

## Health Research and Privacy through the Lens of Public Interest

### *A Monocle for the Myopic?*

*Mark Taylor and Tess Whitton*

#### 24.1 INTRODUCTION

Privacy and public interest are reciprocal concepts, mutually implicated in each other's protection. This chapter considers how viewing the concept of privacy through a public interest lens can reveal the limitations of the narrow conception of privacy currently inherent to much health research regulation (HRR). Moreover, it reveals how the public interest test, applied in that same regulation, might mitigate risks associated with a narrow conception of privacy.

The central contention of this chapter is that viewing privacy through the lens of public interest allows the law to bring into focus more things of common interest than privacy law currently recognises. We are not the first to recognise that members of society share a common interest in both privacy and health research. Nor are we the first to suggest that public is not necessarily in opposition to private, with public interests capable of accommodating private and vice versa.<sup>1</sup> What is novel about our argument is the suggestion that we might invoke public interest requirements in current HRR to protect group privacy interests that might otherwise remain out of sight.

It is important that HRR takes this opportunity to correct its vision. A failure to do so will leave HRR unable to take into consideration research implications with profound consequences for future society. A failure will undermine legitimacy in HRR. It is no exaggeration to say that the value of a confidential healthcare system may come to depend on whether HRR acknowledges the significance of group data to the public interest. It is group data that shapes health policies, evaluates success, and determines the healthcare opportunities offered to members of particular groups. Individual opportunity, and entitlement, is dependent upon group classification.

The argument here is three-fold: (1) a failure to take common interests into account when making public interest decisions undermines the legitimacy of the decision-making process; (2) a common interest in privacy extends to include group interests; (3) the law's current myopia regarding group privacy interests in data protection law and the duty of confidence law can be corrected, to a varying extent, through bringing group privacy interests into view through the lens of public interest.

<sup>1</sup> The idea that both privacy and health research may be described as 'public interest causes' is also compelling developed in W. W. Lowrance, *Privacy, Confidentiality, and Health Research* (Cambridge University Press, 2012) and the relationship between privacy and the public interested in C. D. Raab, 'Privacy, Social Values and the Public Interest' in A. Busch and J. Hofmann (eds), *Politik und die Regulierung von Information [Politics and the Regulation of Information]* (Baden-Baden, Germany: Politische Vierteljahresschrift, Sonderheft 46, 2012), pp. 129–151.

## 24.2 COMMON INTERESTS, PUBLIC INTEREST AND LEGITIMACY

In this section, we seek to demonstrate how a failure to take the full range of common (group) interests into account when making public interest decisions will undermine the legitimacy of those decisions.

When Held described broad categories into which different theories of public interest might be understood to fall, she listed three: preponderance or aggregative theories, unitary theories and common interest theories.<sup>2</sup> When Sorauf earlier composed his own list, he combined common interests with values and gave the category the title ‘commonly-held value’.<sup>3</sup> We have separately argued that a compelling conception of public interest may be formed by uniting elements of ‘common interest’ and ‘common value’ theories of public interest.<sup>4</sup> It is, we suggest, through combining facets of these two approaches that one can overcome the limitations inherent to each. Here we briefly recap this argument before seeking to build upon it.

Fundamental to common interest theories of the public interest is the idea that something may serve ‘the ends of the whole public rather than those of some sector of the public’.<sup>5</sup> If one accepts the idea that there may be a common interest in privacy protection, as well as in the products of health research, then ‘common interest theory’ brings both privacy and health research within the scope of public interest consideration. However, it cannot explain how – in case of any conflict – they ought to be traded-off against each other – or other common interests – to determine *the* public interest in a specific scenario.

In contrast to common interest theories, commonly held *value* theories claim the ‘public interest emerges as a set of fundamental values in society’.<sup>6</sup> If one accepts that a modern liberal democracy places a fundamental value upon all members of society being respected as free and equal citizens, then any interference with individual rights should be defensible in terms that those affected can both access and have reason to endorse<sup>7</sup> – with discussion subject to the principles of public reasoning.<sup>8</sup> Such a commitment is enough to fashion a normative yardstick, capable of driving a public interest determination. However, the object of measurement remains underspecified.

