Protecting Informational Privacy in Cyberspace: Exploring Complementary Routes

JEANNE PIA MIFSUD BONNICI*


1. INTRODUCTION

Protecting informational privacy in cyberspace is difficult. The technical infrastructure makes it remarkably easy to collect and use personal information1, while there are few incentives in favour of the respect of privacy over use of personal information for commercial purposes. The Internet and other technologies have created new opportunities for providers of service to collect personal information easily, amass large databases of personal information and capitalize on the personal information for commercial purposes. Our very presence on the Internet leaves valuable traces that internet service providers, search engines, providers of social network sites, credit card companies, web shops etc. can exploit at times with our consent or our connivance or at times surreptitiously without caring to consider our possible opposition. These providers (and users/merchants) of personal information have become a primary threat for users’ privacy, at the same time that the services they offer are simultaneously growingly indispensable for many users. More than 90% of Internet users in Europe have registered anxiety over abuse of personal information online2. Governments too, may be a threat to user privacy in the delivery of e-government services and the centralisation of personal information.

* The Author is Associate Professor and Rosalind Franklin Fellow, University of Groningen, The Netherlands.

To date, states have sought to protect (the fundamental right of) privacy by specific personal data protection legislation and by encouraging businesses to adopt privacy policies and practices to protect consumer/user privacy. These approaches have limited effects, leaving consumers often without any protection or remedies against abusive use of their personal information. While in case of government traditional safeguards provided from fundamental human rights enforcement mechanisms are also available – there is still an option to sue governments for breaches of fundamental rights as judgements of the European Court of Human Rights show – the responsibility of private companies for breaches of informational privacy is still being worked out.

This paper reflects on the role that data protection legislation (namely as implemented in European Member States following Directive 95/46/EC and other later directives) has in the protection of informational privacy online. It looks at two specific scenarios: possible remedies where personal information has been negligently lost or stolen; and possible safeguards or remedies available when two or more private information-rich businesses merge or are taken-over online. In each scenario, it explores possible approaches that can be used to complement the current systems of protection of personal information. The paper explores two potentially complementary approaches:

The first approach is embedded in current theories of public international law arguing for private sector fundamental rights responsibility. In this part of the paper the author explores the usefulness of using developments in public international law on private sector responsibility for breaches of fundamental rights – e.g. in the case of breach of property rights or environmental rights – and the shifting of liability of private sector liability to states in cases of breaches of fundamental rights – e.g. where the state takes responsibility for breaches (of e.g. environmental protection) carried out by private companies established in its territory.

The second approach is a market-based approach using competition policy mechanisms to protect informational privacy. Traditionally, privacy law and competition law have been considered to be two separate and

---

3 Protected by Article 8 of the European Convention of Human Rights.
independent areas of law with very little (if at all) in common. Recent developments\(^4\) in the United States and Europe suggest that perhaps there is more in common between these two areas of law than first thought. This paper will describe and explain these developments.

2. INFORMATIONAL PRIVACY

Before examining the legal protection offered or that can potentially be offered to consumers to protect their personal information, it is important to define what is meant by the phrase ‘informational privacy’ in this paper. Three aspects of informational privacy, loosely based on Roessler’s list in ‘New Ways of Thinking about Privacy’\(^5\), will be considered here.

The first element, based on the US concept of ‘right to be left alone’, finds that “information about a person is worthy of protection even when it involves something that occurs in public”\(^6\). In a European context, this element of informational privacy is often protected in press laws. The European Court of Human Rights has also had the opportunity to elaborate on the remits of this aspect of informational privacy in amongst other Von Hannover v. Germany\(^7\). It has considered that the absence of a remedy in relation to the publication of information relating to private affairs may constitute a lack of respect for private life. In Von Hannover v. Germany the Court acknowledged that, despite being very well known, there was no doubt that the publication by various magazines of photographs of the applicant in her daily life fell within the scope of her private life and warranted protection\(^8\).

The second element of ‘informational privacy’ relates to autonomy – the ability to control what personal information is made public and what

---

\(^4\) In particular following the Google-DoubleClick merger in 2007.


\(^6\) Ibid., p. 704.


personal information is kept private. This aspect – informational self-determination – is to some extent protected (in Europe) by data protection legislation.

The third element of ‘informational privacy’ relates to situations of abuse following from the mass collection and processing of personal information. This third aspect can cover both misuse of personal information by the state and by the private sector. It is this third aspect of informational privacy that will be given most attention in this paper.

