Protection Directive.¹³³ How this fundamental right is affected by the introduction of additional core principles under the GDPR has yet to be worked out. Those difficulties aside, it can be argued that CFR Article 8 is merely an extreme example of reliance on regulatory rules to inform and define the meaning of fundamental rights in technical areas of law. The ECtHR, for example, routinely relies on Council of Europe regulatory guidance in deciding the appropriate application of ECHR right to privacy.¹³⁴

In the United States, there has not been a similarly decisive break with the concept of privacy in legal protections for personal information. Among the many differences between European and American privacy and data protection laws, it is probable that theories of privacy matter less in the absence of a general U.S. constitutional right to privacy. Without that general right, there is more limited scope for innovations in privacy in the expansive manner of ECHR Article 8.

¹²⁹ *Niemietz v. Germany*, n 40 above para 29; *Pretty v. United Kingdom* (2002) 35 EHRR 1, para 6; *Peck v. United Kingdom*, n 79 above, para 57; *S. and Marper v. the United Kingdom*, n 89 above, para 66

¹³⁰ Data Protection Directive, n 54 above, see, for example, Recital 10

¹³¹ O. Lynskey, *The Foundations of EU Data Protection Law*, (Oxford University Press, 2015) Chapter Four

¹³² M. Tzanou, *The Fundamental Right to Data Protection: Normative Value in the Context of Counter-Terrorism Surveillance*, (Oxford: Hart Publishing, 2017); R. Post, 'Data Privacy and Dignitary Privacy: Google Spain, the Right To Be Forgotten, and the Construction of the Public Sphere', (2018) 67 *Duke Law Journal*, 981

¹³³ M. Tzanou, *ibid*

¹³⁴ See, for example, *Catt v. United Kingdom*, (Application no. 43514/15, 24 January 2019) ECtHR

The proprietary and spatial language of the Fourth Amendment has also been a notable barrier to innovative ideas about privacy in relation to government uses of new surveillance technologies.¹³⁵ Nonetheless, this constitutional right to be secure against unreasonable searches and seizures, including its ‘reasonable expectation of privacy’ standard, has evolved through the analysis of law enforcement legislation and practices over many decades.¹³⁶ Its language may be simple, but its applications are usually technical and even obscure.¹³⁷

Consequently, in the United States as much as Europe, privacy and data protection laws continue to encourage the individual exercise of consent and choice in the face of the extraordinary technical, legal and ethical complexity of information governance. Well crafted paternalist solutions, such as explicit prohibitions on particular kinds of personal data collection or use, would undoubtedly protect citizens and consumers more effectively from unfairly discriminatory or manipulative data analytics. Yet, such protectionist paternalism not only stands in the way of more efficient state services or effective information markets, but is also vulnerable to the parallel criticism of restricting personal autonomy and agency.¹³⁸

Information law’s weakest field

After more than a century of legislative and judicial efforts, most liberal democracies now possess varying sets of rights, duties and remedies intended to protect personal information from unjustified access and use. In the previous two sections the ineffectiveness of these protections as defences against increasing transparency has been explained through the lenses of technological change and informational complexity. This section, however, explains that ineffectiveness as a structural weakness in privacy and data protection laws within the interfaces of information law.

In the face of deep commitments to the effective state and efficient markets, privacy and data protection laws are inevitably defensive measures. Unlike the other fields of law that together compose the wider sphere of information law, these laws are pitted directly against the prevailing dynamic of ultimate state access and potential marketability. Unsurprisingly, their

¹³⁵ D. Gray et al, n 70 above

¹³⁶ O. Kerr, ‘Four Models of Fourth Amendment Protection’, (2007) 60 *Stanford Law Review* 503

¹³⁷ See, for example, the conflicting or divergent judicial pronouncements not only in *Carpenter v United States*, n 47 above, but also in *United States v. Jones*, 565 U.S. 400 (2012)

¹³⁸ D. Solove, ‘Privacy Self-Management and the Consent Dilemma’, (2013) 126 *Harvard Law Review*, 1880

protective purposes are routinely outmatched by other fields that are more synergistically aligned with the contemporary political economy of information law. These notably include information rights based on the fundamental right to freedom of expression, including rights to access and use personal information for journalistic purposes.

