Principles-based regulation of personal data: the case of 'fair processing'

Winston J. Maxwell*

Key Points

- This article reviews the concept of fair processing under US and EU laws, highlighting the Federal Trade Commission's cost–benefit analysis and comparing it with the European approach.
- The article examines how 'fairness' in the privacy field would be approached from a law and economics standpoint, highlighting the difficulties of conducting cost–benefit analyses of privacy risks.
- The article concludes with a discussion of the advantages of 'principles-based' regulation versus 'rules-based' regulation and suggests a methodology of regulatory restraint that should be applied by policymakers before enacting detailed privacy rules to deal with digital privacy threats. The methodology is inspired by the existing EU framework for the regulation of electronic communications.

The proposed General Data Protection Regulation[1] in Europe currently contains more than 90 articles. Some say that the proposal is too long, complex, and prescriptive.[2] One reason the proposal is so detailed is that policymakers feel that new Internet-based platforms, algorithms, and data analytics raise specific risks that require specific regulatory solutions. But is this necessarily true? To contribute to the debate on 'principles-based' versus 'rules-based' regulation, this article will examine the concept of 'fair processing', which is one of the pillars of data protection legislation in Europe and in the USA. The principle of fair processing appears in the OECD Guidelines,[3] the European Charter of Fundamental Rights,[4] the European Data Protection Directive,[5] the Council of Europe Convention on Data Protection,[6] and in Section 5 of the Federal Trade Commission (FTC) Act.[7] However, little has been written about what the 'fair processing' really means. This article will examine how the FTC and two data protection authorities in Europe approach the question of 'fairness' in data processing.

The article will then examine how fairness might be approached from a law and economics perspective, before addressing the debate on 'principles-based' versus 'rules-based' regulation.

The article will conclude by proposing that policymakers exercise caution before enacting new rules that target digital privacy risks. Digital markets can raise new challenges. Yet the nature of the challenges and the probability of consumer harm are poorly understood. Policymakers will nonetheless have a natural bias towards proposing new rules rather than relying on existing legal principles to deal with new digital risks. In dynamic markets, detailed rules often miss their mark and become quickly obsolete. By contrast, principles such as

* Winston J. Maxwell, Hogan Lovells LLP (Paris), 17 Avenue Matignon, 75008 Paris, France. Tel: 33 1 5367 4847; Fax: 33 1 5367 4748; Email: winston.maxwell@hoganlovells.com. A previous version of this paper was presented at the University of Toulouse symposium '*Quelle protection des données personnelles en Europe?*' March 2014. The author would like to thank Timothy Tobin (Hogan Lovells LLP—Washington, DC) and Mac MacMillan (Hogan Lovells International—London) for their helpful comments and assistance in the preparation of this article.

1 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), COM(2012) 11 final, 25 January 2012 (hereinafter 'Proposed General Data Protection Regulation').

2 BJ Koops, 'The Trouble with European Data Protection Law' (2014) 4 Int'l Data Privacy L 250.

3 Organisation for Economic Co-operation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2013), para. 7 ('data should be obtained by lawful and fair means').

4 Charter of Fundamental rights of the European Union (2010/C 83/02), O.J. C 83/389, 30 March 2010 (hereinafter 'European Charter'), Article 8 of which states that 'data must be processed fairly'.

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, O.J. L 281, 23 November 1995, pp. 31–50 (hereinafter 'Directive 95/46/EC'), Article 6 of which states that 'data must be processed fairly and lawfully'.

6 Council of Europe, convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, ETS n° 108, 28 January 1981 ('Convention 108'), Article 5 of which states that 'personal data. . .shall be obtained fairly and lawfully'.

7 Federal Trade Commission Act of 1914 ('FTC Act') is today codified at 15 U.S.C. §41–58, section 5 of which prohibits 'unfair or deceptive acts or practices'.

fair processing can easily adapt to new digital environments. I propose a methodology for regulatory restraint, based on the methodology used for the regulation of electronic communications in the EU. Under this methodology, the sponsor of a regulatory proposal would have to establish that there is an enduring market failure that is not likely to be addressed by technological or market evolution, and that existing law is insufficient to treat the problem. Full consideration of existing law, including the option of improving enforcement of existing law, is also required before proposing new regulatory solutions.

