Bournemouth University Working Papers in Law, No 1/2018

Infosoc 2018: Informational Rights, Informational Wrongs, and Regulatory Responsibilities

Roger Brownsword*

* Bournemouth University and King's College London

Infosoc 2018: Informational Rights, Informational Wrongs, and Regulatory Responsibilities

Roger Brownsword*

1 Introduction

In our information societies, in Infosoc 2018, we embark on another new year with mixed hopes and expectations, as well as with significant fears and concerns. For example, we hope and expect that, when the General Data Protection Regulation comes into force in late Spring, it will prompt data controllers to take their responsibilities more seriously and offer data subjects improved protection of their rights; and many hope that there will be some reduction in the gratuitously abusive and offensive content that we find online.[1] However, at the same time, we fear that there will be new forms of attacks on our cyber infrastructures (such as the WannaCry ransomware that disabled many hospitals in the United Kingdom in 2017); and we are concerned not only that Internet intermediaries are abdicating their responsibility for a range of dangerous and undesirable content that they host but also that it is becoming difficult in the world of current affairs to know what is 'true' and what is 'fake' news.

At the root of these hopes and expectations together with these fears and concerns, there are, so to speak, a number of 'informational interests' on the basis of which certain rights are claimed and wrongs denounced. If we connect these interests to the kinds of rights that are claimed and the wrongs that are denounced, we might say that, on the one hand, they express an interest in the accessibility, integrity, accuracy and authenticity of public information (and information systems) while on the other, they express an interest in controlling access to and the use of personal and private information. While it would be premature to conceive of a human agent's informational interests in these terms, for present purposes, a working definition of 'informational interests' might be proposed along some such lines. In other words, for

* This Working Paper is based on a seminar given at Bournemouth University on December 13, 2017. I am grateful to those who participated in the seminar for their many helpful comments and questions, as well as to those who assisted after the seminar with the preparation of this Working Paper. Needless to say, the usual disclaimers apply.

1 In general, see Saul Levmore and Martha C. Nussbaum (eds), *The Offensive Internet: Speech, Privacy and Reputation* (Cambridge, Mass.: Harvard University Press, 2010); and in relation to UK politicians, see CSPL, *Intimidation in Public Life: A Review by the Committee on Standards in Public Life* (Cm 9543, HC 1017273996 2017-18). But compare Matthew Parris, 'The internet is a jungle that can't be tamed' *The Times*, December 30, 2017 p 23, who suggests that, because there is little chance of censoring the social media, we might as well 'learn to ignore the insults'.

present purposes, we might define our informational interests as relating primarily to the integrity of the informational eco-system as well as to our individual ability to control the outward and inward flows of information that relate directly to ourselves.[2]

Although many of the claimed rights and wrongs that are provoked by our informational interests can be related very directly to developments in modern information and communication technologies, they are not limited to such developments. For example, developments in human genetics (rather than in ICTs) have led to the articulation of claimed rights 'to know' and, conversely, 'not to know'[3]; developments in robotics, machine-learning and artificial intelligence are already provoking a claimed right to an explanation (where decision-making is automated); and, of course, we should not forget that, in the Nineteenth Century, the right to privacy was provoked, not by the latest digital technologies but by early photographic technologies.[4] It is also the case that some of our informational interests do not relate to any kind of technology—for example, traditional interests in truthfulness and the condemnation of deception and fraud arose, and continue to make sense, in contexts that are not at all technological.

Against this background, the purpose of this Working Paper is to introduce the field of informational rights and wrongs as one that invites further inquiry. While it is trite that new technologies have disruptive effects, the particular ways in which technological developments disrupt our understanding of our informational interests as well as our sense of the kind of information society that we want to be merit further analysis. Without a clearer understanding of these matters, we cannot expect the legal and regulatory environment to be fit for purpose and acceptable in relation to the protection and privileging of our informational interests.

The Working Paper is in three principal parts. First, we undertake an initial tentative 'mapping' of the landscape of informational rights and wrongs. To the extent that certain informational interests are articulated as rights, they can be placed in one hemisphere; and to the extent that they are articulated as wrongs they can be placed in the other hemisphere. Within each hemisphere the interests can be further positioned by locating them in clusters or groups of

---

2 Compare Roger Brownsword, 'Informed Consent in the Information Society' *Health and Society Review* (2012) (Carla Faralli edited special issue) 161.

3 Notably, see Ruth Chadwick, Mairi Levitt, and Darren Shickle (eds), *The Right to Know and the Right Not to Know* (second edition) (Cambridge: Cambridge University Press, 2014). This collection of essays is sub-titled 'Genetic Privacy and Responsibility'.

4 See, Samuel Warren and Louis Brandeis, 'The Right to Privacy' (1890) 4 *Harvard Law Review* 193.

rights and wrongs; and, with further analysis, it might be possible to identify and locate the underlying interests in, so to speak, certain 'regions' (possibly relating to the generic needs of human agents—such as the needs they have relating to their health and well-being or their capacity for prospective agency, for self-development and for moral development). Secondly, a way of framing the interests, relative to their importance for a community of human agents, is suggested. Viewing the interests through this lens, we can not only treat some interests as more important than others (which matters when, for example, particular interests conflict), we can relate the interests to a three-tiered scheme of regulatory responsibilities (namely, protecting the 'commons', protecting the values that are fundamental to the identity of a particular information society, and giving effect to (and balancing) residual legitimate interests). This way of framing the interests also has implications for the way that we allocate various informational rights and wrongs to particular regions. Thirdly, a number of lines of inquiry are suggested concerning, inter alia, the tensions that we find in the regulatory discourse relating to informational interests, the competence of respectively the courts and legislatures/executives in responding to new informational claims and concerns, and the articulation of a 'new coherentism' to guide regulators as they seek to make acceptable and effective interventions in relation to such claims and concerns.

Finally, it should be emphasised that, by the end of the Working Paper, there will be many loose ends that remain to be tied up and business that is still to be finished. Indeed, this is an understatement. It bears repetition that the purpose of the Working Paper is not to provide all the answers—how could it be when we do not yet know what the questions are. Rather, we are at a more preliminary stage. What the Working Paper aims to do is simply to suggest that it might be worth taking a harder look at the field of informational rights and wrongs and then to highlight some of the features of the field that might warrant further inquiry.

2 Mapping the Landscape of Informational Rights and Informational Wrongs

In this Part of the Working Paper, we begin in a very provisional way to map the landscape of informational rights and wrongs. The map employs two hemispheres, one of informational rights and the other of informational wrongs. We make no assumptions about how these hemispheres might connect or relate to one another. Within each hemisphere, the interests are not simply listed; rather, they are allocated to clusters—for example, a cluster on privacy and confidentiality (in the hemisphere of informational rights) and a cluster on cybercrimes (within the hemisphere of informational wrongs). On further analysis, it might be possible to tease out the informational interests that underlie these clusters and then begin to map the interests more

specifically relative to particular 'regions' (for example, a region of control, or a region of accessibility, and so on) within each hemisphere.

Immediately, though, we seem to be getting ahead of ourselves. After all, the field of informational interests has yet to be theorised; we are supposedly simply laying out the ground. Yet, here we are already talking about the field in terms of some interests that are expressed as rights claims while others are expressed as wrongs (implying a breach of duty). Given that interests do not necessarily convert into claim rights, and given that duty perspectives do not always correspond to rights perspectives, we need to be careful not to beg too many questions. Accordingly, two caveats are in order.

First, let me suggest that, provided that we are agnostic about the significance of those discursive practices that express some interests as rights and others as wrongs, we can follow the practice in characterising some informational interests as matters of right and others as matters of wrong—and, then, we can imagine the former as lying in one hemisphere of interests and the latter in another in the way that we have indicated. This is merely presentational; and it is revisable.[5]

Secondly, the inventory of informational rights or wrongs that we itemise is not intended to be comprehensive and nor is it assumed that these particular rights and wrongs must appear in the field. The intention is to put forward these rights and wrongs in a way that should be treated as indicative and illustrative only. Moreover, the clusters to which these rights and wrongs are assigned, like any suggestions about possible regions of underlying interests, are again to be treated as highly provisional.

2.1 Informational Rights

Within the hemisphere of informational rights, we will speak to the following five indicative clusters: (i) rights to privacy and confidentiality; (ii) data protection rights; (iii) the right to know and the right not to know; (iv) the right to truth; and (v) intellectual property rights.

---

[5] I should declare, however, that, in ethics, I am not actually agnostic. Rather, I favour a rights perspective over a duty perspective—or, at any rate, I do so in relation to what I later refer to in this Working Paper as the commons conditions (i.e., those conditions that relate to the generic needs of [human] agents). See, e.g., Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (Oxford: Oxford University Press, 2001); Deryck Beyleveld and Roger Brownsword, *Consent in the Law* (Oxford: Hart, 2007); and Roger Brownsword, *Rights, Regulation and the Technological Revolution* (Oxford: Oxford University Press, 2008).

2.1.1 Privacy and confidentiality

Given that privacy is such a protean concept, privacy rights being engaged in so many different ways, it is difficult to express the basic or organising informational interest.[6] We might follow Serge Gutwirth and Paul de Hert in saying that, by contrast with data protection rights (which are about transparency), privacy is about opacity[7]; or we might say that, by contrast with a right to know, privacy is about a right that others do not know. However, if we simply focus on privacy itself, we might say that the basic idea is that there are certain contexts, or zones, or areas, or places and spaces, or situations in which we reasonably expect that others will not try to gather information about our mental states or our acts; and, to the extent that such an expectation is reasonable, the information is covered by our privacy interest.[8] Alternatively, or additionally, we might try to characterise certain kinds of information as inherently private.[9]

Although in English law, the idea of confidentiality has been used to connect domestic law to the privacy right in Article 8 of the European Convention on Human Rights, this is generally regarded as conceptually inappropriate[10]; privacy is not grounded in the idea of confidentiality—indeed, if anything, we might see the relationship as being precisely the other way round. On this latter understanding, confidentiality is engaged where A shares with B information that is private. Then, tracking what we have just said about the basic idea of privacy, we can say that there are certain contexts or situations or relationships in which we reasonably expect that information that we share with another will not be communicated to

---

6 Seminally, see, Samuel Warren and Louis Brandeis (n 4). However, for further iterations, see e.g. William L. Prosser, 'Privacy' (1960) 48 *California Law Review* 383, Charles Fried, 'Privacy' (1968) 77 *Yale Law Journal* 475, Graeme Laurie, *Genetic Privacy* (Cambridge: Cambridge University Press, 2002), Daniel J. Solove, *Understanding Privacy* (Cambridge, Mass.: Harvard University Press, 2008), and Helen Nissenbaum, *Privacy in Context* (Stanford: Stanford University Press, 2010).

7 Serge Gutwirth and Paul de Hert, 'Privacy, Data Protection and Law Enforcement. Opacity of the Individual and Transparency of Power' in E. Claes, A. Duff, and S. Gutwirth, (eds), *Privacy and the Criminal Law*, (Antwerp and Oxford: Intersentia, 2006).

8 Any attempt to map privacy onto private spaces, as opposed to public spaces, is likely to be difficult, and arguably it is increasingly so because we regularly carry and use our private information-bearing mobile devices in public spaces. For analysis, see Tjerk Timan, Bryce Clayton Newell, and Bert-Jaap Koops (eds), *Privacy in Public Space* (Cheltenham: Edward Elgar, 2017).

9 Compare Roger Brownsword, 'Regulating Brain Imaging: Questions of Privacy and Informed Consent' in Sarah J.L. Edwards, Sarah Richmond, and Geraint Rees (eds), *I Know What You Are Thinking: Brain Imaging and Mental Privacy* (Oxford: Oxford University Press, 2012) 223.

10 See, e.g., Rachael Mulheron, 'A New Framework for Privacy? A Reply to Hello!' (2006) 69 MLR 679.

third parties or exploited in ways that are inappropriate. Alternatively, or additionally, we might say that any information that is inherently private is to be treated as confidential.

There are many things that are unclear about our interests in privacy and confidentiality—in particular, it is unclear whether their scope and weight is contingent on social custom, practice and convention (which then holds the key to whether our expectations of privacy and confidentiality are reasonable) or whether there are some aspects of these interests that are fixed and non-contingent. However, they are interests that seem to belong within a region where 'control and access' are central. In other words, to the extent that we have the benefit of these interests, we determine who, if anyone, has access to the information in question. We are the information controllers and gatekeepers.

Yet, is this understanding of privacy and confidentiality not antithetical to the development of modern information societies, conceived as societies where there is more information, more accessible information, more information that flows? Certainly, it would seem odd to treat privacy and confidentiality as cornerstones of such societies. Rather, these interests would represent constraints or reservations that set limits to the informational flows of such societies. Is this, then, how we should view privacy and confidentiality? And, to pose a recurrent question: if this is so, then is this the kind of information society that we want? Is this a template for Infosoc 2018?

2.1.2 Data protection

The European Charter of Fundamental Rights is unusual in distinguishing explicitly between a right to privacy and a right to data protection. While the former is provided for in Article 7 of the Charter (copying Article 8 of the European Convention on Human Rights), the latter is provided for in Article 8. According to Article 8(1), 'Everyone has the right to the protection of personal data concerning him or her.' Then Article 8(2), giving further particulars (in line with the principles of Directive 95/46/EC on data protection) provides:

> Such [personal] data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

What should we make of this? What kind of 'protection' does Article 8 of the Charter offer in relation to our personal data, or the collection and processing of our personal data? While

transparency in relation to the collection and processing of personal data is surely a necessary condition, it does not seem to be sufficient.