The structural advantages that freedom of expression based media rights enjoy over the protection of personal information are in fact twofold. They arise, first, from close connections between the political, moral and economic justifications for the free flow of information in liberal democracies. These connections go beyond the obvious alignment of rights to freedom of expression with notions of openness and transparency. It is the practical cross leverage of market forces, commercial law and free speech arguments that can often overwhelm the individual exercise of privacy or data protection rights.¹³⁹ In Europe, for example, there is a developed interplay between EU free movement rights to offer media services and European fundamental rights to freedom of expression, which also protect the publication and distribution rights of those services.¹⁴⁰ In the United States, the connection between political and economic speech rights is even more expressly stated. In recent years, commercial speech claims have gained increasing protection under the U.S. Constitution First Amendment, which has been invoked, for example, to invalidate restrictions on the disclosure of lawfully purchased personal information.¹⁴¹

Second, freedom of expression rights are easily adapted to the opportunities afforded by the erosion of circumstantial privacy. Freedom of expression based claims to access and use of personal information are, for example, well suited to take advantage of expanding concepts of public space and public domain. Simply put, the right to freedom of expression gives legal weight to journalistic claims to use personal information deemed to be public in nature. In *Von Hannover (No 2)*, for example, the ECtHR Grand Chamber, when balancing the rights to privacy and freedom of expression, saw little objection to recording and publishing ordinary

¹³⁹ M. Kaminski, 'Privacy and the Right to Record', (2017) 97 *Boston University Law Review*, 167

¹⁴⁰ Although ultimately unsuccessful before the ECtHR Grand Chamber, the *Satakunnan Markkinapörssi Oy and Satamedia Oy* claims to freedom of expression rights for purely commercial data services demonstrates this close conceptual interplay. See, Case C-73/07 *Tietosuojavaltuutettu v Satakunnan Markkinapörssi Oy and Satamedia Oy*, [2008] ECR I 9831 *Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland* [2017] ECHR. 607

¹⁴¹ *Sorrell v. IMS Health Inc.*, n 69 above. On connections between First Amendment freedom of speech rights and information markets, see R. Post and A. Shanor, 'Adam Smith's First Amendment', (2015) 128 *Harvard Law Review Forum* 165

events occurring in a busy street.¹⁴² In the United States, privacy interests in public space or public domain situations are routinely brushed aside when opposed by First Amendment free speech rights.¹⁴³

The synergistic advantages of freedom of expression rights do more than demonstrate the comparative weaknesses of legal protections for personal information. The interfaces between the major fields of law that constitute information law are mutually defining. In common with governmental powers to access and use personal information for national security and criminal law enforcement purposes, information rights exercised for journalistic purposes often determine and discipline the boundaries of privacy and data protection laws. Given the defensive nature of privacy and data protection laws, the reverse is less often the case.

In Europe, the interface between privacy and freedom of expression rights has worked its way across an expanding range of personal information access and use issues. Largely as a consequence of the ECHR Article 8 positive obligation doctrine,¹⁴⁴ the fundamental right to privacy arises, directly or indirectly, in many private law actions opposing the information access claims of the media, including social media and other platform based services. Widely reported successes against media defendants,¹⁴⁵ however, tend to obscure the daily, uncontested use of public figure and public interest justifications to disclose personal information. In the United States, the lack of a general constitutional right to privacy or a similar doctrine of positive rights, has left privacy and data protections laws often virtually defenceless in the face of First Amendment free speech claims. As the U.S. Supreme Court has gradually extended the scope of the First Amendment,¹⁴⁶ the disclosure of private facts

¹⁴² *Von Hannover v. Germany* (No. 2), n 80 above, para 123; See also, *Alpha Doryforiki Tileorasi Anonymi Etairia v. Greece*, n 78 above