It is through combining aspects of common interest and common value approaches that a practical conception of the public interest begins to emerge: any trade-off between common interests ought to be defensible in terms of common value: for reasons that those affected by a decision can both access and have reason to endorse.<sup>9</sup>

<sup>2</sup> V. P. Held, *The Public Interest and Individual Interests* (New York: Basic Books, 1970).

<sup>3</sup> F. J. Sorauf, ‘The Public Interest Reconsidered’, (1957), *The Journal of Politics*, 19(4), 616–639.

<sup>4</sup> M. J. Taylor ‘Health Research, Data Protection, and the Public Interest in Notification’, (2011) *Medical Law Review*, 19(2), 267–303; M. J. Taylor and T. Whitton, ‘Public Interest, Health Research and Data Protection Law: Establishing a Legitimate Trade-Off between Individual Control and Research Access to Health Data’, (2020) *Laws*, 9(1), 6.

<sup>5</sup> M. Meyerson and E. C. Banfield, cited by Sorauf ‘The Public Interest Reconsidered’, 619.

<sup>6</sup> J. Bell, ‘Public Interest: Policy or Principle?’ in R. Brownsword (ed.), *Law and the Public Interest: Proceedings of the 1992 ALSP Conference* (Stuttgart: Franz Steiner, 1993) cited in M. Feintuck, *Public Interest in Regulation* (Oxford University Press, 2004), p. 186.

<sup>7</sup> There is a connection here with what has been described by Rawls as ‘public reasons’: limited to premises and modes of reasoning that are accessible to the public at large. L. B. Solum, ‘Public Legal Reason’, (2006) *Virginia Law Review*, 92(7), 1449–1501, 1468.

<sup>8</sup> ‘The virtue of public reasoning is the cultivation of clear and explicit reasoning orientated towards the discovery of common grounds rather than in the service of sectional interests, and the impartial interpretation of all relevant available evidence.’ Nuffield Council on Bioethics, ‘Public Ethics and the Governance of Emerging Biotechnologies’, (Nuffield Council on Bioethics, 2012), 69.

<sup>9</sup> G. Gaus, *The Order of Public Reason: A Theory of Freedom and Morality in a Diverse and Bounded World* (Cambridge University Press, 2011), p. 19. Note the distinction Gaus draws here between the Restricted and the Expansive view of Freedom and Equality.

An advantage of this hybrid conception of public interest is its connection with (social) legitimacy.<sup>10</sup> If a decision-maker fails to take into account the full range of interests at stake, then not only do they undermine any public interest claim, but also the legitimacy of the decision-making process underpinning it.<sup>11</sup> Of course, this does not imply that the legitimacy of a system depends upon everyone perceiving the ‘public interest’ to align with their own contingent individual or common interests. Public-interest decision-making should, however, ensure that when the interests of others displace *any* individual’s interests, including those held in common, it should (ideally) be transparent why this has happened and (again, ideally) the reasons for displacement should be *acceptable* as ‘good reasons’ to the individual.<sup>12</sup> If the displaced interest is more commonly held, it is even more important for a system practically concerned with maintaining legitimacy, to transparently account for that interest within its decision-making process.

Any failure to account transparently for common interests will undermine the legitimacy of the decision-making process.

### 24.3 COMMON INTERESTS IN (GROUP) PRIVACY

In this section, the key claim is that a common interest in privacy extends beyond a narrow atomistic conception of privacy to include group interests.