To some extent, the extent of data protection rights depends on how key regulatory concepts, such as 'personal data', 'data processing', and 'data controller' are interpreted. The broader the reading of these concepts, the broader the sweep of the regulatory provisions and the broader the protective effect of the rights. However, the fundamental question with data protection laws, including the new GDPR, is whether each individual data subject has controlling rights (akin to privacy and confidentiality) in relation to accessing and using personal data or whether data subjects have a regulated right to the fair collection and acceptable use of their personal data. On the former view, each individual data subject is a gatekeeper; but, on the latter view, the regulatory scheme aspires only to achieve an acceptable balance of the interests of those who have a stake in accessing and using personal data.

This fundamental ambivalence about the nature of the informational interests that are protected by data protection law may be detected in the reasoning of the CJEU in the *Google Spain* case.[11] There, the CJEU accepted that a right to be forgotten is implicit in the conjunction of Articles 7 (respect for private life) and 8 (protection of personal data) of the EU Charter of Fundamental Rights together with Articles 12(b) and 14(a) of the Data Protection Directive—these provisions of the Directive concerning, respectively, the data subject's right to obtain rectification, erasure or blocking where the processing of the data is not compliant with the Directive and the data subject's right to object on 'compelling legitimate grounds' to the processing of the data which itself is ostensibly justified by reference to the legitimate interests of the controller or third parties. The significance of the newly recognised right to be forgotten is that a data subject who objects to certain personal data being flagged up—in this case, the information in question was an announcement made some 16 years earlier in a Spanish newspaper that identified the data subject in connection with a real estate auction that was related to attachment proceedings for the recovery of social security debts—where a search is made under that data subject's name may require the link to be erased. Moreover, this right may be exercised even if the data to be forgotten is perfectly lawful and accurate and even if there is no evidence of prejudice to the data subject.

[11] Case C-131/12, *Google Spain SL, Google Inc v Agencia Española de Protection de Datos (AEPD), Mario Costeja González* [2014] available at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065.

However, the judgment is riddled with references to a 'balancing of interests' leaving the precise basis of the right unclear. If the right is derived from Articles 7 and 8 of the Charter then, as the Court observes, it belongs to a privileged class of rights that 'override, as a rule, not only the economic interests of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name.'[12] In other words, it would only be other, conflicting, fundamental rights (such as the fundamental right to freedom of expression that is recognised by Article 11 of the Charter) that could be pleaded against such an overriding effect. Immediately after saying this, though, the court muddies the waters by suggesting that the right to be forgotten would not have overriding effect if 'it appeared, *for particular reasons*, such as the role played by the data subject in public life, that the interference with his fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.'[13] Clearly, care needs to be taken that the only reasons that qualify as 'particular reasons' here are that fundamental rights are implicated. If, on the other hand, the right to be forgotten rests on the rights in Articles 12(b) and 14(a) of the Directive, it would not be privileged in the way that fundamental rights are and a general balancing of interests (seeking an acceptable or reasonable accommodation of relevant interests) would be appropriate. On this analysis, the particular reasons relied on against the right to be forgotten could be much broader—or, at any rate, this would be so unless we read the more particular provisions of Article 8 of the Charter as elevating the specific rights of the Directive to the status of fundamental rights.

Applying its principles to the case at hand, the Court holds as follows:

> As regards a situation such as that at issue in the main proceedings…it should be held that, having regard to the sensitivity for the data subject's private life of the information contained in those announcements and to the fact that its initial publication had taken place 16 years earlier, the data subject establishes a right that that information should no longer be linked to his name by means of such a list. Accordingly, since in the case in point there do not appear to be particular reasons substantiating a preponderant interest of the public in having, in the context of such a search, access to that

[12] (n 11) at para 97.

[13] (n 11) at para 97 (emphasis added).

> information, a matter which is, however, for the referring court to establish, the data subject may, by virtue of Article 12(b) and subparagraph (a) of the first paragraph of Article 14 of Directive 95/46, require those links to be removed from the list of results.[14]

What is puzzling here is not so much that privacy rights to opacity are being mixed up with data protection rights to transparency and the like (puzzling though this is), but that fundamental rights (to privacy) are being mixed with rights (in the Directive) that are subject to balancing and that belong to a different class of interests.[15] Whereas, from a fundamental rights perspective, it makes no sense to think that the passage of 16 years is a relevant consideration, from a simple balancing perspective, the privacy-sensitive nature of the data has no privileged status.[16] Arguably, the Court, like the Directive itself, is trying to strike some intermediate position between fundamental rights and simple balancing. If so, what might this be?

In principle, a community might treat a right to be forgotten as: (i) a fundamental right that is necessarily privileged and overriding in relation to all non-fundamental rights (as a right that is constitutive of this particular community); or (ii) as an interest that is not protected as a fundamental right but which, in the general balancing of interests, has more weight (although still susceptible to being outweighed by the preponderance of interests); or (iii) as a simple legitimate interest to be balanced against other such interests. If (ii) is an intermediate position, is this what the Court is questing after?

Although the GDPR makes provision for the right to be forgotten within its provisions about the right to erasure, the questions raised by the reasoning in the *Google Spain* case remain to

---

14 (n 11) at para 98.

15 Compare the insightful critique in Eleni Frantziou, 'Further Developments in the Right to be Forgotten: The European Court of Justice's Judgment in Case C-131/12, *Google Spain SL, Google Inc v Agencia Española de Proteccion de Datos*' (2014) 14 *Human Rights Law Review* 761, esp at 768-769.

16 Whether or not the elapse of time is a relevant consideration seems to depend on the particular facts of the case: see Article 29 Data Protection Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/32* (November 26, 2014) at 15-16 ('Depending on the facts of the case, information that was published a long time ago…might be less relevant [than] information that was published 1 year ago.).

be resolved. In Infosoc 2018, European lawmakers and courts, like European citizens, seem to be unclear about the scope and status of this claimed right.[17]

2.1.3 The right to know and the right not to know

The right to know has applications in relation to both public and personal information. So far as access to *public* information is concerned, over one hundred countries worldwide have freedom of information laws.[18] The general purpose of these laws, implicitly recognising a right to know, is to enable citizens to access official information and documents. This is designed to enable citizens to play a more effective role in the public sphere and to hold public officials to account. In some spheres, notably in the sphere of environmental law, the right to know is specifically underpinned by legal provisions—as for example, in the Aarhus Convention, the Preamble to which provides:

> Recognizing also that every person has the right to live in an environment adequate to his or her health and well-being, and the duty, both individually and in association with others, to protect and improve the environment for the benefit of present and future generations,
>
> Considering that, to be able to assert this right and observe this duty, citizens must have access to information, be entitled to participate in decision-making and have access to justice in environmental matters …[19]

In this way, the aspiration of the Convention is to enhance the quality and implementation of decisions relating to the environment, raise public awareness of environmental issues, and enhance the public's opportunity to express its concerns as well as to enable public authorities to take account of such concerns.[20]

---

17 See further, Stavroula Karapapa and Maurizio Borghi, 'Search engine liability for autocomplete suggestions: personality, privacy and the power of the algorithm' (2015) 23 *International Journal of Law and Information Technology* 261.

18 https://en.wikipedia.org/wiki/Freedom_of_information_laws_by_country (last accessed, January 9, 2017).

19 UNECE Aarhus Convention Access to Information, Public Participation in Decision-Making and Access to Justice in Environmental Matters (1998), 2161 UNTS 447.

20 Aarhus Convention, Preamble (n 19)

We should also note schemes for disclosure of information relating to domestic violence (Clare's law) and child sex offending (Sarah's law). Strictly speaking, these schemes fall short of recognising a right to know: members of the public have a right to ask the police for disclosure but judgments then have to be made by the police. Recently, concerns have been expressed about regional variations in the police responses to requests or referrals made under Clare's law.[21]

Turning to access to *personal* information, developments in human genetics have prompted claimed rights both to know and not to know in relation to information about one's own genetic profile. For example, if A tests positive for Huntington's Disease, it might be claimed that A's close relatives (also A's prospective employers or insurers) have a right to know about A's test results;[22] but, equally, it might be claimed that those who do not wish to know about these results have a right not to know?[23] When genetic sequencing is increasingly affordable, when genetic information—thanks to big data sets and machine learning—promises to be increasingly interpretable, and when genetic information is readily available in a global marketplace[24], there are many stakeholders debating these rights. In particular, there are patients and research participants (some wanting to know, others preferring not to know), clinicians and medical researchers (some wanting to disclose, others preferring not to), and various commercial interests and lobbyists (some supporting the rights, others opposing them).

---

21 See John Simpson and Maeve McClenaghan, 'Police fail to use Clare's law for domestic abuse alerts' *The Times*, January 9, 2018, p. 4.

22 On which, see *ABC v St George's Healthcare NHS Trust & Ors* [2015] EWHC 1394 (QB), [2017] EWCA Civ 336. In this case, the claimant, who was pregnant at the relevant time, sued the defendants, complaining that they had failed to inform her that her father had been diagnosed with Huntington's Disease. Had the claimant been so informed, she would have known that she was at risk of having the disease and, knowing that her children would also be at risk, she would have terminated the pregnancy. In the High Court, the claim was struck out (as unarguable) on the ground that, because the defendants obtained the information about the father's health status in confidence, and because the father was emphatic that he did not want his daughter to be told, it would not be fair, just, and reasonable to impose on them a duty to inform the daughter. For comment, see Victoria Chico, 'Non-disclosure of Genetic Risks: The Case for Developing Legal Wrongs' (2016) 16(1-2*) Medical Law International* 3; and, Michael Fay, 'Negligence, Genetics and Families: A Duty to Disclose Actionable Risks' (2016) 16(3-4) *Medical Law International* 115. Not altogether surprisingly, the Court of Appeal has now reversed this decision and remitted the case for trial.

23 See, e.g., the Nuffield Council on Bioethics, *Genetic Screening: Ethical Issues* (London, 1993); and Ruth. Chadwick, Mairi. Levitt, and Darren Shickle (n 3).

24 Nb Gina Kolata, 'FDA Will Allow 23andMe to Sell Genetic Tests for Disease Risk to Consumers' *The New York Times* (April 6, 2017): see, https://www.nytimes.com/2017/04/06/health/fda-genetic-tests-23andme.html?_r=0 (last accessed April 7, 2017).

Although questions of this kind have been debated for some years, two developments have served to concentrate the mind once again on these matters. One is the development of non-invasive prenatal testing (NIPT)—which is now being piloted within the UK national screening pathway for Down's syndrome.[25] The attraction of the test is that it promises to reduce the need for an invasive amniocentesis test or chorionic villus sampling and, with that, to reduce the number of babies lost during pregnancies.[26] However, because NIPT presents an opportunity to provide information about the fetus that goes beyond the trisomies,[27] even to the point of full genomic profiling, as well as returning information about the mother,[28] it invites questions about how broad the test should be and how far the mother's right to know might extend.[29] The other development is the emergence of big biobanks (comprising large collections of biosamples and participant data) all being curated for the benefit of health researchers. For some time, one of the most problematic aspects of biobank governance has been whether researchers who access a biobank have any responsibility to return potentially clinically significant results to individual (identifiable) participants.[30] At UK Biobank, where the general rule is that there will be no individual feedback of research findings, but where the biosamples of all 500,000 participants have now been genotyped, and where a major imaging sub-study

---

25 See J. Gallagher, 'Safer Down's test backed for NHS use' (2016) (http://www.bbc.co.uk/news/health-35311578) (last accessed September 25, 2016).

26 For a successful trial led by Professor Lyn Chitty at Great Ormond Street Hospital, see http://www.rapid.nhs.uk/about-rapid/evaluation-study-nipt-for-down-syndrome (last accessed September 25, 2016).

27 For example, Sequenom's MaterniT 21 PLUS 'can tell you if you are having a boy or a girl, and screens for both common and rare chromosomal abnormalities. The test screens for trisomy 21 (Down syndrome), trisomy 18 (Edwards syndrome), trisomy 13 (Patau syndrome), and many others that can affect your baby's health': see https://sequenom.com/tests/reproductive-health/maternit21-plus#patient-overview (last accessed April 5, 2017).

28 See, e.g., K. Oswald, 'Prenatal blood test detects cancer in mothers-to-be', *Bionews* 739 (2015) at http://www.bionews.org.uk/page_503998.asp. (last accessed September 25, 2016).

29 For discussion, see Roger Brownsword and Jeff Wale, 'The Development of Non-Invasive Prenatal Testing: Some Legal and Ethical Questions' (2016) 24 *Jahrbuch für Recht und Ethik* 31, and 'The Right to Know and the Right Not to Know Revisited' (two parts) (2017) 9 *Asian Bioethics Review* 3.

30 See, e.g., Catherine Heeney and Michael Parker, 'Ethics and the Governance of Biobanks' in Jane Kaye, Susan M.C. Gibbons, Catherine Heeney, Michael Parker and Andrew Smart, *Governing Biobanks* (Oxford: Hart, 2012) 282; Deryck Beyleveld and Roger Brownsword, 'Research Participants and the Right to be Informed', in Pamela R. Ferguson and Graeme T. Laurie (eds), *Inspiring a Medico-Legal Revolution* (Essays in Honour of Sheila McLean) (Farnham: Ashgate, 2015) 173; and Roger Brownsword, 'Big Biobanks, Big Data, Big Questions' in Regina Ammicht Quinn and Thomas Potthast (eds), *Ethik in den Wissenschaften* (Tubingen: IZEW, 2015) 247.

aims to enrol 100,000 participants on the basis that potentially clinical significant findings will be returned, there are some complex questions of both principle and practice.[31]

Turning from feedback to access, consider a test-case of the kind that occurred a few years ago in Sweden, where an application was made to a biobank for the purpose of assisting with the identification of Swedes who were victims of the Boxing Day Tsunami. If the governance framework contemplates access only for 'health-related research purposes', even an imaginative lawyer would have difficulty in construing this as covering the identification of victims of disasters. On the other hand, the public interest argument is attractive and it is plausible to suppose (as, indeed, was the case in Sweden) that there would be broad support for access in such circumstances.