¹⁴³ See, *Shulman v. Group W Productions, Inc.*, 955 P.2d 469 (1998); *American Civil Liberties Union v. Alvarez*, 10-CV-05235 (2016), Court of Appeals for the Seventh Circuit

¹⁴⁴ On the relationship between ECHR Articles 8 and 10, see, Council of Europe/European Court of Human Rights, Guide on Article 8 of the Convention – Right to respect for private and family life, home and correspondence (2018); D. Voorhoof, ‘Freedom of Expression versus Privacy and the Right to Reputation How to Preserve Public Interest Journalism’, in (Smet and Brems eds), *When Human Rights Clash at the European Court of Human Rights*, (Oxford University Press, 2017), 148

¹⁴⁵ See, for example, *Sir Cliff Richard v British Broadcasting Corporation and Chief Constable of South Yorkshire Police*, [2017] EWHC 1291 (Ch)

¹⁴⁶ A. Bhagwat, ‘In Defense of Content Regulation’, (2017) 102 *Iowa Law Review*, 1427

tort identified by Prosser has, for example, withered, as have other private and public law remedies for privacy harms.¹⁴⁷

My point here is not to suggest that secrecy is morally better than transparency. It is to focus attention on the ways in which freedom of expression provides a powerful moral and legal right to take advantage of the continuing erosion of circumstantial privacy. Plainly, once artificial intelligence begins to provide accurate analysis of complex emotional states through facial and other analysis, public figure and public interest arguments will be made to justify publication of that information. Freedom of expression is an integral part of the apparently inexorable liberal democratic transition towards radical transparency.

Towards collaborative public scrutiny and accountability

The picture painted so far is undeniably bleak. Over the past hundred years liberal democracies have moved with increasing speed towards the radical transparency of human life. In our major cities, which are the epicentres of automated surveillance, that future is coming into focus. As I have argued in this paper, the most compelling explanation for this transformation lies in the political economy of information law in relation to technological change. Through a powerful combination of governmental and commercial applications of new technologies and an incapacitated or indifferent public, privacy and data protection laws have enabled only modest deviations in the long arc towards fully transparent existence. There is, moreover, no going back. The technology enabled devices and services that have cumulatively demolished much of the circumstantial privacy of human life are now too deeply embedded in the fabric of our ways of life to be undone. Regardless of the more objectionable governmental and commercial objectives they may serve, innovative technologies have also beneficially transformed human life.

Nonetheless, our algorithmic future is not yet determined, even if past efforts to protect personal information have been so often ineffective. Certainly, whether societies find more effective boundaries against further transparency or even change the governance of how personal information is accessed and used in conditions of transparency are primarily

¹⁴⁷ N. Richards, 'The Limits of Tort Privacy' (2011) 9 *Journal of Telecommunications and High Technology Law*, 357

political and economic questions. Constructive changes in law and regulation can, however, feed into those wider processes of decision making. If, as I have argued, information law works as a coherent whole through the interfaces between its different fields, then privacy and data protection laws can potentially play a more disruptive and less accommodating role within that whole. A break in that direction would, however, require much more than sporadic disruptions. The necessary paradigm shift in information law would require instead a more participatory and collaborative regulatory approach to information processing.

The place to begin is recognition of the failure of a primary focus on individual interests, harms and rights in the protection of personal information. While there are many good reasons to retain, and even strive to make more effective, individual rights and remedies, collective interests in the protection of personal information and collaborative ways of securing those interests have been neglected. Plainly, this has not occurred through lack of intellectual ideas or discourse about group and societal interests in defining and preventing unjustifiable access or use of personal information,¹⁴⁸ importantly including the consequences for individual and collective capacities to engage in democratic association and participation.¹⁴⁹ The transition towards radical transparency has also stimulated useful debates over what values or principles might better express these societal needs than the increasingly over-freighted concepts of autonomy and dignity. This includes significant attention to neo-republican concepts of non-domination in relation to mass surveillance¹⁵⁰ as well as the role of informed trust in underpinning the legitimacy of privacy and data protection laws and sustaining critically engaged citizenship.¹⁵¹