We are aware of no ‘real definition’ of privacy.<sup>13</sup> There are, however, many stipulative or descriptive definitions, contingent upon use of the term within particular cultural contexts. Here we operate with the idea that privacy might be conceived in the legal context as representing ‘norms of exclusivity’ within a society: the normative expectation that *some* states of information separation are, by default, to be maintained.<sup>14</sup> This is a broad conception of privacy extending beyond the atomistic one that Bennet and Raab observe to be the prevailing privacy paradigm in many Western societies.<sup>15</sup> It is not necessary to defend a broad conception of privacy in order to

<sup>10</sup> We here associate legitimacy with ‘the capacity of the system to engender and maintain the belief that the existing political institutions are the most appropriate ones for the society’ S. M. Lipset, *Political Man: The Social Bases of Politics* (Baltimore, MD: Johns Hopkins University Press, 1981 [1959]), p. 64. This is consistent with recognition that the ‘liberal principle of legitimacy states that the exercise of political power is justifiable only when it is exercised in accordance with constitutional essentials that all citizens may reasonably be expected to endorse in the light of principles and ideals acceptable to them as reasonable and rational’, Solum, ‘Public Legal Reason’, 1472. See also D. Curtin and A. J. Meijer, ‘Does Transparency Strengthen Legitimacy?’, (2006) *Inform Polity II*, 11(2), 109–122, 112 and M. J. Taylor, ‘Health Research, Data Protection, and the Public Interest in Notification’, (2011) *Medical Law Review*, 19(2), 267–303.

<sup>11</sup> The argument offered is a development of one originally presented in M. J. Taylor, *Genetic Data and the Law* (Cambridge University Press, 2012), see esp. pp. 29–34.

<sup>12</sup> The term ‘accept’ is chosen over ‘prefer’ for good reason. M. J. Taylor and N. C. Taylor ‘Health Research Access to Personal Confidential Data in England and Wales: Assessing Any Gap in Public Attitude between Preferable and Acceptable Models of Consent’, (2014) *Life Sciences, Society and Policy*, 10(1), 1–24.

<sup>13</sup> A ‘real definition’ is to be contrasted with a nominal definition. A real definition may associate a word or term with elements that must necessarily be associated with the referent (a priori). A nominal definition may be discovered by investigating word usage (a posteriori). For more, see Stanford Encyclopedia of Philosophy, ‘Definitions’, (Stanford Encyclopedia of Philosophy, 2015), [www.plato.stanford.edu/entries/definitions/](http://www.plato.stanford.edu/entries/definitions/).

<sup>14</sup> G. Laurie recognises privacy to be a state of non-access. G. Laurie, *Genetic Privacy: A Challenge to Medico-Legal Norms* (Cambridge University Press, 2002) p. 6. We prefer the term ‘exclusivity’ rather than ‘separation’ as it recognises a lack of separation in one aspect does not deny a privacy claim in another. E.g. one’s normative expectations regarding use and disclosure are not necessarily weakened by sharing information with health professionals. For more see M. J. Taylor, *Genetic Data and the Law: A Critical Perspective on Privacy Protection* (Cambridge University Press, 2012), pp. 13–40.

<sup>15</sup> See, C. J. Bennet and C. D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (Ashgate, 2003), p. 13.

recognise a common interest in privacy protection. It is, however, necessary to broaden the conception in order to bring all of the *possible* common interests in privacy into view. As Bennet and Raab note, the atomistic conception of privacy

fails to properly understand the construction, value and function of privacy within society.<sup>16</sup>

Our ambition here is not to demonstrate an atomistic conception to be ‘wrong’ in any objective or absolute sense; but, rather to recognise the possibility that a coherent conception of privacy may extend its reach and capture additional values and functions. In 1977, after a comprehensive survey of the literature available at the time, Margulis proposed the following consensus definition of privacy

[P]rivacy, as a whole or in part, represents control over transactions between person(s) and other(s), the ultimate aim of which is to enhance autonomy and/or to minimize vulnerability.<sup>17</sup>

Nearly thirty years after the definition was first offered, Margulis recognised that his early attempt at a consensus definition

failed to note that, in the privacy literature, control over transactions usually entailed limits on or regulation of access to self (Allen, 1998), sometimes to groups (e.g., Altman, 1975), and occasionally to larger collectives such as organisations (e.g., Westin, 1967).<sup>18</sup>

The adjustment is important. It allows for a conception of privacy to recognise that there may be relevant norms, in relation to transactions involving data, that do not relate to identifiable individuals but are nonetheless associated with normative expectation of data flows and separation. Not only is there evidence that there are already such expectations in relation to non-identifiable data,<sup>19</sup> but data relating to groups – rather than just individuals – will be of increasing importance.<sup>20</sup>