3. DATA PROTECTION LAW

Data protection legislation provides (in different ways and different extents) for the three aspects of informational privacy just described. In Europe primarily, data protection legislation is based on a fundamental right to live one’s private life without unnecessary interference identified in the Universal Declaration of Human Rights and the European Convention of Human Rights (ECHR). Since the 1980s, the right to private life (envisaged in Art. 8 ECHR) has been extended to cover protection of personal information. By 1981, well ahead of the commercial introduction of the Internet, the Council of Europe had opened for signatory Convention 108 – the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data – for its Member States. The main principles found in Convention 108 were later taken up by the European Union, in its Directive 95/46/EC on the protection of individuals with regard to the processing of personal data. This Directive, was agreed on in 1995 (at the start of the commercial Internet era) came into force by 1998 (at the start of the first major growth of the Internet) and is still in force today. The developments in (tele)communications technology and the use of personal data information in the offering of services are covered by another Directive – Directive 2002/58 on Privacy and Electronic Communications – introduced after the 2000, ‘.com’ fall out.

The approach taken to the protection of personal information (in Europe) can be described as a ‘fundamental rights approach’ where what
is protected is not the information itself but the individual (and his/her right to a private life). Protection of personal information in data protection is based not on ownership of the personal information but on the fact that that personal information identifies the data subject. The protection attached to personal information has since 2000 been included as a separate fundamental right in the Charter of Fundamental Rights of the European Union10.

Directive 95/46/EC establishes some fundamental principles in accordance with which personal data can be collected, processed and kept. It also gives some powers to a data subject to access, seek rectification or deletion of inaccurate or no longer appropriate information. Directive 2002/58 complements Directive 95/46/EC and applies to areas not specifically identified in Directive 95/46/EC such as treatment of traffic data, spam, cookies and confidentiality of information. This paper will not proceed with a detailed review of what these two Directives protect, instead it will focus on two scenarios of possible abuse following from the mass collection and processing of personal information where, it is argued here, the Directives do not provide enough protection.

Before proceeding with the scenarios, it is important to keep in mind that in the US the position is somewhat different as there is no comprehensive privacy protection. Direct legislation to protect personal information has been sporadic and sectoral. Information privacy is protected only through an amalgam of narrowly targeted rules11. Instead the approach has been one that relies on market self-regulation, that is, protection of personal information privacy is dependent on businesses introducing self-imposed rules identifying fair information practices. To a

10 Article 8 – Charter of Fundamental Rights of the European Union.
Article 8 - Protection of personal data 1. Everyone has the right to the protection of personal data concerning him or her. 2. Such 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. 3. Compliance with these rules shall be subject to control by an independent authority.

large extent, the market has had few incentives to self-regulate. In practice there are many significant gaps in protection and few clear remedies for violations of fair information practices.

4. SCENARIO 1: NEGLIGENT LOSS OR THEFT OF PERSONAL INFORMATION

The first situation to be considered here is the following: The increased ease in collecting personal information (on the Internet or through other media) seems to have led to increased occasions of negligent loss or theft of personal information stored on moveable storage systems. An informal track of personal data losses in the Europe and the US in the past three years\(^\text{12}\) shows that millions of personal records have been lost, misplaced or stolen in often the most mundane of situations—a laptop with stored personal information of employees/clients etc. stolen when left unattended in a car; storage media left on trains; a cd with personal information (including bank records, social security numbers and other important personal identifiers) lost in the mail; banks’ or shops’ client information systems hacked and so on.

The Data Protection Directive and the national laws implementing it all impose an obligation on the data controller to keep the personal information collected and processed in a secure manner\(^\text{13}\) and “to implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction, accidental loss”\(^\text{14}\).

While all the national legislations include this obligation, there are a number of limitations to the effectiveness of this obligation. One major limitation lies with the reduced or limited powers of Data Protection authorities to enforce this obligation and impose sanctions when this obligation is breached. For a wide variety of reasons, some Member States have chosen to give their data protection authorities very limited powers to police the implementation of the data protection obliga-

---


\(^{13}\) Art 17 - Data Protection Directive.

\(^{14}\) Art 17(1) - Data Protection Directive.
While the data protection authorities in some countries, like Italy, have relatively wide powers to inspect premises where personal information is kept by companies, in other countries such as the UK, the Information Commissioner was effectively barred from spot-checks of either the public or the private sectors. His officers could only inspect premises and records after giving advance warning and with the agreement of the civil servants or companies concerned.