Application of the fair processing principle in the USA

Section 5 of the FTC Act prohibits 'unfair or deceptive acts or practices in or affecting commerce'.[8] The 'FTC' is an independent government agency whose mission is to enforce competition and consumer protection laws in the USA. The FTC has used Section 5 of the FTC Act to enforce data protection principles against a broad range of companies in the USA, including in the Internet sector. The FTC has developed what Professors Solove and Hartzog call a 'new common law of privacy'.[9] The FTC's enforcement actions, guidelines, and settlement agreements provide details on how the FTC applies the broad principles set forth in the FTC Act to particular facts. This process is similar to what courts do when adjudicating common law tort claims. By examining how claims have been dealt with in the past, observers can anticipate how a standard such as 'fairness' will be applied in the future.

Howard Beales describes how the fairness test has been applied by the FTC from 1938 to present.[10] In the 1970s, the FTC used its authority to prohibit unfair practices in a broad variety of circumstances, relying in part on broad public policy criteria. Critics—and in particular the US Congress—became concerned that the unfairness standard was too subjective. In 1980, the FTC clarified its approach by adopting its 'Unfairness Policy Statement'.[11] Congress then inserted the FTC's methodology into the FTC Act itself in 1994. The US Congress wanted to make sure that the FTC would refer to an objective methodology when evaluating 'fairness', and not rely solely on subjective public policy considerations.

8 Ibid.

9 D. Solove and W. Hartzog, 'The FTC and the New Common Law of Privacy' (2014) 114 Col. L. Rev. 583.

10 H Beales, 'The FTC's Use of Unfairness Authority: Its Rise, Fall, and Resurrection' (Federal Trade Commission Marketing and Public Policy Conference, 30 May 2003) <http://www.ftc.gov/public-statements/2003/05/ftcs-use-unfairness-authority-its-rise-fall-and-ressurection> accessed 8 July 2015.

The 1994 revision to the FTC Act states as follows:

> The Commission shall have no authority under this section or section 57a of this title to declare unlawful an act or practice on the grounds that such act or practice is unfair unless the act or practice causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition. In determining whether an act or practice is unfair, the Commission may consider established public policies as evidence to be considered with all other evidence. Such public policy considerations may not serve as a primary basis for such determination. (Underlined by the author)[12]

The FTC's fairness methodology requires that the FTC conduct a cost–benefit test. If the practice causes a substantial injury to consumers that consumers cannot reasonably avoid, and the injury is not offset by corresponding consumer benefits, then the practice will be deemed unfair. The unfairness test is separate from the FTC's analysis of whether a practice is 'deceptive'. According to Beales, a 'deceptive' practice is a subset of the larger category of 'unfair' practices.[13] Under the FTC's methodology, a deceptive practice would not require a cost–benefit analysis and would be presumed to be unfair. This is understandable because a deceptive practice is tantamount to lying to consumers, and such conduct is not likely to have any countervailing consumer benefits. The cost–benefit analysis would necessarily come out in favour of prohibiting the practice.

In the field of data protection, the FTC has used the theory of deceptive practices to sanction companies that do not honour their own privacy policies. In the case where a company has not broken any of its own promises, the FTC will not be able to punish the company for deceptive practices. The FTC will have to show that the practice is 'unfair'.

The FTC's three-step balancing test for evaluating 'unfairness'

To determine whether a practice is unfair, the FTC must first find that the practice causes or is likely to cause substantial injury to consumers. A substantial injury can result from a large injury to a small number of consumers or a small injury to a large number of consumers.

11 Federal Trade Commission (FTC), 'FTC Policy Statement on Unfairness' (17 December 1980) <http://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness> accessed 8 July 2015.

12 15 U.S.C. §45(n).

13 Beales, above, n 10.

In the field of data protection, consumer injury is often difficult to measure and has been the focus of much debate in the USA,[14] where the concept of privacy as a fundamental human right is not as ingrained as in Europe. Under the FTC unfairness test, the injury to each consumer taken individually can be extremely small. For example, the excessive collection of data may marginally increase the risk that a given consumer will fall victim to identity theft or receive unwanted advertisements. The individual injury in these situations would be difficult to quantify. Nevertheless, the FTC has stated its belief that these practices may create a substantial injury to consumers.[15] Any practice that limits a consumer's autonomy and choice may be considered to create a substantial injury. For example, a default setting in software that leads to unexpected sharing of personal computer files was held to be unfair because it hindered consumer choice.[16]

Second, the injury must also be one that cannot be reasonably avoided by consumers. This relates to the FTC's mission to ensure that consumers are sufficiently informed and have the opportunity to make choices relating to their privacy. Any hidden or unexpected collection or uses of personal data could be deemed unfair because the consumer did not have a reasonable opportunity to make a choice in the matter.