There are myriad examples of how aggregated data have led to differential treatment of individuals due to association with group characteristics.<sup>21</sup> Beyond the obvious examples of individual discrimination and stigmatisation due to inferences drawn from (perceived) group membership, there can be group harm(s) to collective interests including, for example, harm connected to things held to be of common cultural value and significance.<sup>22</sup> It is the fact that data relates to the group level that leaves cultural values vulnerable to misuse of the data.<sup>23</sup> This

<sup>16</sup> Ibid.

<sup>17</sup> S. T. Margulis ‘Conceptions of Privacy: Current Steps and Next Steps’, (1977) *Journal of Social Issues*, 33(3), 5–21, 10.

<sup>18</sup> S. T. Margulis ‘Privacy as a Social Issue and a Behavioural Concept’, (2003) *Journal of Social Issues*, 9(2), 243–261, 245.

<sup>19</sup> Department of Health, ‘Summary of Responses to the Consultation on the Additional Uses of Patient Data’, (Department of Health, 2008).

<sup>20</sup> Our argument has no application to aggregate data that does not relate to a group until or unless that association is made.

<sup>21</sup> A number are described for example by V. Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor* (New York: St Martin’s Press, 2018).

<sup>22</sup> See e.g. *Foster v. Mountford* (1976) 14 ALR 71. (Australia)

<sup>23</sup> An example of the kind of common purpose that privacy may serve relates to the protection of culturally significant information. A well-known example of this is the harm associated with the research conducted with the Havasupai Tribe in North America. R. Dalton, ‘When Two Tribes Go to War’, (2004) *Nature*, 430(6999), 500–502; A. Harmon, ‘Indian Tribe Wins Fight to Limit Research of Its DNA’, *The New York Times* (21 April 2010). Similar concerns had been expressed by the Nuu-chah-nulth of Vancouver Island, Canada, when genetic samples provided for one purpose (to discover the cause of rheumatoid arthritis) were used for other purposes. J. L. McGregor, ‘Population Genomics and Research Ethics with Socially Identifiable Groups’, (2007) *Journal of Law and Medicine*, 35(3), 356–370, 362. Proposals to establish a genetic database on Tongans floundered when the ethics policy focused on the notion of individual informed consent and failed to take account of the traditional role played by the extended family in decision-making. B. Burton, ‘Proposed Genetic Database on Tongans Opposed’, (2002) *BMJ*, 324(7335), 443.

goes beyond a recognition that privacy may serve ‘not just individual interests but also common, public, and collective purposes’.<sup>24</sup> It is recognition that it is not only individual privacy but group privacy norms that may serve these common purposes. In fact, group data, and the norms of exclusivity associated with it, are likely to be of increasing significance for society. As Taylor, Floridi and van der Sloot note,

with big data analyses, the particular and the individual is no longer central. . . . Data is analysed on the basis of patterns and group profiles; the results are often used for general policies and applied on a large scale.<sup>25</sup>

This challenges the adequacy of a narrow atomistic conception of privacy to account for what will increasingly matter to society. De-identification of an individual as a member of a group, including those groups that may be created through the research and may not otherwise exist, does not protect against any relevant harm.<sup>26</sup> In the next part, we suggest that not only can the concept of the public interest be used to bring the full range of privacy interests into view, but that a failure to do so will undermine the legitimacy of any public interest decision-making process.

#### 24.4 GROUP PRIVACY INTERESTS AND THE LAW

The argument in this section is that, although HRR does not currently recognise the concept of group privacy interests, through the concept of public interest inherent to both the law of data protection and the duty of confidence, there is opportunity to bring group privacy interests into view.

##### 24.4.1 Data Protection Law

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (hereafter, Treaty 108) (as amended)<sup>27</sup> cast the template for subsequent data protection law when it placed the individual at the centre of its object and purpose<sup>28</sup> and defined ‘personal data’ as:

any information relating to an identified or identifiable individual (‘data subject’)<sup>29</sup>

This definition narrows the scope of data protection law even further than data relating to an individual. Data relating to unidentified or unidentifiable individuals fall outside its concern. This blinkered view is replicated through data protection instruments from the first through to the most recent: the EU General Data Protection Regulation (GDPR).