Although the question of accessing biobanks in such circumstances is still relatively unexplored, there has been much more discussion about creating exceptions to the usual restrictions imposed by privacy and data protection laws.[32] In response to emergencies, special measures have been adopted in some countries—for example, in the wake of the 2002 Bali bombing and the 2004 tsunami, the Australian government amended its privacy laws to permit the collection, use and disclosure of personal information where (in the context of such disasters) an emergency declaration is made.[33] Approving such initiatives, Joel Reidenberg, Robert Gellman, Jamela Debelak, Adam Elewa, and Nancy Liu have argued that:

> sharing information about missing persons is a legitimate objective in emergency situations, that data protection laws should accommodate this objective, and that… emergency circumstances require special exceptions to privacy rules that are

---

31 On the questions of principle, see Roger Brownsword, 'New Genetic Tests, New Research Findings: Do Patients and Participants Have a Right to Know—and Do They Have a Right Not to Know?' (2016) 8 *Law, Innovation and Technology* 247; and on some practical questions about minimising the return of false positive findings, see Lorna M. Gibson, Thomas J. Littlejohns, Ligia Adamska, Steve Garratt, Nicola Doherty, Joanna M. Wardlow, Giles Maskell, Michael Parker, Roger Brownsword, Paul M. Matthews, Rory Collins, Naomi E. Allen, Jonathan Sellors, and Cathie L.M. Sudlow, 'Impact of detecting potentially serious incidental findings during multi-modal imaging' [version 1; referees: awaiting peer review]. *Wellcome Open Res* 2017, 2:114 (doi: 10.12688/wellcomeopenres.13181.1).

32 For an extremely helpful survey, see Joel R. Reidenberg, Robert Gellman, Jamela Debelak, Adam Elewa, and Nancy Liu, *Privacy and Missing Persons After Natural Disasters* (Washington DC and New York, NY: Center on Law and Information Policy at Fordham Law School and Woodrow Wilson International Center for Scholars, 2013).

33 Formally, this was achieved by the introduction of Part VIA into the Privacy Act, 1988; see Reidenberg et al (n 32) 11-14.

proportional to the circumstances, including appropriate safeguards, and that remain in place only as long as the emergency circumstances necessitate.[34]

If privacy and data protection (which, after all, will be regarded by many as fundamental rights) should accommodate such a pressing need, then should not a similar accommodation be made in respect of access to biobank data? On the one hand, the argument for granting access is that the purpose relates to a strand of the public interest—indeed, New Zealand's Assistant Privacy Commissioner, Blair Stewart, has put this in terms of acts that are 'essential in the cause of common humanity'[35]; on the other hand, the argument for denying access is that access for this kind of application has not been authorised by the participants (assuming that no implicit authorisation can be read into the governance framework). Although the purpose of this test-case application is neither health-related nor for research, it raises questions about competing strands of the public interest. Given the evolving practice and philosophy in relation to privacy, together with the Swedish biobanking precedent, it seems likely that this would be one case where the public interest in access would be judged to be stronger than the public interest in denying it.

Whether or not the right to know and the right not to know reflect the same underlying informational interest is moot. On the face of it, while the latter reflects the kind of control interest that underpins privacy, the former is more to do with enhancing one's autonomy and making more informed choices. Indeed, where the right to know arises in the context of clinical care—patients having the right to be made aware of their treatment options, as well as the risks and benefits associated with each option—the underlying interest seems very clearly to be about being able to operationalise one's autonomy by making informed choices.[36] That said, if the right not to know articulates a dimension of privacy, and if privacy itself is about creating an environment in which one is free to make choices that are not necessarily conformist, then both rights reflect an interest in being able to make free and informed choices.

2.1.4 The right to truth

In the international law of human rights, the right to truth is recognised both explicitly and implicitly. For example, the UN International Convention for the Protection of All Persons

---

34 Reidenberg et al (n 32) at 6.

35 Reidenberg et al (n 32) at 1 (Foreword).

36 Compare *Montgomery v Lanarkshire Health Board* [2015] UKSC 11.

from Enforced Disappearance not only affirms (in its Preamble) 'the right of any victim to know the truth about the circumstances of an enforced disappearance and the fate of the disappeared person, and the right to freedom to seek, receive and impart information to this end', in Article 25.2 it is provided that 'Each victim has the right to know the truth regarding the circumstances of the enforced disappearance, the progress and results of the investigation and the fate of the disappeared person.'

Provisions of this kind are important in building arguments for a more general recognition in international criminal law of the right to truth (given its relevance both to alleviating physical and psychological suffering and to upholding the Rule of Law).[37] Underlining this point, in *El-Masri v The Former Yugoslav Republic of Macedonia*, the Grand Chamber of the ECtHR said that the inadequate character of the investigation in the 'extraordinary rendition' case at hand had impaired the right to truth—'not only for the applicant and his family, but also for other victims of similar crimes and the general public, who had the right to know what had happened.'[38] So, there are both individual and collective interests in this right.

However, minds have been concentrated on the right to truth not only by Conventions and Courts but also by the establishment and operation of Truth and Reconciliation Commissions. As is well-known, the Truth and Reconcilation Commission in post-apartheid South Africa has provoked a great deal of comment.[39] While many support the mission to uncover the truth of the apartheid years, to create a collective record of that time, this is no straightforward exercise and there are tough questions about whether such a project is compatible with reconciliation. Moreover, to the extent that there are amnesties and immunities granted to those who assist the Commission, there are questions about the trade-off with the demands of corrective justice.

Although the South African Commission has become something of a byword for a third way approach to the achievement of truth and reconciliation—between, on the one side, courts and

---

37 See, e.g., Melanie Klinkner and Howard Davis, 'A right to truth, victims and the International Criminal Court' (2014) 3 *Torture: Asian and Global Perspectives* (Asian Human Rights Commission) 55.

38 Application no. 39630/09, [2012] ECHR 2067. See, further, Alice M. Panepinto, 'The Right to the Truth in International Law. The Significance of Strasbourg's Contributions' (2017) 37 *Legal Studies* 739. At 755, Panepinto suggests that the jurisprudence of the Strasbourg Court betrays a 'fragmented approach in engaging the right to the truth incidentally, by attaching it to different substantive articles depending on the facts, the applicant's submissions, the state's responses, and often the persuasiveness of third party interventions, and at times referring to it as an overarching principle not appended to a listed right.'

39 See, e.g. Audrey R. Chapman and Hugo van der Merwe (eds), *Truth and Reconciliation in South Africa: Did the TRC Deliver?* (Philadelphia: University of Pennsylvania Press, 2008).

trials and, on the other, amnesia and drawing a line—the fact of the matter is that, in post-conflict contexts, many such Commissions have been so mandated.[40] Before we move on, we want to know what really happened. Moreover, if we set aside the quest for reconciliation, we might say that, in such situations, referring cases to international criminal courts or tribunals is an all out quest for the truth: truth as desirable in itself and truth as a predicate of corrective justice.[41]

2.1.5 Intellectual property rights

We talk about IPRs, intellectual property *rights*; but, those who hold IPRs can be vocal in claiming informational *wrongs*, because the hard edge of IPRs is visible in the context of alleged infringement. Arguably, then, this is a case where we have a strong connection between interests in the rights hemisphere and interests in the wrongs hemisphere. What, though, are the specifically *informational* aspects of IPRs? And, do IPRs as currently constituted and practised serve our informational interests as intended?

These are large questions that we can leave to IP specialists. Suffice it here to make three short comments.

First, as property rights, IPRs are traditionally in tension with the free flow of information. Against IPRs, proponents of open source, open access, copyleft, and the like, advocate for significant modifications to the usual restrictions associated with IPRs (especially copyright). Similarly, those who argue for easier access to information that is essential for the facilitation of interoperability, push back against IPRs;[42] and, those who draw on Orin Kerr to argue for an 'internal' (user) perspective on information technologies can be understood as pushing back against IPRs that are implicated in an 'external' (engineer's) view.[43] Accordingly, it might be argued that the central thrust of IPRs is contrary to our informational interests.

---

40 See https://en.wikipedia.org/wiki/Truth_and_reconciliation_commission.

41 Compare Klinkner and Davis (n 37).

42 Sally Weston, 'Improving Interoperability by Encouraging the Sharing of Interface Specifications' (2016) 8 *Law, Innovation and Technology* 78.

43 Orin S. Kerr, 'The Problem of Perspective in Internet Law' (2003) 91 *Georgetown Law Journal* 357. Kerr's distinction between internal and external perspectives on acts and operations involving information technologies is central to Hayleigh Bosher's PhD thesis on digital copyright infringement by way of copying and communicating to the public (BU 2017).

Secondly, that said, it should not be forgotten that disclosure is one of the preconditions of patent grants. Patents, unlike trade secrets, do not keep information concerning the working of an invention behind closed doors; a patent gives the rights holder a clear run at commercial exploitation of the invention but only in return for sharing information about how the invention works. In the light of this, rather than asserting that IPRs are contrary to our informational interests, we might want to say that, where a patent is granted, the law recognises that the public has a right to know how the invention works but not a right to exploit that knowledge for commercial advantage.

Thirdly, with regard to copyright, creative work is necessarily published but commercial exploitation is again restricted. Moreover, we might say that there is also an interest here in the originator being recognised as the author of the work. Exactly how this might relate to informational interests (possibly as an aspect of the right to truth) invites further analysis.[44]

So much for some indication of the range of informational rights. We can turn now to a sample of informational wrongs.

2.2 Informational Wrongs

Traditionally, we think that it is wrong for others to misinform us in ways that are fraudulent and dishonest, or to perjure themselves, and so on. Recall, for example, in the early years of the present century, the outrage at not only the deception practised by Enron but also the inadequacy of company audits.[45] However, this was hardly the end of the story. As Stephen Copp and Alison Cronin have argued, corporate misinformation—the systematic use of off balance sheet finance, and the like—should be treated as a serious wrong with the wrongdoers prosecuted and held to account.[46]

In Infosoc 2018, we are concerned not only about individual acts of fraud or deception but about the integrity and reliability of the larger information environment itself. According to David Patrikarakos:

---

44 Compare Maurizio Borghi, 'Copyright and Truth' (2011) 12 *Theoretical Inquiries in Law* 1.

45 See, https://en.wikipedia.org/wiki/Enron_scandal; and, David Kershaw, 'Waiting for Enron: The Unstable Equilibrium of Auditor Independence Regulation' (2006) 33 *Journal of Law and Soc*iety 382.

46 See, Stephen Copp and Alison Cronin, 'The Failure of Criminal Law to Control the Use of Off Balance Sheet Finance During the Banking Crisis (2015) 36 *The Company Lawyer* 99.

> Our information environment is sick. We live in a world where facts are less important than narratives, where people emote rather than debate, and where algorithms shape our view of the world.[47]

In this 'post truth' world, new technologies—particularly the technologies that support the social media, where public broadcasting standards do not apply—are deeply implicated in our sense of where we find the leading informational wrongs.

Within the hemisphere of informational wrongs, we will speak to the following four indicative clusters: (i) cybercrime; (ii) cyberwar and 'fake news'; (iii) super-surveillance; and (iv) AI, profiling and recommending.

2.2.1 cybercrime

If we understand 'cybercrimes' in a broad sense, such crimes will encompass the use of cybertechnologies as instruments of (or as the medium for) the commission of crimes as well as serious wrongdoing directed at cybertechnologies themselves. In other words, we will treat cybercrime, not as a category of entirely novel crime, but as a category of crimes where cybertechnologies might be used as tools by criminals (such as where a computer is used for fraudulent purposes) or where computers and the like might themselves be the target of a crime (such as where a laptop is stolen). Regardless of whether we understand cybercrime quite so broadly, or in some narrower sense, there is no doubt that, as the world becomes more reliant on cybertechnologies there is a global concern about how to combat cybercrime.

Although both the United Nations and the European Union have committed to cooperating in the attempt to deal with cybercrime,[48] it is the Council of Europe, in its Convention on Cybercrime[49]—a Convention now ratified by more than fifty States, including the US—that has taken the lead. While the Convention does not explicitly define 'cybercrime' it implicitly takes a broad view, categorising cybercrimes under four principal headings, namely: (i) offences against the confidentiality, integrity and availability of computer data and systems;

---

47 David Patrikarakos, *War in 140 Characters* (New York: Basic Books, 2017) 264.

48 UN Resolution 55/63. On the European Union, see Marco Gercke, "Europe's Legal Approaches to Cybercrime" (2009) 10 *ERA Forum* 409.

49 Budapest, 23rd November, 2001.

(ii) computer-related offences (viz., fraud and forgery); (iii) content-related offences (viz., child pornography); and (iv) offences related to infringement of copyright and related rights.

From the perspective of our *informational* interests, it is wrongs in the first two of these categories that are particularly a matter of concern. The more that we commit to modern information technologies, the more important it is that our personal data is held securely and that the information that we want to access is available and has not been compromised or corrupted. In this respect, the intentional and unauthorised damaging, deletion, alteration, or suppression of data, as covered by Articles 4 and 5 of the Convention speaks to some fundamental concerns in Infosoc 2018. Moreover, where individual acts of this kind are scaled up as in denial of service attacks on cybersystems, the vulnerability of modern information societies is vividly exposed.