The last step in the US unfairness test requires that the FTC evaluate any countervailing benefits. This step requires that the FTC inquire whether the practice in question generates new valuable services, or lower prices, for consumers. In this connection, the FTC must compare the situation that would exist in the absence of any regulation by the FTC with the situation that would exist if the practice were stopped or regulated. The difference represents the costs associated with the FTC's own regulatory action, and conversely, the benefits associated with leaving the practice unregulated.

The FTC's unfairness test can best be understood through an example. Imagine that the FTC is considering the practice of setting third-party advertising cookies on users' computers when the users open a webpage. Is there a substantial consumer injury? There may be, because the third-party ad cookies could lead to embarrassing situations such as when a user is presented an advertisement that is related to his or her browsing history, and the user would prefer that the browsing history be kept secret. The user may also find such tracking 'creepy',[17] making the consumer less inclined to use certain Internet services in the future. The FTC could view reduced consumer trust in online transactions as a form of harm.

Can the injury be reasonably avoided by the consumer? This may depend on the level of disclosure provided to the consumer and the availability of easy-to-use tools to block the third-party advertising cookies. Finally, is the consumer injury offset by consumer benefits? This step would require the FTC to evaluate the benefits that flow to consumers from the widespread use of third-party advertising cookies. These benefits would consist principally in the wider availability of free content online, which in turn increases consumer choice and freedom of expression.[18] The FTC would have to consider the costs associated with a prohibition of third-party cookies or the imposition of a consumer opt-in mechanism. If the costs associated with these regulatory remedies exceed the costs associated with the consumer injury, then the relevant practice would not be considered unfair and should be allowed.

To date, the FTC has more readily alleged unfairness in data security-related enforcements (for example, data breaches where companies are alleged to have had unreasonable security practices that put personal information at risk of misuse) than it has in pure privacy-related enforcement actions (for example, where the issue is not security but a company's decision to share personal information or to target ads to consumers in alleged unexpected ways). Despite this, the FTC has expressed an increased willingness to utilize unfairness even for privacy enforcement.

The difficulties of conducting a cost–benefit analysis are examined in more detail in the 'Difficulties of conducting a cost–benefit analysis for data protection regulation' section of this article, and some additional discussion of the FTC's use of unfairness in practice is contained in the '"Principles-based" versus "rules-based" regulation' section.

To summarize:

- The FTC has used the concept 'unfair or deceptive practices' to regulate data privacy for many sectors of the economy in the USA.
- Through its guidelines, sanctions, and settlement agreements, the FTC has created what Professors Solove and Hartzog call a 'common law of privacy'.

14 See eg MR Calo, 'The Boundaries of Privacy Harm' (2011) 86 Indiana L. J. 1131.

15 Solove and Hartzog, above, n 9.

16 *In re Sony BMG Music Entertainment*, FTC complaint n° C-4195, 28 June 2007.

17 On the concept of 'creepy', see below, n 43 and accompanying text.

18 A Goldfarb and C Tucker, 'Privacy and Innovation', National Bureau of Economic Research Working Paper 17124, June 2011.

- What is less known is that the FTC has developed explicit guidelines on how to determine when a given practice is unfair. The process involves a balancing test in which the FTC takes into account the harm caused by the practice, the ease with which the harm can be avoided by consumers, and the benefit that the practice or new service brings to consumers.

Application of the fair processing standard in European data protection law

Article 6 of the European Data Protection Directive 95/46/EC provides that personal data must be processed 'fairly and lawfully'. The concept of fair processing is partially explained in Recital 38 of the Directive:

> (38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection.

Recital 38 links the concept of fairness to the level of information given to the data subject. This is similar to the FTC's approach, which puts emphasis on individual information and choice. If the data subject is given inadequate information, he or she is not being put in a position to exercise autonomy over his or her personal data. This absence of information will make the processing 'unfair'. Article 10 of the Data Protection Directive lists the information that must be given to the data subject and includes a catch-all provision requiring that the data controller provide '*such further information [as] is necessary, having regard to the specific circumstances in which the data are collected, to guarantee fair processing in respect of the data subject*'. Like Recital 38, Article 10 suggests that fair processing is linked to the level of information given to the data subject. This makes sense if the focus of fairness is on the data subject's ability to exercise individual autonomy with regard to his or her personal data.

The proposed General Data Protection Regulation would require that data be processed 'lawfully, fairly and in a transparent manner in relation to the data subject'.[19] The proposed regulation does not define 'fairness'. But the use of the words 'fairly' and 'in a transparent manner' in the same sentence suggests that under the proposed regulation, fairness means more than transparency.