The GDPR is only concerned with personal data, defined in a substantively similar and narrow fashion to Treaty 108. In so far as its object is privacy protection, it is predicated upon a

<sup>24</sup> P. M. Regan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995) p. 221.

<sup>25</sup> L. Taylor et al. (eds), *Group Privacy: New Challenges of Data Technologies* (New York: Springer, 2017), p. 5.

<sup>26</sup> Taylor et al., ‘Group Privacy’, p. 7.

<sup>27</sup> Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Strasbourg, 28 January 1981, in force 1 October 1985, ETS No. 108, Protocol CETS No. 223.

<sup>28</sup> To protect every individual, whatever his or her nationality or residence, with regard to the processing of their personal data, thereby contributing to respect for his or her human rights and fundamental freedoms, and in particular the right to privacy.

<sup>29</sup> ‘Convention for the Protection of Individuals’, Article 2(a).

relatively narrow and atomistic, conception of privacy. However, if the concerns associated with group privacy are viewed through the lens of public interest, then they may be given definition and traction even within the scope of a data protection instrument like the GDPR. The term ‘the public interest’ appears in the GDPR no fewer than seventy times. It has a particular significance in the context of health research. This is an area, such as criminal investigation, where the public interest has always been protected.

Our argument is that it is through the application of the public interest test to health research governance in data protection law, that there is an opportunity to recognise in part common interests in group privacy. For example, any processing of personal data within material and territorial scope of the GDPR requires a lawful basis. Among the legal bases most likely to be applicable to the processing of personal data for research purposes is either that the processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller (Article 6(1)(e)), or, that it is necessary for the purposes of the legitimate interests pursued by the controller (Article 6(1)(f)). In the United Kingdom (UK), where universities are considered to be public authorities, universities are unable to rely upon ‘legitimate interests’ as a basis for lawful processing. Much health research in the UK will thus be carried out on the basis that it is necessary for the performance of a task in the public interest. Official guidance issued in the UK is that the organisations relying upon the necessity of processing to carry out a task ‘in the public interest’

should document their justification for this, by reference to their public research purpose as established by statute or University Charter.<sup>30</sup>

Mere assertion that a particular processing operation is consistent with an organisation’s public research purpose will provide relatively scant assurance that the operation is necessary for the performance of a task in the public interest. More substantial justification would document justification relevant to particular processing operations. Where research proposals are considered by institutional review boards, such as university or NHS ethics committees, then independent consideration by such bodies of the public interest in the processing operation would provide the rationale. We suggest this provides an opportunity for group privacy concerns to be drawn into consideration. They might also form part of any privacy impact assessment carried out by the organisation. What is more, for the sake of legitimacy, any interference with group interests, or risk of harm to members of a group or to the collective interests of the group as a whole, should be subject to the test that members of the group be offered *reasons to accept* the processing as appropriate.<sup>31</sup> Such a requirement might support good practice in consumer engagement prior to the roll out of major data initiatives.

Admittedly, while this may provide opportunity to bring group privacy concerns into consideration where processing is carried out by a public authority (and the legal basis of processing is performance of a task carried out in the public interest), this only provides limited penetration of group privacy concerns into the regulatory framework. It would not, for example, apply where processing was in pursuit of legitimate interests or another lawful basis. There are other limited opportunities to bring group privacy concerns into the field of vision of data protection law

<sup>30</sup> Health Research Authority, ‘Legal Basis for Processing Data’, (NHS Health Research Authority, 2018). [www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/legal-basis-processing-data/](http://www.hra.nhs.uk/planning-and-improving-research/policies-standards-legislation/data-protection-and-information-governance/gdpr-detailed-guidance/legal-basis-processing-data/).