The distributed denial-of-service (DDoS) attack on Estonia in 2007 is a well-known case in point.[50] In a report on large-scale cybercrime, the House of Lords European Committee described the attack on Estonia and its impact in the following terms:[51]

> Estonia has the highest broadband connectivity in Europe. In 2007, 98 percent of all bank transactions in Estonia used electronic channels and 82 percent of all Estonian tax declarations were submitted through the Internet. Nearly every school in Estonia uses an e-learning environment, and the use of ID cards and digital signatures has become routine in both public and private sector administrations in Estonia. Estonia has a significant ethnic Russian population, and the movement of a statue of a Soviet soldier commemorating the end of World War II led to civil unrest within Estonia and complaints by the Russian Government. Online DDoS attacks began to target Estonian government and private sector sites, including banking institutions and news sites. The attacks built up over the course of a few weeks and peaked at 11 pm Moscow time on Victory Day, 9 May. The attacks hit many parts of the infrastructure, including the websites of the prime minister, parliament, most ministries, political parties, and three

50 Compare, too, Richard Norton-Taylor, 'Titan Rain—How Chinese Hackers Targeted Whitehall', *The Guardian*, September 5, 2007, p. 1. One notch down from such incidents are the denial-of-service attacks launched by pro-Wikileaks 'hactivitists' in December 2010: see, e.g., Cahal Milmo and Nigel Morris, 'Prepare for all-out cyber war' *The Independent*, December 14, 2010, p 1.

51 House of Lords European Union Committee, *Protecting Europe Against Large-Scale Cyber-Attacks* (Fifth Report, Session 2009-2010) para 11, Box 1.

> of the biggest news organisations. Members of the Estonian Parliament went for four days without email. Government communications networks were reduced to radio for a limited period. Financial operations were severely compromised, ATMs were crippled, and Hansabank, the largest bank, was forced to close its Internet operations. Most people found themselves effectively barred from financial transactions while the attacks were at their height. Estonia responded by closing large parts of its network to people from outside the country, and a consequence was that Estonians abroad were unable to access their bank accounts.

If Estonian governance and commerce could be disabled in this way, how vulnerable might other European countries be? According to the Committee:

> There are wide differences between the Member States. Some, like Estonia, are very heavily reliant on the Internet but have—or had until very recently—defences wholly inadequate to protect their CII [Critical Information Infrastructures] against even minor attacks. Some, and the United Kingdom is among them, also rely heavily on the Internet, but have sophisticated and well-developed defences to guard against attacks or disruptions. Yet other Member States rely less on the Internet, but their defences are insufficient. We concluded that all Member States have an interest in bringing the defences of the lowest up to those of the highest, and that this is a matter of legitimate concern to the EU as a whole.[52]

Even if defence levels were to be raised in the way that the Committee believes would be desirable, there is a view that nation states are no longer geared to respond to external cyberthreats. According to Susan Brenner, for example, it is not always clear, first, who is responsible for a particular cyberthreat and, secondly, whether it is an act of cyberwar, cyberterror, or even cybercrime—indeed, she maintains that the attacks on Estonia were just such a case.[53] While the importance of identifying the source of the threat is obvious, the relevance of classifying the threat correctly is that responsibility needs to be allocated to the appropriate national agents (the military, the intelligence services, or the police).

2.2.2 cyberwar and ‘fake news’

---

52 Ibid., Summary.

53 Susan W. Brenner, *Cyberthreats: The Emerging Fault Lines of the Nation State* (New York: Oxford University Press, 2009).

A decade on from the Estonian outage, the lines—between war, crime, and politics, and between militia and civilians—can seem even more blurred. Wars are now fought in more than one dimension—physical, narrative and discursive;[54] the instruments of war are both kinetic and non-kinetic; and the targets include national critical cyber-infrastructures.

In a world of 'hybrid warfare'—a term that nowadays connotes an approach that draws on a range of instruments, including 'terrorism, insurgency, criminality, and conventional operations, along with the extensive use of information operations'[55]—an attack might take more than one form including cyberattacks on 'military command and control, air traffic control systems, hospital power supplies, the electricity grid, water supplies, nuclear power, satellite communications, Internet attacks on the banking system, and cyberattacks on dams/water supply and other eco threats.'[56] When cyber chiefs warn that the only question about such a category one attack, disrupting critical infrastructure is not if but when, there is real cause for concern.[57]

One of the most alarming implications of such attacks are drawn out in a recent report from Chatham House.[58] This is that cyberattacks might disable nuclear command, control, and communication systems but also that inadvertent nuclear launches might stem from reliance on false information and data.[59] As Lawrence Freedman rightly says, the term 'information war' invites confusion: it might refer to 'measures designed to disable systems dependent upon flows of information'; or it might refer to 'attempts to influence perceptions by affecting the

54 See Patrikarakos (n 47).

55 Lawrence Freedman, *The Future of War: A History* (London: Allen Lane, 2017) at 223. See, too, Sascha-Dominik Dov Bachmann and Anthony Paphiti, 'Russia's Hybrid war and its Implications for Defence and Security in the United Kingdom' (2016) 44 *Scientia Militaria, South African Journal of Military Studies* 28; and Sascha-Dominik Dov Bachmann and Håkan Gunneriusson, 'Russia's Hybrid Warfare in the East: The Integral nature of the Information Sphere' (2015) 16 *Georgetown Journal of International Affairs* 198.

56 Bachmann and Paphiti (n 55) at 31.

57 Ewan MacAskill, 'Destructive attack on UK a matter of "when, not if" warns cyber chief' *The Guardian*, January 23, 2018, p. 1.

58 Beyza Unal and Patricia Lewis, *Cybersecurity of Nuclear Weapons Systems: Threats, Vulnerabilities and Consequences* (London: The Royal Institute of International Affairs, Chatham House, 2018).

59 See, too, Freedman (n 55) Ch 21.

content of information.'[60] In the former sense, we are talking about 'engineering', in the latter 'about cognition'.[61] Either way, though, there is plenty to worry about.

The significance of information should not be understated. In this new world, we find ourselves in various wars of words—the protagonists increasingly employing new social media, sometimes simply putting out their own side of the conflict, or their own story, but sometimes 'trolling' and blatantly distorting the truth. Of course, propaganda is not new but when the mainstream media increasingly rely on social media for their stories, there is a concern that what passes for 'the news' is not just filtered and selective but quite possibly corrupted.

Not surprisingly, then, one of the pressing concerns in Infosoc 2018 is so called 'fake news'. The concern is not so much that the tabloid press is full of gossip, rumour, and other unlikely tales. Rather, it is that the new media exacerbate the opportunities for politicians to manipulate their constituencies, that rational democratic debate is distorted and drowned out by the media noise, and that there might also be outside interference, or 'cybermeddling', with domestic politics.[62]

In *The Assault on Reason*,[63] Al Gore bemoans the proliferation of 'fake news'—the 'ludicrous conspiracy theories and determined efforts to discredit the established truth of information that in previous eras would have been challenged among the literate and sane.'[64] In those previous eras, particularly when public discourse was conducted in print, there was an invitation to a 'two-way conversation in which individuals could contribute their own thoughts as well as receive those of others.'[65] In an era of radio and television, there was much less opportunity for this kind of conversation and interaction but, with the new media, the possibility of multi-party participation (coupled with low entry costs) is retrieved. However, the Internet as currently

---

60 Freedman (n 55) at 227.

61 Ibid.

62 See, e.g., Catherine Philip, 'Moscow "meddling in US and Europe for past 20 years"' *The Times*, January 11, 2018 (report by US Congressional committee asserting that 'Russia has been working to undermine democracy at home and across Europe for the past two decades'); and, in the UK, the government recently announced that it was setting up a rapid response unit to counter the spread of online fake news by foreign powers, see Nigel Morris, 'Government sets up "fake news" unit to tackle social media threat' *The Independent* January 24, p 7.

63 Al Gore, *The Assault on Reason* (updated edition) (London: Bloomsbury, 2017).

64 Gore (n 63) at xi.

65 Gore (n 63) at xii-xiii.

employed is hardly a byword for reasoned debate; as a medium for public discussion, like most technological developments, it is both used and abused. The challenge, as Cass Sunstein saw in the early days of the Internet,[66] and as now reiterated by Gore, is to restore 'a healthy information ecosystem that invites and supports the…essential processes of self-government in the age of the Internet so that [communities] can start making good decisions again.'[67]

2.2.3 super-surveillance

Introducing his book on the Snowden revelations, Glenn Greenwald[68] reminds his readers that snooping and suspicionless surveillance is nothing new. Nor, of course, is it just the NSA in the United States that acts, or that has acted, as an agent of surveillance. Famously, three decades ago, the revelations made by Peter Wright (an ex member of the British intelligence services) in his book, *Spycatcher*, caused a furore—both about the publication of 'official secrets' and about the bugging and eavesdropping routinely carried out by MI5.

With each new wave of technologies, the focal points for surveillance change—for example, from the opening of mail to wire-tapping. With the development of the Internet, and with our online activities becoming the focus for surveillance, the threat to privacy is amplified. For, as Greenwald rightly points out, the Internet is much more than our post office or telephone: the Internet 'is the epicentre of our world….It is where friends are made, where books and films are chosen, where political activism is organized, where the most private data is created and stored. It is where we develop and express our very personality and sense of self.'[69]

Faced with this threat, we can hear echoes of Al Gore's critique of the information ecosystem in Greenwald's suggestion that we stand at an historic crossroads. The question, as Greenwald, puts it, is this:

> Will the digital age usher in the individual liberation and political freedoms that the Internet is uniquely capable of unleashing? Or will it bring about a system of omnipresent monitoring and control, beyond the dreams of even the greatest tyrants of

66 Cass Sunstein, *Republic.com* (Princeton: Princeton University Press, 2001).

67 Gore (n 63) at 294.

68 Glenn Greenwald, *No Place to Hide* (London: Penguin, 2014).

69 Greenwald (n 68) at 5-6.

the past? Right now either path is possible. Our actions will determine where we end up.[70]

The question, then, is simply this: what kind of information society do we want to be? However, in Infosoc 2018, who are the 'we' whose actions really matter? Whose actions will be the determining factor? In both the public and the private sector data is being gathered on an unprecedented scale[71]; and, if this data is then used to train smart machines that sift and sort citizens (as mooted by the Chinese social credit system) this could be the basis for a truly dystopian 'system of omnipresent monitoring and control'.

2.2.4 AI, profiling and recommending

In a prescient article, written at the turn of the new century, Richard Ford foresaw the profiling of consumer preferences and the servicing of one's consumption needs by so-called 'cyberbutlers'.[72] Consumers would sign over their paychecks to their cyberbutlers who, guided by the particular consumer's profile, would place appropriate orders so that, each day, the consumer would 'come home to a selection of healthy and nutritious groceries from webvan.com or a Paul Smith shirt from boo.com or the latest Chemical Brothers CD from cdnow.com'.[73]

Moreover, as Ford correctly anticipated, consumers' data would be used by suppliers and others to develop a profile of the-consumer-that-is-me to the point that, functioning proactively, they would 'suggest books I'll enjoy reading, recordings I'll like to listen to, restaurants I'll be glad I tried, even if I wouldn't have chosen any of them on my own.'[74] This is at most a gentle nudge but the more that each consumer's preferences are revealed and used to refine the profile, the more reliant on their cyberbutlers consumers would become.[75]

---

70 Greenwald (n 68) at 6.

71 With reference to the private sector, compare Siva Vaidhyanathan, *The Googlization of Everything (And Why We Should Worry)* (Oakland: University of California Press, 2011).

72 Richard T. Ford, 'Save the Robots: Cyber Profiling and Your So-Called Life' (2000) 52 *Stanford Law Review* 1572.

73 Ford (n 72) at 1578.

74 Ford (n 72) at 1576.

75 Compare Ariel Ezrachi and Maurice Stucke, *Virtual Competition* (Cambridge, Mass.: Harvard University Press, 2016) at 193, fearing that 'each super-platform will seek through its voice- or text-based interface to become the first, and only, place we will go.'

If our cyberbutlers and on-line suppliers know me better than I know myself, how far does this depart from the world of off-line consumption? Possibly, there will be some marketplaces in which traders really do know their customers but, in many off-line environments, each consumer is simply another number to add to the footfall. Where the latter is the case, the introduction of on-line profiling might give rise to concern with regard to the balance of power, to the transparency of the dealing, and to the autonomy of consumers.

With powerful AI now being built into our devices and invited into our homes, we need to be clearer about the concerns that we might harbour.[76] Is it that we fear that we might be misinformed, or that we need more disclosure about the profiling and recommending processes, or that we become over-reliant on systems that might be compromised, or that we lose vital life skills, or that we become trapped in our own echo chambers, or that there are some choices that we really should make for ourselves (especially moral choices)?[77]

Taking stock, we have a rough map of our informational rights and wrongs. What should regulators do with this map? For regulators who take their responsibilities seriously, what is the significance of this mapping of our informational interests? This question takes us to the next Part of the Working Paper.

3 Framing the Interests Relative to their Importance

In this Part of the Working Paper, I will present a sketch of the bigger picture of regulatory responsibilities, these responsibilities being ranked in three tiers of importance. At the first and most important tier, regulators have a responsibility for maintaining the pre-conditions for human social existence, for any kind of human social community. I will call these conditions 'the commons'. At the second tier, regulators have a responsibility to respect the fundamental values of a particular human social community, that is to say, the values that give that community its particular identity. At the third tier, regulators have a responsibility to seek out an acceptable balance of legitimate interests. The responsibilities at the first tier are cosmopolitan and non-negotiable (the red lines here are hard); the responsibilities at the second and third tiers are contingent, depending on the fundamental values and the interests recognised

---

[76] For discussion, see Argyro P. Karanasiou and Dimitirs A. Pinotsis, 'A study into the layers of automated decision-making: emergent normative and legal aspects of deep learning' (2017) 31 *International Review of Law, Computers and Technology* 170.

[77] See, further, Roger Brownsword, 'Disruptive Agents and Our Onlife World: Should We Be Concerned?' (2017) 4 *Critical Analysis of Law* (symposium on Hildebrandt, *Smart Technologies and the End(s) of Law*) 61, and 'From Erewhon to Alpha Go: For the Sake of Human Dignity Should We Destroy the Machines?' (2017) 9 *Law, Innovation and Technology* 117.

in each particular community. Any conflicts between these responsibilities are to be resolved by reference to the tiers of importance: responsibilities in a higher tier always outrank those in a lower tier. In what follows, I speak briefly to each of these three tiers.