Taken together, ideas of non-domination and meaningful trust offer a critical perspective on the effectiveness of information governance in circumstances of increasing transparency. Picking up Nissenbaum's well known argument that what people care about is not having complete control over personal information or preventing any sharing of that information, but

¹⁴⁸ See, for example, A. Mantelero, 'Personal Data for Decisional Purposes in the Age of Analytics: From an Individual to a Collective Dimension of Data Protection', (2016) 32 *Computer Law & Security Review*, 2, 238; B. Mittelstadt, 'From Individual to Group Privacy in Big Data Analytics', (2017) 30 *Philosophy & Technology*, 4, 475; J. Cohen, n 107 above

¹⁴⁹ See, for example, the major annual conference 'Computers, Privacy and Data Protection, which has made democracy the core theme for the 2019 conference: 'CPDP 2019 : Data Protection and Democracy, 12th International Conference' - <https://www.cpdpcferences.org>

¹⁵⁰ On non-domination in relation the privacy theories, see n 29 above

¹⁵¹ N. Richards and W. Hartzog, n 110 above. See, also, A. Waldman, *Privacy as Trust: Information Privacy for an Information Age* (Cambridge University Press, 2018)

that their information should be shared appropriately,¹⁵² a society that makes non-domination and trust central to its information practices should be able to use fully identified information to harness new technologies when needed and publicly accepted.¹⁵³ Selective transparency without chilling effects would, moreover, be consistent with the importance of openness to democratic societies.

Nor has the neglect of collective interests or collaborative enforcement occurred because the societal nature of the problem is obscure or lacks urgency. The conceptual connections between privacy, data protection and the democratic interests are strikingly apparent in contemporary political and social life.¹⁵⁴ As urban environments, in particular, have lost their historic protections of anonymity and obscurity, the conditions for reflective public association and participation have radically changed. Even casual public participation in demonstrations or other significant public events carry an expectation of potential identifiability and traceability.¹⁵⁵ While electronic surveillance is only one element in the control of mass political gatherings and events in cities, knowledge of being recorded and identified inevitably raises the commitment barrier to association and participation.¹⁵⁶ An individual has to be sufficiently audacious and technically aware to understand and exploit the weaknesses of surveillance systems.¹⁵⁷

Additionally, while current legal principles and models for the protection of personal information are inadequate to challenge the long run trend towards greater transparency, they have stimulated a proliferation of useful new regulatory practices and ideas. In fairness, many of these rest directly or potentially on duties imposed by the GDPR on governmental or commercial personal information users ('controllers' and 'processors' in EU terminology). These include built-in technical solutions, risk or impact assessments, algorithmic auditing, sector codes of conduct, self-certification and representative actions.¹⁵⁸

¹⁵² H. Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, (Stanford University Press, 2009) 2

¹⁵³ Cohen n. 107 above, 21

¹⁵⁴ L. Moerel and A. Wolk, 'Big Data Analytics Under the EU General Data Protection Regulation', (May, 2017), 3-4, <<https://ssrn.com/abstract=3006570>> accessed 26 June 2019

¹⁵⁵ Metropolitan Police (London), 'Live Facial Recognition Trial', <https://www.met.police.uk/live-facial-recognition-trial/>> accessed 26 June 2019

¹⁵⁶ D. Balson, 'How to Silence Peaceful Protesters in Four Easy steps' 2 July 2018, <https://medium.com>

¹⁵⁷ F. Brunton and H. Nissenbaum, *Obfuscation: A User's Guide for Privacy and Protest* (MIT Press, 2015).