A related limitation to inadequate enforcement is the absence of real sanctions for breaches of the obligations of this article. Data protection authorities have limited sanctions that they can apply after investigating breaches. Proper sanctions can work as incentive for data controllers (and employees within a company) to take the obligations of article 17 seriously.

The Data Protection directive (in article 23) requires that Member States provide a way for persons “who have suffered damage as a result of an unlawful processing operation or of any act incompatible” with the Directive to be entitled to compensation from the controller for the damage suffered. In many national legislations, individual citizens may bring a claim of compensation under general private (or civil) law provisions. Had a citizen to take such action however, the burden of proof for the damage caused by a negligent loss of a company would lie with the citizen – a burden, one may argue, that is disproportionately large.

While arguing for necessary changes to be made to the power of data protection authorities, we may also consider whether there are complementary courses of action can be followed in such cases. In this part of the paper the author explores the usefulness of using developments in

---

15 Bignami argues that “compared to other areas of European law, the Data Protection Directive gives surprisingly few powers to the European network of privacy regulators; the bargaining history [she claims] shows that this decision was driven by extreme disagreement on the importance of privacy.” F. BIGNAMI, Transgovernmental Networks vs. Democracy: The Case of the European Information Privacy Network, in “Michigan Journal of International Law”, Vol. 26, 2005, p. 810.

16 J. CANNATACI, J.P. MIFSUD BONNICI, op. cit.

17 Article 23 - Data Protection Directive.

18 See for example Article 46 of the Maltese Data Protection Act (Chapter 440 of the Laws of Malta).
public international law on private sector responsibility for breaches of fundamental rights – e.g. in the case of breach of property rights or environmental rights – and the shifting of liability of private sector liability to states in cases of breaches of fundamental rights – e.g. where the state takes responsibility for breaches (of e.g. environmental protection) carried out by private companies established in its territory.

4.1. Responsibility of Non-state Actors for Human Rights Violations

There is a growing literature on the responsibility of states and non-state actors in violations of human rights. Traditionally the responsibility for the protection of human rights lies with states. States have the responsibility to provide the necessary environment and laws for the protection of human rights within a state and for relevant sanction where human rights are violated. Citizens can bring actions against the state where the state alleged violates the citizens’ human rights. Courts have, in most European courts reviewed actions of governments for human rights violations and citizens in Europe can, once local remedies are exhausted, bring their claims before the European Court of Human Rights. What this in fact means for our debate on protection of informational privacy, is that violations by a state or parastatal organisations of informational privacy may be brought before a court and citizens may be compensated (and/or laws changed) if the court finds for the citizen bringing the action. Numerous allegations of the violation of the right to non-infringement of one’s private and family life (including protection for informational privacy) have been brought before the European Court of Human Rights.

While the responsibility of states for their own actions is often clear, it is not clear whether private corporate entities have enforceable obligations to protect human rights and whether states are also responsible for the actions of private corporate entities established in its territory. It is


20 E.g. Hannover v. Germany; S and Marper v. UK etc.
increasingly argued, e.g. in the environmental field, that private companies can be directly held responsible for violations of human rights (e.g. the right to property). As a response to this devolution of responsibility of human rights violations to the private sector, the private sector has in many areas developed codes of practice or standards of practices delimiting their responsibility. Steinhardt argues that “one dominant critique of the corporate responsibility initiative suggests that it subverts shareholder primacy by requiring management to develop an expertise in human rights law and exercise de facto control over abuses …raising costs without raising revenues”22. Yet one can also argue that human rights are rights that every human being has erga omnes and not solely against his own State or another state, as guarantors of an environment of human rights’ protection. No person should be allowed with impunity to breach the fundamental human rights of others.

Unlike other areas, as noted earlier, where private companies have taken what has been called an “entrepreneurial approach to human rights”23 and have identified their human rights obligations as an industry and adopted these obligations in the standard business practices, this has not yet happened for the protection of informational privacy. Even if most businesses active online have privacy policies, none of these policies contain any provision on the remedies available to individuals if personal information kept by the company is accidentally or negligently lost or stolen.

Apart from waiting for business to take an entrepreneurial approach to human rights, one could also argue that businesses can also be held responsible for human rights violations. It has also been argued that human rights obligations are not different in kind from other sources of obligation in trade law24. In support of this argument is that any business can be held liable for damages caused by the negligence or intentional acts of its employees. Following this logic, negligent acts or intentional acts that violate human rights obligations should not be treated any differently.