3.1 The regulatory responsibility for the commons

The basic idea of the commons is that there is a set of conditions that sets the stage for any kind of human purposeful activity, whether individually or in groups or larger communities. These conditions do not privilege any particular individual, group or community and they do not privilege any particular activity, project or plan. These are conditions that are needed by each and every human agent irrespective of the particular way in which they want to operationalise their agency.

We might get to this idea by an *a priori* route that focuses on developing an understanding of what it is to view oneself as an agent (or human agent)[78]; or, we might simply tease out the presuppositions of the standard demands that are made on regulators as we debate the social licence for new technologies. Taking this latter approach, we will note, first, that we expect regulators to be mindful that we, as humans, have certain biological needs and that there should be no encouragement for technologies that are dangerous in that they compromise the conditions for our very existence; secondly, we will note that we have a (self-interested) sense of which technological developments we would regard as beneficial and on the basis of which we will press regulators to support and prioritise such developments (and, conversely, to reject developments that we judge to be contrary to our self-interest); and, thirdly, we will note that, even where proposed technological developments are neither dangerous nor lacking utility, some will argue that they should be prohibited because their development would be contrary to morality or unethical—as argued famously by Francis Fukuyama in relation to modern human biotechnology.[79]

If we build on this analysis, we will argue that the paramount responsibility for regulators is to protect, preserve, and promote:

- the essential conditions for human existence (given human biological needs);

[78] Such a strategy, I suggest, can be found in the 'Gewirthian' tradition that originates in Alan Gewirth, *Reason and Morality* (Chicago: University of Chicago Press, 1978). For detailed analysis of this strategy, see Deryck Beyleveld, *The Dialectical Necessity of Morality* (Chicago: University of Chicago Press, 1991).

[79] Francis Fukuyama, *Our Posthuman Future* (London: Profile Books, 2002).

- the generic conditions for self-development and human agency; and,
- the essential conditions for the development and practice of moral agency.

These, it bears repeating, are imperatives for regulators in all regulatory spaces, whether international or national, public or private. Of course, determining the nature of these conditions will not be a mechanical process and I do not assume that it will be without its points of controversy.[80] Nevertheless, let me give an indication of how I would understand the distinctive contribution of each segment of the commons.

In the first instance, regulators should take steps to protect, preserve and promote the natural ecosystem for human life.[81] At minimum, this entails that the physical well-being of humans must be secured; humans need oxygen, they need food and water, they need shelter, they need protection against contagious diseases, if they are sick they need whatever medical treatment is available, and they need to be protected against assaults by other humans or non-human beings. It follows that the intentional violation of such conditions is a crime against, not just the individual humans who are directly affected, but humanity itself.[82]

Secondly, the conditions for meaningful self-development and agency need to be constructed (largely in the form of positive support and negative restriction): there needs to be sufficient trust and confidence in one's fellow agents, together with sufficient predictability to plan, so as to operate in a way that is interactive and purposeful rather than merely defensive. As Maria Brincker puts it:

> Agents act in relation not to singular affordances but to affordance spaces: choices are always situated calibrations of multiple interests and purposes given the perceived

---

80 Moreover, even if it is agreed where the bottom lines are to be drawn, a community still has to decide how to handle proposals for uses of smart machines that do not present a threat to any of the bottom line conditions.

81 Compare, J. Rockström et al, 'Planetary Boundaries: Exploring the Safe Operating Space for Humanity' (2009) 14 *Ecology and Society* 32 (http://www.ecologyandsociety.org/vol14/iss2/art32/) (last accessed November 14, 2016); and, Kate Raworth, *Doughnut Economics* (London: Random House Business Books, 2017) 43-53.

82 Compare Roger Brownsword, 'Crimes Against Humanity, Simple Crime, and Human Dignity' in Britta van Beers, Luigi Corrias, and Wouter Werner (eds), *Humanity across International Law and Biolaw* (Cambridge University Press, 2014) 87.

> opportunities. To assess the values and risks of potential actions we need to have expectations regarding the consequences of those actions.[83]

It follows, argues Brincker, that without some degree of privacy 'our very ability to act as autonomous and purposive agents' might be compromised.[84]

Let me suggest that the distinctive capacities of prospective agents include being able:

- to freely choose one's own ends, goals, purposes and so on ('to do one's own thing')
- to understand instrumental reason
- to prescribe rules (for oneself and for others) and to be guided by rules (set by oneself or by others)
- to form a sense of one's own identity ('to be one's own person').

Accordingly, the essential conditions are those that support the exercise of these capacities. With existence secured, and under the right conditions, human life becomes an opportunity for agents to be who they want to be, to have the projects that they want to have, to form the relationships that they want, to pursue the interests that they choose to have and so on. In the twenty-first century, no other view of human potential and aspiration is plausible; in the twenty-first century, it is axiomatic that humans are prospective agents and that agents need to be free.

The gist of these agency conditions is nicely expressed in a recent paper from the Royal Society and British Academy where, in a discussion of data governance and privacy, we read that:

> Future concerns will likely relate to the freedom and capacity to create conditions in which we can flourish as individuals; governance will determine the social, political, legal and moral infrastructure that gives each person a sphere of protection through which they can explore who they are, with whom they want to relate and how they want to understand themselves, free from intrusion or limitation of choice.[85]

---

83 Maria Brincker, 'Privacy in Public and the Contextual Conditions of Agency' in Tjerk Timan, Bryce Clayton Newell, and Bert-Jaap Koops (eds) (n 8) 64, at 88.

84 Brincker (n 83) at 64.

85 The Royal Society and British Academy, *Connecting Debates on the Governance of Data and its Uses* (London, December 2016) 5.

In this light, we can readily appreciate that—unlike, say, Margaret Atwood's post-apocalyptic dystopia, *Oryx and Crake*[86]—what is dystopian about George Orwell's *1984*[87] and Aldous Huxley's *Brave New World* [88] is not that human *existence* is compromised but that human *agency* is compromised.[89] We can appreciate, too, that dataveillance practices in Infosoc 2018, as much as *1984*'s surveillance, 'may be doing less to deter destructive acts than [slowly to narrow] the range of tolerable thought and behaviour.'[90]

Thirdly, where human agents have moral aspirations, the commons must secure the conditions for a moral community. Agents who reason impartially will understand that each human agent is a stakeholder in the commons that protects the essential conditions for human existence together with the generic conditions of agency; and that these conditions must, therefore, be respected. Beyond these conditions, the moral aspiration is to do the right thing relative not simply to one's own interests but relative to the interests that other human agents might have. While respect for the commons' conditions is binding on all human agents, these conditions do not rule out the possibility of moral contestation and moral pluralism. Rather, these are pre-conditions for moral debate and discourse, giving each agent the opportunity to develop his or her own view of what is morally prohibited, permitted, or required in relation to those acts, activities and practices that are predicated on the existence of the commons.

3.2 The regulatory responsibility to respect the community's fundamental values

The next tier of responsibility is for the fundamental values of each particular community. Just as each individual human agent has the capacity to develop their own distinctive identity, the same is true if we scale this up to communities of human agents. There are common needs but distinctive identities.

---

86 (London: Bloomsbury, 2003).

87 (London: Penguin Books, 1954) (first published 1949).

88 (London: Vintage Books, 2007) (first published 1932).

89 Again, see Brincker (n 83). To be sure, there might be some doubt about whether the regulation of particular acts should be treated as a matter of the existence conditions or the agency conditions. For present purposes, however, resolving such a doubt is not a high priority. The important question is whether we are dealing with a bottom-line condition.

90 Frank Pasquale, *The Black Box Society* (Harvard University Press, 2015) at 52.

From the middle of the Twentieth Century, many nation states have expressed their fundamental (constitutional) values in terms of respect for human rights and human dignity.[91] These values (most obviously the human right to life) clearly intersect with the commons conditions and there is much to debate about the nature of this relationship and the extent of any overlap. So, for example, if we understand the root idea of human dignity in terms of humans having the capacity freely to do the right thing for the right reason,[92] then human dignity reaches directly to the commons' conditions for moral agency.[93] However, nation states most obviously articulate their particular identities by the way in which they interpret their commitment to respect for human dignity. Whereas, in some communities, the emphasis of human dignity is on individual empowerment and autonomy, in others it is on constraints relating to the sanctity, non-commercialisation, non-commodification, and non-instrumentalisation of human life.[94] These differences in emphasis mean that communities articulate in very different ways on a range of beginning of life and end of life questions as well as questions of human enhancement, and so on.[95]

With the realisation that technologies can be applied with both regulatory intent and regulatory effect,[96] one question that should now be addressed is whether, and if so how far, a community sees itself as distinguished by its commitment to regulation by *rule*. For example, in some smaller scale communities, there might be resistance to a technocratic approach because compliance that is guaranteed by technological means compromises the context for trust. Or, again, a community might prefer to stick with regulation by rules because it values public

---

91 See Roger Brownsword, 'Human Dignity from a Legal Perspective' in M.Duwell, J. Braavig, R. Brownsword, and D. Mieth (eds), *Cambridge Handbook of Human Dignity* (Cambridge: Cambridge University Press, 2014) 1.

92 For such a view, see Roger Brownsword, 'Human Dignity, Human Rights, and Simply Trying to Do the Right Thing' in Christopher McCrudden (ed), *Understanding Human Dignity* (Proceedings of the British Academy 192) (Oxford: The British Academy and Oxford University Press, 2013) 345.

93 See, Roger Brownsword, 'From Erewhon to Alpha Go: For the Sake of Human Dignity Should We Destroy the Machines?' (2017) 9 *Law, Innovation and Technology* 117.

94 See Deryck Beyleveld and Roger Brownsword, *Human Dignity in Bioethics and Biolaw* (Oxford: Oxford University Press, 2001); Tim Caulfield and Roger Brownsword, 'Human Dignity: A Guide to Policy Making in the Biotechnology Era' (2006) 7 *Nature Reviews Genetics* 72; and Roger Brownsword, *Rights, Regulation and the Technological Revolution* (Oxford: Oxford University Press, 2008).

95 The development of NIPT raises just such larger questions. See Roger Brownsword and Jeff Wale, 'Testing Times Ahead' (2018).

96 Cf section 4.2.1.2 below).

participation in setting standards and is worried that this might be more difficult if the debate were to become technocratic.[97]

If a community decides that it is generally happy with an approach that relies on technological features rather than rules, it then has to decide whether it is also happy for humans to be out of the loop. Where the technologies involve AI (as in anything from steering public buses to decisions made by the tax authorities), the 'computer loop' might be the only loop that there is. This raises an urgent question, namely: 'do we need to define essential tasks of the state that must be fulfilled by human beings under all circumstances?'[98] Having posed this question, the community will then need to ask further questions, such as whether its particular conception of the information society includes rights or legal personality for robots and other smart agents.[99]

Whatever particular communities decide about such matters, it is, of course, essential that the fundamental values to which a particular community commits itself are consistent with (or cohere with) the commons conditions.

3.3 The regulatory responsibility to seek an acceptable balance of interests

At the third tier of regulatory responsibility, the challenge is to promote general policy objectives (such as supporting and encouraging beneficial innovation) while balancing this with countervailing interests. Given that different balances will appeal to different interest groups, finding an acceptable balance is a major challenge for regulators.

Today, we have the perfect example of this challenge in the debate about the liability (both criminal and civil) of Internet intermediaries for the content that they carry or host.[100] In

---

97 See, further, Roger Brownsword, The Rule of Law, Rules of Law, and Technological Management' (edited version of an introductory keynote given at the ACELG's sixth annual conference, Amsterdam, November 4, 2016) [The Rule of Law in the Technological Age Challenges and Opportunities for the EU Collected Papers (July 20, 2017) 9-17. Amsterdam Law School Research Paper No. 2017-35. Available at SSRN: https://ssrn.com/abstract=3005914].

98 Shawn Bayern, Thomas Burri, Thomas D. Grant, Daniel M. Häusermann, Florian Möslein, and Richard Williams, 'Company Law and Autonomous Systems: A Blueprint for Lawyers, Entrepreneurs, and Regulators' (2017) 9 *Hastings Science and Technology Law Journal* 135, 156.

99 See, e.g., Bert-Jaap Koops, Mireille Hildebrandt, and David-Olivier Jaquet-Chiffelle, 'Bridging the Accountability Gap: Rights for New Entities in the Information Society?' (2010) 11 *Minnesota Journal of Law, Science and Technology* 497.

100 Almost by the day, the media carry pieces that further fuel and contribute to this debate: see, e.g., David Aaronovitch, 'Bringing law and order to digital Wild West' *The Times*, January 4, 2018, p 25; and Edward Munn, 'YouTube severs (some of) its ties with Logan Paul' available at http://www.alphr.com/life-culture/1008081/youtube-severs-some-of-its-ties-with-logan-paul (last accessed January 11, 2018).

principle, we might argue that such intermediaries should be held strictly liable for any or some classes of illegal content; or that they should be liable if they fail to take reasonable care; or that they should be immunised against liability even though the content is illegal. If we take a position at the strict liability end of the range, we might worry that the liability regime is too burdensome to intermediaries and that on-line services will not expand in the way that we hope; but, if we take a position at the immunity end of the range, we might worry that this treats the Internet as an exception to the Rule of Law and is an open invitation for the illegal activities of copyright infringers, paedophiles, terrorists and so on. In practice, most legal systems balance these interests by taking a position that confers an immunity but only so long as the intermediaries do not have knowledge or notice of the illegal content. Predictably, now that the leading intermediaries are large US corporations with deep pockets, and not fledgling start-ups, many think that the time is ripe for the balance to be reviewed.[101] However, finding a balance that is generally acceptable, in both principle and practice, is another matter.[102] Moreover, it does not follow that a balance that is acceptable in, say, China will also be acceptable in, say, Europe or the United States.[103]

Where the content that is carried or hosted is perfectly lawful, we might think that there is no interest to set against its online presence. Indeed, we might think that, in a community that is fundamentally committed to freedom of expression, there are strong reasons for keeping such content available. However, there might be an interest, not in relation to the removal of the content, but in relation to the way in which search engines 'advertise' or 'signpost' or 'direct towards' the content at issue. In other words, there might be a 'right to be forgotten' of the kind

---

101 For a particularly compelling analysis, see Marcelo Thompson, 'Beyond Gatekeeping: the Normative Responsibility of Internet Intermediaries' (2016) 18 *Vanderbilt Journal of Entertainment and Technology Law* 783.