¹⁵⁸ GDPR, n 55 above, Article 25 (Data Protection by design and default), Article 35 GDPR (Data protection impact assessment), Article 40 (Codes of conduct), Article 42 (Certification), Article 80 (Representation of data subjects). While the GDPR does not expressly mandate auditing of data analytics, Recital 71 refers to an

Nonetheless, contemporary awareness of our transparency predicament and our rich accompanying discourse has created little more than openings and possibilities for a more participatory and collaborative regulatory approach. The actions of individuals in pursuing remedies may be catalytic and even occasionally decisive, but much of the heavy lifting will need to be done through the cooperation of public authorities, privacy NGO's and, as much as possible, commercial businesses and organisations. Privacy NGO's, for example, which have already played a leading role in European fundamental rights litigation challenging government surveillance measures,¹⁵⁹ are beginning to make highly informed interventions with government data protection authorities to initiate GDPR based investigations into key elements of the commercial surveillance network.¹⁶⁰

Yet, if the aim is to challenge and disrupt the information law status quo that favours further access and use of personal information, privacy activism through litigation or strategic pressure on regulators will not be sufficient. Such targeted, high profile acts need to be tied into broader efforts to build and maintain ecosystems of public accountability. To be most effective, this would include independent scrutiny and public participation in the responsibility mechanisms required by law or developed as good governmental or commercial practice. In Europe, national data protection authorities, such as the UK Information Commissioner's Office (ICO), as one example, could be re-structured to become more participatory and collaborative in regulatory oversight.

Drawing on environmental regulation models, data impact assessments that address the broader consequences of large scale surveillance would, for example, provide an access point for external scrutiny.¹⁶¹ This could include public bodies, such as national data protection authorities, as well as NGO's and research bodies capable of evaluating and auditing the uses of algorithms and innovations in artificial intelligence.¹⁶² Well informed, external scrutiny of

obligation to use appropriate 'technical and organisational measures' in relation to profiling and automated decision-making.

¹⁵⁹ See, for example, *Big Brother Watch and Others v. the United Kingdom*, n 90 above

¹⁶⁰ See, for example, Privacy International, 'Why We've Filed Complaints against Companies that Most People Have Never Heard Of – And What Needs to Happen Next', 8 November 2018, <https://privacyinternational.org>.

¹⁶¹ A. Froomkin, 'Privacy impact notices to address the privacy pollution of mass surveillance', in *Privacy in Public Space: Conceptual and Regulatory Challenges*, n. 73 above, 184; D. Hirsch, 'Big Data Sustainability: An Environmental Management Systems Analogy', (2016) 72 *Washington & Lee Law Review* 409

¹⁶² A. Tutt, 'An FDA for Algorithms' (2017) 69 *Administrative Law Review* 83; (UK) House of Commons Science and Technology Committee, Report on Algorithms in decision-making (15 May 2018) HC 351.

data analytics could thus potentially address problems of technical opacity in the use of data analytics that the individual exercise of rights to information is unlikely to breach.¹⁶³ A widespread practice of independent auditing would also strengthen the publicity work of public authorities¹⁶⁴ and privacy NGO's¹⁶⁵ as well as media reporting of algorithmic decision making.¹⁶⁶ Beyond auditing, meaningful external participation in other aspects of personal information governance, such as governmental and industry standard setting, would also build informed public trust in the governance of surveillance.

Nonetheless, the difficulties in transforming privacy and data protection laws and regulation into a more challenging and disruptive element within the legal governance of information cannot be understated. Privacy and data protection laws are not structured to facilitate a diverse ecosystem of accountability involving an array of empowered intermediary parties. The GDPR, for example, is structured around the data subject as both primary object of protection and bearer of rights.¹⁶⁷ The external bodies permitted to assist data subjects in claiming redress or empowered to enforce their rights and remedies are strictly limited. GDPR Article 80 regarding representative actions is confined to not-for-profit bodies, organisations or associations that have statutory public interest objectives and are active in the field of the protection of data subjects' rights and freedoms. Assistance from these bodies will be often limited by their modest resources. Even national data protection authorities, who possess considerable powers under the GDPR to resolve the claims of data subjects and enforce the duties of data controllers and processors, will nonetheless only fulfil these responsibilities to the extent their enforcement policies and funding allow.¹⁶⁸