<sup>31</sup> M. J. Taylor and T. Whitton, ‘Public Interest, Health Research and Data Protection Law: Establishing a Legitimate Trade-Off between Individual Control and Research Access of Health Data,’ (2020) *Laws*, 9(6), 1–24, 17–19; J. Rawls, *The Law of Peoples* (Harvard University Press, 1999), pp. 129–180.

through the lens of public interest.<sup>32</sup> However, for as long as the gravitational orbit of the law is around the concept of ‘personal data’, the chances to recognise group privacy interests are likely to be limited and peripheral. By contrast, more fundamental reform may be possible in the law of confidence.

#### 24.4.2 *Duty of Confidence*

As with data protection and privacy,<sup>33</sup> there is an important distinction to be made between privacy and confidentiality. However, the UK has successfully defended its ability to protect the right to respect for private and family life, as recognised by Article 8 of the European Convention on Human Rights (ECHR), by pointing to the possibility of an action for breach of confidence.<sup>34</sup> It has long been recognised that the law’s protection of confidence is grounded in the public interest<sup>35</sup> but, as Lord Justice Briggs noted in *R (W,X,Y and Z) v. Secretary of State for Health* (2015),

the common law right to privacy and confidentiality is not absolute. English common law recognises the need for a balancing between this right and other competing rights and interests.<sup>36</sup>

The argument put forward here is consistent with the idea that the protection of privacy and other competing rights and interests, such as those associated with health research, are each in the public interest. The argument here is that *when* considering the appropriate balance or trade-off between different aspects of the public interest, then a broader view of privacy protection than has hitherto been taken by English law is necessary to protect the legitimacy of decision-making. Such judicial innovation is possible.

The law of confidence has already evolved considerably over the past twenty or so years. Since the *Human Rights Act 1998*<sup>37</sup> came into force in 2000, the development of the common law has been in harmony with Articles 8 and 10 of the ECHR.<sup>38</sup> As a result, as Lord Hoffmann put it,

What human rights law has done is to identify private information as something worth protecting as an aspect of human autonomy and dignity.<sup>39</sup>

Protecting private information as an aspect of *individual* human autonomy and dignity might signal a shift toward the kind of narrow and atomistic conception of privacy associated with data protection law. This would be as unnecessary as it would be unfortunate. In relation to the idea of privacy, the European Court of Human Rights has itself said that

The Court does not consider it possible or necessary to attempt an exhaustive definition of the notion of ‘private life’ . . . Respect for private life must also comprise to a certain degree the right to establish and develop relationships with other human beings.<sup>40</sup>

<sup>32</sup> E.g. The conception of public interest proposed in this chapter would allow concerns associated with processing in a third country, or an international organisation, to be taken into consideration where associated with issues of group privacy. Article 49(5) of the General Data Protection Regulation, Regulation (EU) 2016/679, OJ L 119, 4 May 2016.

<sup>33</sup> Although data protection law seeks to protect fundamental rights and freedoms, in particular the right to respect for a private life, without collapsing the concepts of data protection and privacy.

<sup>34</sup> *Earl Spencer v. United Kingdom* [1998] 25 EHRR CD 105.

<sup>35</sup> *W v. Egdell* [1993] 1 All ER 835. Ch. 359.

<sup>36</sup> *R (W, X, Y and Z) v. Secretary of State for Health* [2015] EWCA Civ 1034, [48].

<sup>37</sup> *Campbell v. MGN Ltd* [2004] UKHL 22, [2004] ALL ER (D) 67 (May), *per* Lord Nicholls [11].

<sup>38</sup> *Ibid.* [14].

<sup>39</sup> *Ibid.* [50].

<sup>40</sup> *Niemietz v. Germany* [1992] 13710/88 [20].