102 In the EU, there is also the question of whether national legislative initiatives—such as the recent German NetzDG, which is designed to encourage social networks to process complaints about hate speech and other criminal content more quickly and comprehensively—are compatible with the provisions of Directive 2000/31/EC on e-commerce: see, for discussion of this particular question, Gerald Spindler, 'Internet Intermediary Liability Reloaded—The New German Act on Responsibility of Social Networks and its (In-) Compatibility With European Law', available at https://www.jipitec.eu/issues/jipitec-8-2-2017/4567.

103 Dr Lingling Wei has led a team researching this question in relation to intermediaries in China: see https://microsites.bournemouth.ac.uk/cippm/2017/03/01/regulating-isp-in-china-dissemination-conference-in-beijing/ (last accessed February 6, 2018).

upheld by the Court of Justice of the European Union (the CJEU) in the *Google Spain* case that we have already discussed.[104]

Summing up, if we frame our understanding of regulatory responsibilities in this way, we will have the shape of an answer to our earlier question of what regulators should make of the mapping of informational interests. Quite simply, the first priority is for regulators to scan the map to consider whether any of these interests are implicated in the commons conditions. In particular, if there are any informational wrongs that touch and concern the commons, regulators should take protective steps. Secondly, regulators should endeavour to protect those interests, whether expressed as rights or wrongs, that give the community its particular identity as an information society. Thirdly, regulators should strive to find acceptable balances of the plurality of legitimate interests that compete and conflict with one another in the day-to-day legal disputes and general politics of the community.

4 Some Lines of Inquiry

There is much in the foregoing that invites further analysis and further inquiry. In what remains of the Working Paper, I will outline two avenues for further inquiry. The first, focusing on the particular roles and competences that we typically assign to different branches of government, asks whether we are geared institutionally to do justice to the challenges of Infosoc 2018. The second, focusing on the disruptions occasioned by new technologies to the legal and regulatory mind-set, asks whether we are engaging with the regulation of novel technologies in the right way. In other words, are we institutionally prepared to engage with technologies that impact on our informational interests and do we engage with new technological developments in the right way?

4.1 Institutional Roles and Responsibilities

In the late 1970s, when techniques for assisted conception were being developed and applied, but also being seriously questioned, the response of the UK government was to set up a Committee of Inquiry chaired by Mary Warnock. In 1984, the Committee's report (the Warnock Report) was published.[105] However, it was not until 1990, and after much debate in Parliament, that the framework legislation, the Human Fertilisation and Embryology Act 1990,

---

104 See section 2.1.2 above.

105 *Report of the Committee of Inquiry into Human Fertilisation and Embryology* (London: HMSO, Cm. 9314, 1984).

was enacted. This process, taking the best part of a decade, is regularly held up as an example of best practice when dealing with emerging technologies. Nevertheless, this methodology is not in any sense the standard operating procedure for engaging with new technologies—indeed, there is no such procedure.[106]

The fact of the matter is that legal and regulatory responses to emerging technologies vary from one technology to another, from one legal system to another, and from one time to another. Sometimes, there is extensive public engagement, sometimes not. On occasion, special Commissions (such as the now defunct Human Genetics Commission in the UK) have been set up with a dedicated oversight remit; and there have been examples of standing technology foresight commissions (such as the US Office of Technology Assessment)[107]; but, often, there is nothing of this kind. Most importantly, questions about new technologies sometimes surface, first, in litigation (leaving it to the Courts to determine how to respond) and, at other times, they are presented to the legislature (as was the case with assisted conception).

With regard to the question of which regulatory body engages with new technologies and how, there can of course be some local agency features that shape the answers. Where, as in the United States, there is a particular regulatory array with each agency having its own remit, a new technology might be considered in just one lead agency or it might be assessed in several agencies.[108] Once again, there is a degree of happenstance about this. Nevertheless, in a preliminary way, we can make three general points.

First, if the question is put to the Courts, their responsibility for the integrity of the law will push them towards a 'coherentist' assessment.[109] By this, I mean that courts, and the lawyers who argue cases in the courts, will tend to look for existing doctrinal pegs and anchors. Typically, the courts, being neither sufficiently resourced nor mandated to undertake a risk assessment let alone adopt a risk management strategy (unless the legislature has already put

---

106 See Roger Brownsword, Law, Regulation, and Technology: Supporting Innovation, Managing Risk and Respecting Values' in Todd Pittinsky (ed), *Handbook of Science, Technology and Society* (Cambridge: Cambridge University Press, 2018).

107 On which, see Bruce Bimber, *The Politics of Expertise in Congress* (Albany: State University of New York Press, 1996) charting the rise and fall of the Office and drawing out some important tensions between 'neutrality' and 'politicisation' in the work of such agencies.

108 Compare, Albert C. Lin, 'Size Matters: Regulating Nanotechnology' (2007) 31 *Harvard Environmental Law Review* 349.

109 See section 4.2.2.1 below.

in place a scheme that delegates such a responsibility to them),[110] will default to recognised legal concepts, categories, and principles. The aim of the exercise will be to subsume the new technology within the existing legal framework.[111]

Secondly, if the question finds its way into the legislative arena, it is much more likely that politicians will engage with it in a regulatory-instrumentalist way; and, once the possibility of technological measures gets onto the radar, it is much more likely that (as with institutions in the EU) we will see a more technocratic mind-set.

Thirdly, if leaving so much to chance seems unsatisfactory, then it is arguable that there needs to be a body that is charged with undertaking the preliminary engagement with new technologies. The task of such a body would be to ensure that such technologies are channelled to our most urgent needs (relative to the commons); and, for each community, the challenge is to address the basic question of the kind of society that it distinctively wants to be—and, to do that, moreover, in a context of rapid social and technological change. As Wendell Wallach rightly insists:

> Bowing to political and economic imperatives is not sufficient. Nor is it acceptable to defer to the mechanistic unfolding of technological possibilities. In a democratic society, we—the public—should give approval to the futures being created. At this critical juncture in history, an informed conversation must take place before we can properly give our assent or dissent.[112]

Granted, the notion that we can build agencies that are fit for such purposes might be an impossible dream. Nevertheless, I join those who argue that this is the right time to set up a suitably constituted body[113]—possibly along the lines of the Centre for Data Ethics and

---

110 Perhaps we should view Patent Offices in this light. In the 1980s, there were major decisions to be made about the patentability of biotechnological products and processes, models of which could not be brought into the Office to demonstrate how they worked and which also raised complex moral issues. For extended discussion, see Alain Pottage and Brad Sherman, *Figures of Invention: A History of Modern Patent Law* (Oxford: Oxford University Press, 2010); and, on the moral dimension of these debates, see Deryck Beyleveld and Roger Brownsword, *Mice, Morality and Patents* (London: Common Law Institute of Intellectual Property, 1993).

111 Compare the analysis in Bayern et al (n 94) where company structures that are provided for in US, German, Swiss, and UK law are reviewed to see whether they might plausibly act as a host for autonomous systems that provide a service (such as file storage, file retrieval and metadata management).

112 See, Wendell Wallach, *A Dangerous Master* (Basic Books, 2015) at 10.

113 Amongst many matters in this paper that invite further discussion, the composition of such a Commission invites debate. See, too, Wallach (n 112) Chs 14-15.

Innovation (to set standards for the ethical use of AI and data) as announced by the UK government in late 2017[114]—that would underline our responsibilities for the commons as well as facilitating the development of each community's regulatory and social licence for these technologies.[115]

4.2 Tensions in the regulatory discourse

Technology disrupts the law in two ways; first, it impacts on the content of traditional law which, no longer being appropriate, has to be revised; and, secondly, it disrupts the assumption that social ordering has to be directed by rules (or norms or standards)—instead, there might be technological fixes. These disruptions provoke three legal mind-sets: coherentist, regulatory-instrumentalist, and technocratic.

We can start with the disruptions before moving on to the three mind-sets and then asking which mind-set should be engaged.

4.2.1 Two kinds of disruption

It is trite that technology has disruptive effects on both economic and social relations. The context in which law operates is thus disrupted and this generates the first kind of disruption on law itself. However, as technology presents itself as a regulatory tool, we have a second form of disruption.[116]

4.2.1.1 The first disruption

---

114 See 'Autumn Budget 2017: 25 things you need to know' (H.M. Treasury, November 22, 2017) point 16: available at https://www.gov.uk/government/news/autumn-budget-2017-25-things-you-need-to-know (last accessed November 25, 2017).

115 Compare Geoff Mulgan's proposal for the establishment of a Machine Intelligence Commission: available at http://www.nesta.org.uk/blog/machine-intelligence-commission-uk (blog 'A machine intelligence commission for the UK', February 22, 2016: last accessed December 11, 2016); Olly Bustom et al, *An Intelligent Future? Maximising the Opportunities and Minimising the Risks of Artificial Intelligence in the UK* (Future Advocacy, London, October 2016) (proposing a Standing Commission on AI to examine the social, ethical, and legal implications of recent and potential developments in AI); HC Science and Technology Committee, *Robotics and Artificial Intelligence* HC 145 2016-17.

116 For this second kind of disruption and its significance, see e.g. Roger Brownsword, 'In the Year 2061: From Law to Technological Management' (2015) 7 *Law, Innovation and Technology* 1; 'Field, Frame and Focus: Methodological Issues in the New Legal World' in Rob van Gestel, Hans Micklitz, and Ed Rubin (eds), *Rethinking Legal Scholarship* (Cambridge: Cambridge University Press, 2016) 112; and, '*Law as a Moral Judgment*, the Domain of Jurisprudence, and Technological Management' in Patrick Capps and Shaun D. Pattinson (eds), *Ethical Rationalism and the Law* (Oxford: Hart, 2016) 109.

In the nineteenth century, we find technology disrupting the content of criminal law, torts, and contract law. So, while intentionality and fault were set aside in the regulatory parts of criminal law and torts, classical transactionalist ideas of consent and agreement were marginalised in the *mainstream* of contract law being replaced by 'objective' tests and standards set by reasonable business practice. As Morton Horwitz puts it, with the disruption of legal rules, there was a dawning sense that 'all law was a reflection of collective determination, and thus inherently regulatory and coercive.'[117]

What we see across these developments is a pattern of disruption to legal doctrines that were organically expressed in smaller-scale non-industrialised communities. Here, the legal rules presuppose very straightforward ideas about holding those who engage intentionally in injurious or dishonest acts to account, about expecting others to act with reasonable care, and about holding others to their word. Once new technologies disrupt these ideas, we see the move to strict or absolute criminal liability without proof of intent, to tortious liability without proof of fault, and to contractual liability (or limitation of liability) without proof of actual intent, agreement or consent. Even if the development in contract is less clear at this stage, in both criminal law and torts we can see the early signs of a risk management approach to liability. Moreover, we also see the early signs of doctrinal bifurcation,[118] with some parts of criminal law, tort law and contract law resting on traditional principles (and representing, so to speak, 'real' crime, tort and contract) while others deviate from these principles—often holding enterprises to account more readily but also sometimes easing the burden on business for the sake of beneficial innovation[119]—in order to strike a more acceptable balance of the benefits and risks that technological development brings with it.

---

117 Morton J. Horwitz, *The Transformation of American Law 1870-1960* (Oxford: Oxford University Press, 1992) at 50.

118 As recognised, for example, in the Canadian Supreme Court case of *R. v. Sault Ste. Marie* [1978] 2 S.C.R. 1299, where (at 1302-1303) Dickson J remarks:

> In the present appeal the Court is concerned with offences variously referred to as "statutory," "public welfare," "regulatory," "absolute liability," or "strict responsibility," which are not criminal in any real sense, but are prohibited in the public interest….Although enforced as penal laws through the utilization of the machinery of the criminal law, the offences are in substance of a civil nature and might well be regarded as a branch of administrative law to which traditional principles of criminal law have but limited application. They relate to such everyday matters as traffic infractions, sales of impure food, violations of liquor laws, and the like. In this appeal we are concerned with pollution.

119 For example, in the United States, the interests of the farming community were subordinated to the greater good promised by the development of the railroad network: see Morton J. Horwitz, *The Transformation of American Law 1780-1860* (Cambridge, Mass.: Harvard University Press, 1977).

4.2.1.2 The second disruption

Arguably, the second technological disruption (manifesting itself in the turn to architecture, design, coding, and the like as a regulatory tool) is as old as the (defensive) architecture of the pyramids and the target-hardening use of locks. However, the variety and sophistication of the instruments of technological management that are available to regulators today is strikingly different to the position in both pre-industrial and early industrial societies. Whether or not this amounts to a difference of kind or merely one of degree scarcely seems important; we live in different times, with significantly different regulatory technologies. In particular, there is much more to technological management than traditional target-hardening: the management involved might—by designing products and places, or by coding products and people—disable or exclude potential wrongdoers as much as harden targets or immunise potential victims; and, there is now the prospect of widespread automation that takes humans altogether out of the regulatory equation. Crucially, with a risk management approach well-established, regulators now find that they have the option of responding by employing various technological instruments rather than rules. This is the moment when, so to speak, we see a very clear contrast between the legal and regulatory style of the East coast (whether traditional or progressive) and the style of the West coast.[120]

Two things are characteristic of technological management. First, as I have emphasised elsewhere, unlike rules, the focus of the regulatory intervention is on the practical (not the paper) options of regulatees.[121] Secondly, whereas legal rules back their prescriptions with *ex post* penal, compensatory, or restorative measures, the focus of technological management is entirely *ex ante*, aiming to anticipate and prevent wrongdoing rather than punish or compensate after the event. As Lee Bygrave puts it in the context of the design of information systems and the protection of both IPRs and privacy, the assumption is that, by embedding norms in the

120 Seminally, see Lawrence Lessig, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999). See, too, Roger Brownsword, 'Code, Control, and Choice: Why East is East and West is West' (2005) 25 *Legal Studies* 1.