From a civil liberties perspective, this focus on individual harm and individual rights is appropriate. To the varying degrees information privacy and even data protection are recognised as fundamental rights in liberal democracies, they are closely connected to

¹⁶³ R. Caplan, J. Donovan, L. Hanson, and J. Matthews, n 121 above

¹⁶⁴ ICO, Investigation into the use of data analytics in political campaigns, Report to Parliament (6 November 2018) <<https://ico.org.uk>> accessed 26 June 2019

¹⁶⁵ See, for example, Privacy International, 'Report on How Apps on Android Share Data with Facebook', 29 December 2018, <https://privacyinternational.org>.

¹⁶⁶ See, for example, N. Diakopoulos, 'What a report from Germany teaches us about investigating algorithms', *Columbia Journalism Review*, 10 January 2019.

¹⁶⁷ O. Lynskey, n. 131 above, Chapter 6, 'The role of individual control in EU Data Protection Law' 177.

¹⁶⁸ L. Edwards and M. Veale, 'Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For', (2017) 16 *Duke Law & Technology Review* 1, 18.

concepts of personal autonomy, dignity and agency as well as liberalism's inherent scepticism towards protective paternalism.¹⁶⁹ Yet, something is plainly not working.

To return a last time to the lessons we might draw from the contemporary life of cities, which are epicentres not only of governmental and commercial surveillance, but also of environmental pollution. Both of these crises has different but obvious negative effects on the lives of urban residents. In the field of environmental law, however, societal and individual harms figure equally prominently.¹⁷⁰ Undoubtedly, environmental law methods can only provide analogies and not solutions to the surveillance crisis. The protection of personal information from unjustified access and use requires principles, rules and remedies particular to the nature of its harms.

Nonetheless, echoing environmental law, a key step would be to shift the focus from individual to collective harm.¹⁷¹ Once surveillance, including its growing potential for unfair discrimination and hidden manipulation, is identified as a societal harm of global proportions, a gradual re-structuring of privacy and data protection law and regulation would be possible. While retaining and even strengthening the means to address individual harms, a more open and coherent regulatory regime for information uses could be given the means to prevent or remedy the negative impact of new technologies and services on informational privacy.

In this more optimistic view of the future, the transformation of human life into a state of radical transparency could itself become an explicit subject for both public assessment and legal or regulatory intervention. This could include active public monitoring of existing degrees of identifiability, intrusion and disclosure as well as data driven selection for decision making and resulting consequences, such as modulations of behaviour. If done well, this ongoing public assessment would lead to a parallel transparency about the nature of the irrevocable choices being made as new technologies are adopted for governmental or commercial purposes. The public would then at least have a greater collective awareness of which specific aspects of their residual privacy would need to be further compromised

¹⁶⁹ D. Solove, n 137 above.

¹⁷⁰ On the protection of the societal interest, see, for example, Air Quality Standards Regulations 2010 (SI 2010/1001), (UK) enforced in part by means of Regulatory Enforcement and Sanctions Act 2008 (SI 2008/13)

¹⁷¹ As Julie Cohen has advocated, this means 'departing from subject centred frameworks'. J. Cohen, n 107 above.

individually and collectively to secure the promised benefits of specific new technologies and services.

The recently announced decision of the San Francisco Board of Supervisors to prohibit the use of facial recognition technology by police and other government agencies in the city is an example of the kind of collective privacy decision making that could become more common.¹⁷² On the other hand, a better informed public may well be persuaded that a further loss of privacy is a price worth paying for more convenience or security. That decision, however, would be reached more openly through democratic processes rather than through the incremental, opaque practices of the past century. In this more open and hopefully deliberative process, the public is also more likely to demand more effective safeguards against attendant risks of disclosure, discrimination and manipulation.

¹⁷² K. Conger, R. Fausset, S. Kovalesski, 'San Francisco Bans Facial Recognition Technology', *New York Times*, 15 May 2019.