21 See Code of practice for diamonds - Kimberly Process Certification Scheme; for forestry etc.
It is legally more difficult however to claim that citizens can bring an action for damages caused by a violation of their right to informational privacy based not on data protection law but directly on the basis of fundamental rights. The question here is, are Article 8 ECHR and Articles 7 (protecting the right to private life) and 8 (protecting the right to data protection) Charter of Fundamental Rights of the European Union justiciable against private parties? Arguably (given the novelty (post coming into force of the Lisbon Treaty in December 2009)) one will first need to answer the question whether Articles 7 and 8 of the Charter of Fundamental Rights of the EU have direct effect vertically against the action of states and horizontally against the action of private actors. Following Article 6 TEU the Charter of Fundamental Rights has “the same legal value as the Treaties” and is addressed “to the Member States only when they are implementing Union law”\textsuperscript{25}. This does not however mean that each of the fundamental rights is directly effective.

In case of Treaty provisions, the ECJ has held in \textit{Van Gend en Loos} (and developed further in subsequent decisions such as \textit{Van Duyn} and \textit{Defrenne}) that “a Treaty Article will be accorded direct effect provided that it is intended to confer rights on individuals and that it is sufficiently clear, precise and unconditional”\textsuperscript{26}. Whether Articles 7 and 8 satisfy these criteria is yet to be decided.

4.2. State Responsibility in Case of Non-state Actor Violation of Human Rights

Contemporaneously, there is a tendency to consider states also liable for violation of human rights by companies established in their territory. What is argued here is that states have the ultimate responsibility to protect human rights and cannot relinquish their responsibility when the violations are committed by a private company established within its territory.

What are the implications of this trend for the protection of informational privacy in cyberspace? Within this second approach – holding states

\textsuperscript{25} Article 51(1) Charter of Fundamental Rights of the European Union OJ 2010/C 83/02.

responsible for human rights violations committed by private companies – this could in practice mean that citizens’ can bring human rights actions against the state when a private company would have in any way (negligent loss, theft, mishandling) misused the private information it held.

One important aspect not discussed so far is the question of jurisdiction. Collection of personal information on the Internet is, to many extents, borderless or not specifically bound to one geographical space. If one were to take as an example the social network Facebook with more than half a million users, the personal information collected from and about those users is no bound to one geographical territory. Where would a user bring an action to remedy a human rights violation? Which state can be held responsible for the breach of informational privacy by Facebook? Are the ‘traditional’ of jurisdiction – e.g. territorial or personal link between the dispute and the jurisdiction of the court – enough? And what law should apply? Given the universality of human rights one would argue that the choice of law problem should not arise here.

However, given that the right to informational privacy is only unambiguously identified as a fundamental right in the EU Charter of Fundamental Rights, the universal aspect of the human right might come into question. There is a possibility that state courts take a parochial approach, preferring a narrow interpretation of jurisdiction, preferring their own jurisdiction over possibly the jurisdiction of other courts and preferring their restrictive interpretation on the possibilities of holding states and private actors liable for human rights violations. This uncertainty on jurisdiction acts against citizens as it offers no clear route to avail themselves of possible (possibly also undetermined) remedies.

5. Scenario 2: Mergers and Acquisitions

The second situation to be considered here is the following: similar to business enterprises active off-line, businesses online often merge or are bought-off by other businesses. In these business transactions personal information of clients or employees etc. coming from the different businesses are also merged. Combining already large collections of personal information in a reality where so much can be done with the personal information can be considered to be another threat to personal informational privacy unless appropriate safeguards are in place.
In the current data protection legislation structure there is no method to forestall situations or impose specific protections where a commercial entity in the course of its transactions with other commercial entities (e.g. during a merger or take-over) increases its store of consumer personal data. The urgency of adequate protection of consumer information becomes even more acute when two online companies merge giving one company exceptionally wide access to consumer information, as in the Google-DoubleClick merger in 2007 where it was argued that the acquisition of DoubleClick would permit Google to have more information about the Internet activities of consumers than any other company in the world. Data protection legislation would need to be followed after the merger but there is no means in the legislation to impose specific safeguards to ensure that the personal information would not be exploited in a way to threaten consumer privacy.

Under fair competition/antitrust rules, a merger can be reviewed by the EU Commission in Europe and the Federal Trade Commission (FTC) in the United States to establish whether the merger could potentially constitute unfair and deceptive trade practices. Could one of the review criteria be the potential threats of privacy by the concentration of too much consumer information in the control of one corporate entity?