121 See, e.g., Roger Brownsword, 'Whither the Law and the Law Books: From Prescription to Possibility' (2012) 39 *Journal of Law and Society* 296; and 'Law, 'Law, Liberty and Technology' in Roger Brownsword, Eloise Scotford, and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford University Press, 2016 [e-publication]; and 2017) 41.

architecture, there is 'the promise of a significantly increased *ex ante* application of the norms and a corresponding reduction in relying on their application *ex post facto*.'[122]

4.2.2 Three Legal Mind-Sets

According to Edward Rubin, we live in the age of modern administrative states where the law is used 'as a means of implementing the policies that [each particular state] adopts. The rules that are declared, and the statutes that enact them, have no necessary relationship with one another; they are all individual and separate acts of will.'[123] In other words,

> Regulations enacted by administrative agencies that the legislature or elected chief executive has authorized are related to the authorizing statute, but have no necessary connection with each other or to regulations promulgated under a different exercise of legislative or executive authority.[124]

In the modern administrative state, the 'standard for judging the value of law is not whether it is coherent but rather whether it is effective, that is, effective in establishing and implementing the policy goals of the modern state.'[125] By contrast, the distinctive feature of 'coherentism' is the idea that law forms 'a coherent system, a set of rules that are connected by some sort of logical relationship to each other'[126]—or 'a system of rules that fit together in a consistent logically elaborated pattern'.[127] Moreover, within the modern administrative state, the value of coherence itself is transformed: coherence, like the law, is viewed as 'an instrumental device that is deployed only when it can be effective.'[128] In a concluding call to arms, Rubin insists

---

122 Lee A. Bygrave, 'Hardwiring Privacy' in Roger Brownsword, Eloise Scotford, and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford University Press, 2017) 754, at 755.

123 Edward L. Rubin, 'From Coherence to Effectiveness' in Rob van Gestel, Hans-W Micklitz, and Edward L. Rubin (eds), *Rethinking Legal Scholarship* (New York: Cambridge University Press, 2017) 310 at 311.

124 Rubin (n 123) at 311.

125 Rubin (n 123) at 328.

126 Rubin (n 123) at 312.

127 Rubin (n 123) at 313.

128 Rubin (n 123) at 328.

that legal scholarship needs to 'wake from its coherentist reveries'[129]; and that legal scholars 'need to relinquish their commitment to coherence and concern themselves with the effectiveness of law and its ability to achieve our democratically determined purposes.'[130]

No doubt, there are some caveats that we might have in relation to Rubin's view, particularly with regard to the relationship between regulatory effectiveness and regulatory legitimacy. However, for my purposes, we can draw on Rubin to construct two ideal-typical mind-sets in thinking about the way that the law should engage with new technologies and, more generally, about the reform and renewal of the law. One ideal-type, 'regulatory-instrumentalism', views legal rules as a means to implement whatever policy goals have been adopted by the State; the adequacy and utility of the law is to be assessed by its effectiveness in delivering these goals. The other ideal-type is 'coherentism', according to which the adequacy of the law is to be assessed by reference to the doctrinal consistency and integrity of its rules. Where 'regulatory-instrumentalism' informs a proposal for reform, the argument will be that some part of the law 'does not work' relative to desired policy goals. By contrast, where 'coherentism' informs a proposal for reform, the argument will be that there is a lack of clarity in the law or that there are internal inconsistencies or tensions within the law that need to be resolved.

Although Rubin does not suggest that the shift from a traditional coherentist to a regulatory-instrumentalist mind-set is associated with the emergence of technologies, it is of course precisely this shift that I am suggesting reflects the first technological disruption of the law.

We can now say a bit more about both coherentist and regulatory-instrumentalist views before focusing on the technocratic mind-set that is distinctively provoked by the second disruption; and then we can begin to reflect on the question of which of these mind-sets should be engaged and when it should be engaged.

4.2.2.1 Coherentist

It is axiomatic within coherentism that the law should be formally consistent; and, while there might be some confusion, uncertainty and inefficiency if legal rules are contradictory or in

[129] Rubin (n 123) at 349. For scholarly concerns that include but also go beyond coherentism, see Roger Brownsword, 'Maps, Critiques, and Methodologies: Confessions of a Contract Lawyer' in Mark van Hoecke (ed), *Methodologies of Legal Research* (Oxford: Hart, 2011) 133.

[130] Rubin (n 123) at 350; and, compare the seminal ideas in Hugh Collins, *Regulating Contracts* (Oxford: Oxford University Press, 1999).

tension, the coherence of legal doctrine is typically viewed as desirable in and of itself.[131] However, coherentism also has a substantive dimension. Thus, in Rubin's account of coherentism, the law (when satisfying coherentist standards) not only displays an internal consistency and integrity, it also expresses and concretises higher 'natural law' principles, all this being distilled by an intellectual elite applying their rational wisdom.[132] Although, even now, we might detect traces of such top-down 'pre-modern' thinking (as Rubin puts it), this is not a necessary characteristic. Rather, coherentists draw on simple traditional principles that are generally judged to be both reasonable and workable. The law, on this view, is about responding to 'wrongs', whether by punishing wrongdoers or by compensating victims; it is about correction and rectification, and holding wrongdoers to account. In the field of transactions, there are echoes of this idea in the notion that the law of contract should be guided, as Lord Steyn has put it, by the simple ideal of fulfilling the expectations of honest and reasonable people;[133] and, in the field of interactions, it almost goes without saying that the law of tort should be guided by the standards and expectations of these same honest and reasonable people.

Anticipating the contrast between this coherentist mind-set and mind-sets that are more instrumental and/or technocratic, we should emphasise that the formal and substantive dimensions of coherentism betray little or no sense of the direction in which the law should be trying to move things. Coherentism looks up and down, backwards, and even sideways, but not forward. It is not instrumental; it is not about engineering change. Moreover, insofar as coherentists are focused on righting wrongs, their gaze is not on prevention and certainly not on the elimination of practical options.

There is one further important aspect of coherentist thinking, a feature that manifests itself quite regularly now that new technologies and their applications present themselves for classification and characterisation relative to established legal concepts and categories.[134] Here,

---

131 The jurisprudence is replete with illustrations but see, e.g., Arden LJ in *Stena Line v Merchant Navy Ratings Pension Fund Trustees Limited* [2011] EWCA Civ 543 at [36]:

> The internal coherence of the law is important because it enables the courts to identify the aims and values that underpin the law and to pursue those values and aims so as to achieve consistency in the structure of the law.

132 Rubin (n 123).

133 Seminally, see Johan Steyn, 'Contract Law: Fulfilling the Reasonable Expectations of Honest Men' (1997) 113 *Law Quarterly Review* 433.

134 Compare Bayern et al (n 98); and Koops et al (n 99).

we find a coherentist reluctance to abandon existing categories and contemplate bespoke responses. For example, rather than recognise new types of intellectual property, coherentists will prefer to tweak existing laws of patents and copyright.[135] Similarly, we will recall Lord Wilberforce's much-cited remarks on the heroic efforts made by the courts—confronted by modern forms of transport, various kinds of automation, and novel business practices—to force 'the facts to fit uneasily into the marked slots of offer, acceptance and consideration'[136] or whatever other traditional categories of the law of contract might be applicable. And, in transactions, this story continues; coherentism persists. So, for example, coherentists will want to classify e-mails as either instantaneous or non-instantaneous forms of communication (or transmission),[137] they will want to apply the standard formation template to online shopping sites, they will want to draw on traditional notions of agency in order to engage electronic agents and smart machines,[138] and they will want to classify individual 'prosumers' and 'hobbyists' who buy and sell on new platforms (such as platforms that support trade in 3D printed goods)[139] as either business sellers or consumers.[140] As the infrastructure for transactions becomes ever more technological the tension between this strand of common law coherentism and regulatory-instrumentalism becomes all the more apparent.[141]

---

135 Compare the analysis of multi-media devices in Tanya Aplin, *Copyright Law in the Digital Society: the Challenges of Multimedia* (Oxford: Hart, 2005).

136 As Lord Wilberforce put it in *New Zealand Shipping Co Ltd v A.M. Satterthwaite and Co Ltd : The Eurymedon* [1975] AC 154, 167.

137 See, e.g., Andrew Murray, 'Entering into Contracts Electronically: the Real WWW' in Lilian Edwards and Charlotte Waelde (eds), *Law and the Internet: A Framework for Electronic Commerce* (Oxford: Hart, 2000) 17; and Eliza Mik, 'The Effectiveness of Acceptances Communicated by Electronic Means, Or – Does the Postal Acceptance Rule Apply to Email?' (2009) 26 *Journal of Contract Law* 68 (concluding that such classificatory attempts should be abandoned).

138 Compare, e.g., Emily Weitzenboeck, 'Electronic Agents and the Formation of Contracts' (2001) 9 *International Journal of Law and Information Technology* 204.

139 On IP and the governance of 3D platforms, see Dinusha Mendis, '"Clone Wars": Episode II – The Next Generation: The Copyright Implications Relating to 3D Printing and Computer-Aided Design (CAD) Files' (2014) 6 *Law, Innovation and Technology* 265; and Dinusha Mendis, Jane Nielsen, Dianne Nicol, and Phoebe Li, 'The Coexistence of Copyright and Patent Laws to Protect Innovation: A Case Study of 3D Printing in UK and Australian Law' in Roger Brownsword, Eloise Scotford, and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford University Pres, 2017) 451.

140 Compare e.g., Christian Twigg-Flesner,'Conformity of 3D Prints—Can Current Sales Law Cope?' in R. Schulze and D. Staudenmayer (eds), *Digital Revolution: Challenges for Contract Law in Practice* (Baden-Baden: Nomos, 2016) 35.

141 For further discussion, see Roger Brownsword, 'After Brexit: Regulatory-Instrumentalism, Coherentism, and the English Law of Contract' (2018) 35 *Journal of Contract Law* (forthcoming) and 'Smart

4.2.2.2 Regulatory-Instrumentalist

'Regulation' is generally understood as a process of directing regulatees, monitoring and detecting deviation, and correcting for non-compliance, all of this relative to specified regulatory purposes. The regulatory mind-set is, at all stages, instrumental. The question is: what works? When a regulatory intervention does not work, it is not enough to restore the status quo; rather, further regulatory measures should be taken, learning from previous experience, with a view to realising the regulatory purposes more effectively. Hence, the purpose of the criminal law is not simply to respond to wrongdoing (as corrective justice demands) but to reduce crime by adopting whatever measures of deterrence promise to work.[142] Similarly, in a safety-conscious community, the purpose of tort law is not simply to respond to wrongdoing but to deter practices and acts where agents could easily avoid creating risks of injury and damage. For regulatory-instrumentalists, the path of the law should be progressive: we should be getting better at regulating crime and improving levels of safety.[143]

One of the striking features of the European Union has been the single market project, a project that the Commission has pursued in a spirit of conspicuous regulatory-instrumentalism. Here, the regulatory objectives are: (i) to remove obstacles to consumers shopping across historic borders; (ii) to remove obstacles to businesses (especially small businesses) trading across historic borders; and (iii) to achieve a high level of consumer protection. In order to realise this project, it has been essential to channel the increasing number of member states towards

---

Contracts: Coding the Contract, Decoding the Legal Debates' (forthcoming) (further distinguishing between a 'transactionalist' variant of coherentism and a 'relationalist' variant).

142 Compare David Garland, *The Culture of Control: Crime and Social Order in Contemporary Society* (Oxford: Oxford University Press, 2001); and Amber Marks, Benjamin Bowling, and Colman Keenan, 'Automatic Justice? Technology, Crime, and Social Control' in Roger Brownsword, Eloise Scotford, and Karen Yeung (eds), *The Oxford Handbook of Law, Regulation and Technology* (Oxford: Oxford University Press, 2017) 705.

143 The parallel development of a risk-management ideology in both criminal law and tort is noted by Malcolm Feeley and Jonathan Simon, 'Actuarial Justice: The Emerging New Criminal Law' in David Nelken (ed), *The Futures of Criminology* (London: Sage, 1994) 173. At 186, Feeley and Simon say:

> Although social utility analysis or actuarial thinking is commonplace enough in modern life…in recent years this mode of thinking has gained ascendancy in legal discourse, a system of reasoning that traditionally has employed the language of morality and focused on individuals….
> Thus, for instance, it is by now the conventional mode of reasoning in tort law. Traditional concerns with fault and negligence standards—which require a focus on the individual and concern with closely contextual causality—have given way to strict liability and no-fault. One sees this in both doctrines, and even more clearly in the social vision that constitutes the discourse about modern torts. The new doctrines ask, how do we 'manage' accidents and public safety. They employ the language of social utility and management, not individual responsibility.

convergent legal positions. Initially, minimum harmonisation Directives were employed, leaving it to member states to express the spirit and intent of Directives in their own doctrinal way. To this extent, a degree of divergence was tolerated in the way that the regional inputs were translated into national outputs that, in turn, might become the relevant legal material for interpretation and application. However, where the Commission needed a stronger steer, it could (and did) resort to the use of maximum harmonisation measures (restricting the scope for local glosses on the law); and, where Directives did not work, then Regulations could be used (a case in point being the recent GDPR[144]), leaving member states with even less room for local divergence.