It remains open to the courts to recognise that the implications of group privacy concerns have a bearing on an individual's ability to establish and develop relations with other human beings. Respect for human autonomy and dignity may yet serve as a springboard toward a recognition by the law of confidence that data processing impacts upon the conditions under which we live social (not atomistic) lives and our ability to establish and develop relationships as members of groups. After all, human rights are due to members of a group and their protection has always been motivated by group concerns.<sup>41</sup>

One of us has argued elsewhere that English Law took a wrong turn when *R (Source Informatics) v. Department of Health*<sup>42</sup> was taken to be authority for the proposition that a duty of confidence cannot be breached through the disclosure of non-identifiable data. It is possible that the ratio in *Source Informatics* may yet be re-interpreted and recognised to be consistent with a claim that legal duties may be engaged through use and disclosure of non-identifiable data.<sup>43</sup> In some ways, this would simply be to return to the roots of the legal protection of privacy. In her book *The Right to Privacy*, Megan Richardson traces the origins and influence of the ideas underpinning the legal right to privacy. As she remarks, 'the right from the beginning has been drawn on to serve the rights and interests of minority groups'.<sup>44</sup> Richardson recognises that, even in those cases where an individual was the putative focus of any action or argument,

Once we start to delve deeper, we often discover a subterranean network of families, friends and other associates whose interests and concerns were inexorably tied up with those of the main protagonist.<sup>45</sup>

As a result, it has always been the case that the right to privacy has 'broader social and cultural dimensions, serving the rights and interests of groups, communities and potentially even the public at large'.<sup>46</sup> It would be a shame if, at a time when we may need it most, the duty of confidence would deny its own potential to protect reasonable expectations in the use and disclosure of information simply because misuse had the potential to impact more than one identifiable individual.

## 24.5 CONCLUSION

The argument has been founded on the claim that a commitment to the protection of common interests in privacy and the product of health research, if placed alongside the commonly held value in individuals as free and equal persons, may establish a platform upon which one can construct a substantive idea of the public interest. If correct, then it is important to a proper calculation of the public interest to understand the breadth of privacy interests that need to be accounted for if we are to avoid subjugating the public to governance, and a trade-off between competing interests, that they have no reason to accept.

<sup>41</sup> Regan, 'Legislating Privacy', p. 8.

<sup>42</sup> [1999] EWCA Civ 3011.

<sup>43</sup> M. J. Taylor, '*R (ex p. Source Informatics) v. Department of Health* [1999]' in J. Herring and J. Wall (eds), *Landmark Cases in Medical Law* (Oxford: Hart, 2015), pp. 175–192; D. Beyleveld, 'Conceptualising Privacy in Relation to Medical Research Values' in S. A. M. MacLean (ed.), *First Do No Harm* (Farnham, UK: Ashgate, 2006), p. 151. It is interesting to consider how English Law may have something to learn in this respect from the Australian courts e.g. *Foster v. Mountford* (1976) 14 ALR 71.

<sup>44</sup> M. Richardson, *The Right to Privacy* (Cambridge University Press, 2017), p. 120.

<sup>45</sup> *Ibid.*, p. 122.

<sup>46</sup> *Ibid.*, p. 119.



Enabling access to the data necessary for health research is in the public interest. So is the protection of group privacy. Recognising this point of connection can help guide decision-making where there *is* some kind of conflict or tension. The public interest can provide a common, commensurate framing. When this framing has a normative dimension, then this grounds the claim that the full range of common interests ought to be brought into view and weighed in the balance. One must capture all interests valued by the affected public, whether individual or common in nature, to offer them a reason to accept a particular trade-off between privacy and the public interest in health research. To do otherwise is to get the balance of governance wrong and compromise its social legitimacy.

That full range of common interests must include interests in group data. An understanding of what the public interest requires in a particular situation is short-sighted if this is not brought into view. An implication is that group interests must be taken into account within an interpretation and application of public interest in data protection law. Data controllers should be accountable for addressing group privacy interests in any public interest claim. With respect to the law of confidence, there is scope for even more significant reform. If the legitimacy of the governance framework, applicable to health data, is to be assured into the future, then it needs to be able to see – so that it might protect – reasonable expectations in data relating to groups of persons and not just identifiable individuals. Anything else will be a myopic failure to protect some of the most sensitive data about people simply on the grounds that misuse does not affect a sole individual but multiple individuals simultaneously. That is not a governance model that we have any reason to accept and we have the concept of public interest at our disposal to correct our vision and bring the full range of relevant interests into view.