There is a growing trend (seen particularly in the US) to attempt to include privacy concerns in anti-trust/unfair competition proceedings. Indeed in 2007, the Google-DoubleClick merger was challenged by a number of organisations in the US on privacy and antitrust grounds.

---


28 One can argue that if information has been supplied to a particular company on trust and for the purposes informed of at the moment of collection, it would not only be a major breach of trust if that information is passed to another but also a breach of data protection obligations (to process and keep personal information only for specified purposes).


30 The Electronic Privacy Information Center (EPIC) file a complaint on 20 April 2007 with the Federal Trade Commission requesting the FTC to (a) issue an injunction to prevent
Access to personal information of consumers was also one of the concerns investigated by the EU Commission in the proceedings examining whether the merger would significantly impede fair competition. Both the US Federal Trade Commission and the EU Commission eventually found that there was no situation of distortion of competition by the merger and authorised the merger to proceed. This notwithstanding, this case (and others) has given rise to increased awareness of the possibility of using competition (and anti-trust) principles to protect individuals’ informational privacy. One can question however whether competition and anti-trust principles are in fact appropriate mechanisms to be used in the protection of consumer personal information privacy.

5.1. Personal Information as a Commercial Asset

As pointed out in the beginning of this paper thanks to the advances in information technology it is relatively easy and cheap for companies to amass personal consumer information. Thinking in market terms, the ease with which personal consumer information can be collected produces a steady supply of personal information which is taken up by companies that increasingly consider large data sets of consumer information as essential assets for companies trading online. By using consumer information, companies can tailor their goods and services to match the preferences and dislikes of the market. One can expect that a company with a wide and large data set of consumer information can have a competitive edge over other competitors who may have lesser stores of personal data. Having large sets of personal information could also be exploited in a way that threatens consumers’ privacy.

the merger and (b) to conduct an investigation regarding the circumstances of the merger. The complaint alleged that “the acquisition of DoubleClick will permit Google to track both a person’s Internet searches and a person’s web site visit...giving one company access to more information about the Internet activities of consumers than any other company in the world. Moreover, Google will operate with virtually no legal obligation to ensure that privacy, security and accuracy of the personal data that it collects”, available at http://www.epic.org/privacy/ftc/google/epic_complaint.pdf.

The personal information market is not quite as perfect as it seems with supply and demand keeping each other in check. The market is not transparent: the original supplier of the person information (the data subject) has little or no control over the use of the personal information supplied. Data protection legislation in Europe tries to address this lack of transparency by requiring consent of the data subject and that the data subject is informed of the purpose of collection and use of the personal information. Theoretically at least, the giving of information allows the data subject/consumer to then make informed choices about the use of his/her personal information. As in other areas of consumer law, where the notion of informed consumer is central, there are limits to the effectiveness of this obligation as a remedy against abusive use of personal information. One could argue that companies in a leading position in the market may potentially afford to ignore traditional privacy safeguards (where they exist at all). The difference between companies abiding with data protection or other privacy legislation and those which do not can also result in the non-abiders having a competitive edge on competitors following the more onerous obligations of privacy protection. Data protection legislation does not provide remedies to balance the inequality between abiders and non-abiders with the laws. Furthermore, where the reach of European data protection law does not reach (or is ignored), the consumer is left in an even more vulnerable position with his/her personal information being traded while he/she has little power over the use of personal information.

There is a growing school of thought that law should grant the data subject/consumer a property right in their own personal data and be

---


allowed to negotiate with business which personal data to reveal to which firms for what purposes and for what price. This approach assumes a move towards a market-based approach rather than a fundamental rights approach which has so far dominated European thinking. While a property rights model has some appeal in (theoretically at least empowering the consumer), it is hard so far to imagine its viability in practice and its prospect of achieving information privacy goals34.

5.2. Competition Law

The regulation of mergers between business entities falls under a different area of law to privacy law: competition law (or antitrust law in the US). Prima facie, the aims of competition law have little in common with (if not antithetical to) the concerns privacy law seeks to address. In essence competition law has three elements: a. prohibiting agreements or practices that restrict free trading and competition between business entities; b. prohibiting abusive behaviour by an entity dominating a market or practices that tend to lead to a dominant position; and c. supervision of mergers and acquisitions of entities. The main enforcement entity for fair competition/antitrust rules at a European level is the EU Commission and the Federal Trade Commission (FTC) is the equivalent entity in the United States.

In theory, by applying competition policy ensuring that companies compete with each other in a free and fair manner while offering their goods and services, consumers are also being offered better services and goods. It is often argued35 that the end beneficiary of fair market rules is the consumer (even if the rules as such do not mention consumers or consumer protection).