As the single market project evolves into the digital Europe project, the Commission's regulatory-instrumentalist mind-set is perfectly clear. As the Commission puts it:

> The pace of commercial and technological change due to digitalisation is very fast, not only in the EU, but worldwide. The EU needs to act now to ensure that business standards and consumer rights will be set according to common EU rules respecting a high-level of consumer protection and providing for a modern business friendly environment. It is of utmost necessity to create the framework allowing the benefits of digitalisation to materialise, so that EU businesses can become more competitive and consumers can have trust in high-level EU consumer protection standards. By acting now, the EU will set the policy trend and the standards according to which this important part of digitalisation will happen.[145]

In this context, coherentist thoughts about tidying up and standardising the lexicon of the consumer acquis, or pushing ahead with a proposed Common European Sales Law,[146] or codifying European contract law drop down the list of priorities. For regulatory-instrumentalists, when we question the fitness of the law, we are not asking whether legal doctrine is consistent, we are asking whether it is fit for delivering the regulatory purposes.

---

144 Regulation (EU) 2016/679.

145 European Commission, Communication from the Commission to the European Parliament, the Council and the European Economic and Social Committee, 'Digital contracts for Europe—Unleashing the potential of e-commerce' COM(2015) 633 final (Brussels, 9.12.2015), p 7.

146 Despite a considerable investment of legislative time, the proposal was quietly dropped at the end of 2014. This also, seemingly, signalled the end of the project on the Common Frame of Reference in which, for about a decade, there had been a huge investment of time and resource.

Last but not least, I take it to be characteristic of the regulatory-instrumentalist mind-set that the thinking becomes much more risk-focused. In the criminal law and in torts, the risks that need to be assessed and managed relate primarily to physical and psychological injury and to damage to property and reputation; in contract law, it is economic risks that are relevant. So, for example, we see in the development of product liability a scheme of acceptable risk management that responds to the circulation of products (such as cars or new drugs) that are beneficial but also potentially dangerous. However, this response is still in the form of a revised *rule* (it is not yet technocratic); and it is still in the nature of an *ex post* correction (it is not yet *ex ante* preventive). Nevertheless, it is only a short step from here to a greater investment in *ex ante* regulatory checks (for food and drugs, chemicals, and so on) and to the use of new technologies as preventive regulatory instruments.

4.2.2.3 Technocratic

As is well-known, there was a major debate in the United Kingdom at the time that seat belts were fitted in cars and it became a criminal offence to drive without engaging the belt. Tort law responded, too, by treating claimant drivers or passengers who failed to engage their seat belts as, in part, contributing to their injuries.[147] Critics saw this as a serious infringement of their liberty—namely, their option to drive with or without the seat belt engaged. Over time, though, motorists became encultured into compliance. So far, we might say, so regulatory-instrumentalist.

Suppose, though, that motorists had not become encultured into compliance. Given the difficulty of enforcing a rule requiring seat belts to be engaged, regulatory-instrumentalism might have taken a more technocratic turn. For example, there might have been a proposal to design vehicles so that cars were simply immobilised if seat belts were not worn. In the USA, where such a measure of technological management was indeed adopted before being rejected, the implications for liberty were acutely felt.[148] Although the (US) Department of Transportation estimated that the so-called interlock system would save 7,000 lives per annum and prevent 340,000 injuries, 'the rhetoric of prudent paternalism was no match for visions of

147 *Froom v Butcher* [1976] QB 286.

148 Jerry L. Mashaw and David L. Harfst, *The Struggle for Auto Safety* (Cambridge, Mass.: Harvard University Press, 1990) Chapter 7.

technology and "big brotherism" gone mad'.[149] Taking stock of the legislative debates of the time, Jerry Mashaw and David Harfst remark:

> Safety was important, but it did not always trump liberty. [In the safety lobby's appeal to vaccines and guards on machines] the freedom fighters saw precisely the dangerous, progressive logic of regulation that they abhorred. The private passenger car was not a disease or a workplace, nor was it a common carrier. For Congress in 1974, it was a private space.[150]

Not only does technological management of this kind aspire to limit the practical options of motorists, including removing the real possibility of non-compliance with the law, there is a sense in which it supersedes the rules of law themselves.

Today, similar debates might be had about the use of mobile phones by motorists. There are clear and dramatic safety implications but many drivers persist in using their phones while they are in their cars. If we are to be technocratic in our approach, perhaps we might seek a design solution that disables phones within cars, or while the user is driving. However, once automated vehicles relieve 'drivers' of their safety responsibilities, it seems that the problem will drop away—rules that penalise humans who use their mobile phones while driving will become redundant; humans will simply be transported in vehicles and the one-time problem of driving while phoning will no longer be an issue.

So, unlike coherentists, technocrats are not concerned with doctrinal integrity and their focus is not on restoring the status quo prior to wrongdoing; and, unlike regulatory-instrumentalists who do view the law in a purposive way, technocrats—or, at any rate, those who are contemplating interventions at the hard end of the spectrum—are concerned with preventing or precluding wrongdoing and employing technological measures or solutions, rather than rules or standards, to achieve their objectives.

4.2.3 Which mind-set should be engaged?

Given that regulators might frame their thinking in very different ways, does it matter which mind-set they adopt; and, if so, which mind-set should they adopt? When and why should we think like coherentists, when like regulatory-instrumentalists, and when like technocrats?

---

149 Mashaw and Harfst (n 148) at 135.

150 Mashaw and Harfst (n 148) at 140.

To illustrate the significance of the regulatory framing, consider the following hypothetical posed by John Frank Weaver:

> [S]uppose the Aeon babysitting robot at Fukuoka Lucle mall in Japan is responsibly watching a child, but the child still manages to run out of the child-care area and trip an elderly woman. Should the parent[s] be liable for that kid's intentional tort?[151]

If we respond to this question (of the parents' liability) with the mind-set of a coherentist, we are likely to be guided by traditional notions of fault, responsibility, and corrective justice. On this view, liability would be assessed by reference to what communities judge to be fair, just and reasonable—and different communities might have different ideas about whether it would be fair, just and reasonable to hold the parents liable in the hypothetical circumstances. By contrast, if we respond like a regulatory-instrumentalist, the thinking is likely to be that before retailers, such as the shop at the mall, are to be licensed to introduce robot babysitters, and before parents are permitted to make use of robocarers, there needs to be a collectively agreed scheme of compensation should something 'go wrong'. On this view, the responsibilities and liabilities of the parents would be determined by the agreed terms of the risk management package. However, we might also imagine a third response, a response of a technocratic nature, seeking to design out the possibility of such an accident. Quite what measures of technological management might be suggested is anyone's guess—perhaps an invisible 'fence' at the edge of the care zone so that children (like supermarket trolleys or golf carts) simply could not stray beyond the limits. However, thinking about the puzzle in this way, the question would be entirely about designing the machines and the space in a way that (harmful) collisions between children and mall-goers simply could not happen.

Which of these responses is appropriate? On the face of it, coherentism belongs to relatively static and stable communities, not to the turbulent times of the Twenty-First Century. To assume that traditional legal frameworks enable regulators to ask the right questions and answer them in a rational way seems over-optimistic. If we reject coherentism, we will see regulatory-instrumentalism as a plausible default with the option of a technocratic resolution always to be considered.[152] However, there is a concern that regulatory-instrumentalism 'flattens' decision-

---

151 John Frank Weaver, *Robots Are People Too* (Santa Barbara, Ca: Praeger, 2014) at 89.

152 For a discussion in point, see David S. Wall, *Cybercrime* (Cambridge: Polity Press, 2007) where a number of strategies for dealing with 'spamming' are considered. As Wall says, if the choice is between ineffective legal rules and a technological fix (filters and the like), then most would go for the latter (at 201).

making, reducing all conflicts to a balance of interests and replacing respect for fundamental values such as respect for human rights and human dignity with an all-purpose utilitarianism. Moreover, concerns of this kind are amplified by the prospect of the use of technological management.

If we are to get some critical distance on these questions, we need to draw on the bigger picture of the responsibilities of regulators (as sketched in Part 3 above), including a view of where the red lines are drawn and what the priorities are.

Given that the paramount responsibility is to protect the commons, we might be concerned that, if regulators think in a traditional coherentist way, they might fail to take the necessary protective steps—steps that might involve new rules, or the use of measures of technological management, or both. This suggests that a regulatory-instrumentalist approach is a better default but it is only so if regulators are focused on the relevant risks—namely, the risks presented by technological development to the commons' conditions. Moreover, we might want to add that regulatory-instrumentalism with this particular risk focus is only a better default if it is applied with a suitably precautionary mentality. Regulators need to understand that compromising the commons is always the worst-case scenario.[153] Alongside such a default, a technocratic approach might well be appropriate. For example, if we believe that a rule-based approach cannot protect the planetary boundaries, then a geo-engineering approach might be the answer. However, it needs to be borne in mind that, with a resort to technological management, there is a risk of compromising the commons' conditions for self-development and moral agency (because both autonomy and virtue presuppose a context in which one acts freely). Arguably, this invites the articulation of a 'new coherentism', reminding regulators of two things: first, that their most urgent regulatory focus should be on the commons conditions; and, secondly, that, whatever their interventions, and particularly where they take a technocratic approach, their acts must always be compatible with the preservation of the commons.

If the default for regulators is a regulatory-instrumental mind-set, then the next priority for regulators is to be mindful that they should act in ways that are consistent with the fundamental

---

153 Compare Deryck Beyleveld and Roger Brownsword, 'Complex Technology, Complex Calculations: Uses and Abuses of Precautionary Reasoning in Law' in Marcus Duwell and Paul Sollie (eds), *Evaluating New Technologies: Methodological Problems for the Ethical Assessment of Technological Developments* (Dordrecht: Springer, 2009) 175; and 'Emerging Technologies, Extreme Uncertainty, and the Principle of Rational Precautionary Reasoning (2012) 4 *Law Innovation and Technology* 35.

values that make the community the particular community that it is. As I have suggested, communities experiencing the second technological disruption should try to agree on the relevant principles for the use of technological measures. These principles together with the community's particular constitutive values will represent a key dimension of the local articulation of the Rule of Law. This invites an extension of new coherentism such that regulators check their actions for compatibility with the Rule of Law as articulated in the community.

Finally, in relation to the third tier of regulatory responsibility, in particular cases, there might well be some contestation about whether regulators should be trying to balance interests or apply (in a traditional coherentist way) settled rules, concepts, and classifications. However, if it is agreed that the case is one that calls for a balancing exercise, then the regulatory-instrumentalist default seems to be appropriate.

That said, these remarks might seem to be somewhat divorced from the way in which organised societies allocate particular regulatory responsibilities. Indeed, is it not a feature of the Rule of Law and democratic political arrangements that the Courts will settle disputes in accordance with established legal principles and that it is for the Legislature and the Executive to formulate and agree public policies, plans and priorities? In other words, is it not the case that, while we expect judges and advocates in the Courts to reason like coherentists, we expect policy-making members of the Legislature and Executive to reason in a regulatory-instrumentalist way? To the extent that this is so, where in the regulatory array do we find the ultimate responsibility for stewardship of the commons and for the community's distinctive values? This returns us to where we started our suggestions for further inquiry.[154]

5 Concluding remarks

This Working Paper sketches a very broad field for possible inquiry. In our informational societies, our interests are dynamic and they are constantly disrupted by technological innovation. The field is not just broad, it is also deep; the turbulence that we find in the rhetoric of our claims relating to informational rights and wrongs reaches down to some basic interests that we have as human agents. In both dimensions, that of breadth as well as that of depth, there is much to be done to sharpen up this big picture of Infosoc 2018.

[154] Section 4.1 above.

With regard to the breadth of the field, it should be recalled that the informational rights and wrongs that are listed are intended only as indicative. Are there significant informational claims that we have omitted, and how would they fit in? For example, in our introductory remarks, mention was made of a right to explanation that is now being articulated in relation to decisions made by smart machines. How does this right lie relative to data protection rights, to the right to know, or to the right to truth?[155]

Then there are questions that look deeper into the anchoring of particular claims, and the relationships between particular informational rights and wrongs. For example, the informational wrongs that we associate with the surveillance state are typically expressed as a disproportionate interference with privacy; and, as we noted, privacy also can be read as a constraint on the disproportionate private collection of personal data.

The Working Paper is not only very provisional, it is also extremely uneven. While some lines of inquiry are merely hinted at, others are developed quite fully. For example, I have hinted at the articulation of a 'new coherentism' in our legal thinking but this is much less developed than my sketched scheme of regulatory responsibilities relative to the importance of particular informational interests (in Part 3) and my outline of the disruptions to legal thinking that arise from the development of new technologies (in Part 4). Both these particular sketches offer a lens for viewing debates about the legal framework for our information societies, as a means to interpret what is being said in regulatory debates and to elaborate one's own critical view of the regulatory priorities. We might also find that employing the general lens of informational rights and wrongs offers a new perspective on particular rights and wrongs (such as IPRs) in that landscape.

Let me end by repeating the caveat that I entered at the outset. This is an exercise in thinking aloud and in a very preliminary way. It is a long way from any kind of finished article. Nevertheless, many lawyers have a research interest in the broad field of our informational interests; and the thought occurs that there might be some intellectual gain if we view our particular research projects as contributions to a larger canvas. Furthermore, many communities are struggling with coming to terms with new technologies that bear on what we

[155] Where decision-making is automated, in order to ensure that the processing of data is fair and transparent, Article 13(2)(f) of the GDPR requires data controllers to provide meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject. Whether or not this amounts to a right to an (ex post) explanation of any particular decision actually made is moot.

are calling informational interests. Seeing the bigger picture might also have some impact in helping these communities to work out what kind of community they want to be.