Given that consumer protection is a goal shared by both privacy law and competition policy, and given the evident commercial value of personal information in today’s online trading businesses, there is a growing

34 See SAMUELSON, op. cit. p. 1125 for an eloquent discussion on the viability and difficulties of such a system.
trend (seen particularly in the US) to attempt to include privacy concerns in anti-trust/unfair competition proceedings. There is yet no comprehensive research identifying the role competition policy mechanisms can play (if at all) in the protection of personal informational privacy.

On the one hand it can be argued that competition policy mechanisms play no role in the protection personal informational privacy simply because competition policy is geared towards the regulation of economic factors and not non-economic factors like privacy protection. This position can be defended through economics-based competition analysis, inspired by the so-called “Chicago School” of competition theory that shows that “non-economic” factors, including privacy protection, are best dealt with by legislation and not by competition policy.

On the other hand, it can also be argued that since there is a market for personal information, personal privacy should be framed in market terms and no longer, solely, from a fundamental rights perspective. Following then a market-driven approach to privacy protection, one could argue that privacy protection is so fundamental that there should be an obligation to integrate privacy protection in all regulation and policies, including competition policy.

What one can definitely see however, from the handling of the Google-DoubleClick merger examination, is that while competition policy has mechanisms that can be used to protect personal privacy, integrating privacy matters in the current competition law enforcement structure will need some institutional and cultural changes to happen.

Despite the length of time to instigate and wait for the necessary changes to happen, it is important that interested organisations or individuals continue to challenge mergers and acquisitions of companies having access to broad collections of personal information. The mere process of asking for review can achieve safeguards that consumers would not have otherwise had. An example of this can be seen in the

---


37 See E. Edwards, op. cit.
DoubleClick-Abacus Direct acquisition in 2000. When DoubleClick (an Internet advertising company) purchased Abacus Direct (a market research company), the acquisition also sparked concern that consumer privacy may also be harmed by the transaction. Ultimately, a consent decree maintaining the separation between the consumer databases was awarded, securing to some degree consumers’ informational privacy\textsuperscript{38}.

6. CONCLUSION

In a world where online providers seek to convince their customers that ‘privacy is dead’ in an attempt to enjoy \textit{carte blanche} over the personal information they collect, discussing safeguards and remedies for informational privacy takes on a renewed appeal. It is important for consumers to appreciate that there are viable mechanisms that can be invoked to protect one’s personal information.

With “private enterprises now controll[ing] more powerful resources of information technology than ever before”\textsuperscript{39} is it important to review the current legal framework protecting informational privacy. This paper has looked at two specific scenarios where consumers’ rights to information privacy may be violated, considering the limits of the current data protection legislation and the possibility of using other fields of law to complement the current framework of protection.

In the first scenario – involving situations of possible negligent loss or theft of personal information – one can see that while the current legal framework (set by Directive 95/46/EC) sets an obligation for data controllers to use appropriate mechanisms and institutional setups to secure personal information, the law stops short from giving the data protection enforcement authorities enough power to ensure compliance with the obligation by data controllers. While a first recommendation is to encourage necessary changes to the law, the paper also explored other


possible remedies for consumers. It looked at the responsibility of non-
state actors for the violation of human rights and state responsibility for
non-state actor violations. The routes offered basing one’s claims on the
direct responsibility of non-state actors for violations of information pri-
vacy or of claiming state responsibility for non-state actor violations may
exist but still need to be tested before a court of law.

In the second scenario – involving mergers and acquisitions of com-
panies holding large collections of personal information – the route
explored in this paper, of using FTC and EU Commission anti-trust
scrutiny mechanisms, has already been used in practice. Although the cur-
rent outcomes have been limited, it is, highly unlikely that these mecha-
nisms are not used again in future mergers of key industry players. As
Edwards argues “despite the view of traditional analysts and observers,
the FTC [and the EU Commission] has the authority to analyze data pri-
vacy issues, where appropriate, as part of its merger review”40. It is a mat-
ter of more detailed study, as well as persuading the FTC and EU
Commission, and then mustering the political will to provide for better
protection of informational privacy.

Ultimately what this article aims to show is that consumers can ben-
efit from better data protection legislation safeguards complemented by
developments going in linking human rights violations by the private sec-
tor to states and to the experimental field of using competition law struc-
tures to protect citizens’ informational privacy online.

40 E. EDWARDS, op. cit.