Fairness also means more than transparency under Convention 108 and the European Convention on Human Rights. The European Union Agency for Fundamental Rights, the European Court of Human Rights, and the Council of Europe published in 2014 a handbook on European data protection law summarizing the relevant case law of the Court of Justice of the European Union and of the European Court of Human Rights in data protection matters.[20] The handbook characterizes fair processing as requiring both transparency and trust.[21] According to the handbook, the data subject should be in a position to 'really understand' what is happening to his or her data. Processing operations must not be performed in secret and should not have unforeseeable negative effects.[22] In addition, fair processing means that data controllers must on occasion go beyond minimal legal requirements:

> Fair processing also means that controllers are prepared to go beyond the mandatory legal minimum requirements of service to the data subject, should the legitimate interests of the data subject so require.[23]

Under this approach, the data controller must take into account the legitimate interests of the data subject and refrain from certain processing operations even if they are otherwise legal. Fairness thus requires the data controller to take the interests of the data subject into consideration, and not just the data controller's own interests. This interpretation of fairness also coincides with the broader definition of fairness given by the UK Information Commissioner.

For the Information Commissioner's Office (ICO) in the UK, fair and lawful processing means that the data controller must

- have legitimate grounds for collecting and using the personal data,
- not use the data in ways that have unjustified adverse effects on the individuals concerned,
- be transparent vis-à-vis the data subject as to how the data are being used,
- handle the data in ways not inconsistent with the data subject's reasonable expectations,
- not do anything unlawful with the data.[24]

19 Proposal for a General Data Protection Regulation, above, n 1, Article 5(a).

20 European Union Agency for Fundamental Rights, European Court of Human Rights, and Council of Europe, *Handbook on European Data Protection Legislation* (Publications Office of the European Union, Luxembourg, 2014) ('Handbook'), p. 75.

21 Ibid, p. 75.

22 Ibid, p. 74

23 Ibid, p. 75.

24 ICO, 'Processing Personal Data Fairly and Lawfully (Principle 1)' <https://ico.gov.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/> accessed 30 October 2014.

The second item in the ICO's list resembles the broader cost–benefit test used by the FTC. The concept of 'unjustified adverse effects' requires an assessment of what the adverse effects are and whether those adverse effects are justified by countervailing factors. The ICO's multi-criteria approach to fairness is attributable to Schedule 1 of the Data Protection Act 1998, which sets out guidance on the meaning of 'fair processing':

> In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.[25]

Schedule 1 of the Data Protection Act 1998 also links fairness to the provision of a minimum level of information to the data subjects, essentially reiterating the requirements of Article 10 of the Data Protection Directive.

The concept of fair processing was litigated before English courts in two instances. The first case involved a gas company's use of personal data for a new direct marketing purpose. The court found that the gas company's use of its customers' data was unfair because the data subject had not consented. The court found that fairness requires a balancing of interests: 'fairness, undefined in the Act, requires [the court] to weight up interests of data subjects and data users'.[26] The British Gas case was decided under the Data Protection Act 1984, which contained no definition of fair processing. As noted above, the Data Protection Act 1998 contains more explicit guidance on the 'fair processing' principle.

In the second case, *Johnson v Medical Defense Union* ('MDU'),[27] Dr Johnson was expelled from the MDU, a collective insurance scheme, because the MDU's risk assessment found that Dr Johnson was no longer an acceptable risk. This assessment was performed by MDU based on the information provided by Dr Johnson himself and by other doctors. Dr Johnson claimed that the MDU's handling of his personal data was unfair. The court found that the processing was unfair with regard to information provided by other doctors, because the MDU never gave Dr Johnson an opportunity to see the information provided by his peers and comment on that information. The court found, however, that the overall risk assessment process used by MDU, as well as MDU's use of data provided by Dr Johnson himself, was not unfair under the Data Protection Act. First, Dr Johnson was fully informed that MDU had a risk assessment programme; second, the 'fair processing' principle in the Data Protection Act is not intended to permit courts to second-guess internal procedures of this kind.

In France, the 'fair processing' principle was litigated in a case involving the French yellow pages company, *Les Pages Jaunes*. The French term for fair processing, *traitement loyal*, should not be confused with a 'duty of loyalty' under US law. A duty of loyalty under US law suggests the existence of a fiduciary duty. Under French law, the term *loyauté* is synonymous with 'fairness' in commercial dealings. In fact, as we will see below, French consumer protection law has a provision prohibiting all 'disloyal' practices (*pratiques déloyales*).

In the *Pages Jaunes* case, the French data protection authority Commission Nationale de l'Informatique et des Libertés (CNIL) sanctioned *Les Pages Jaunes* for having collected information about individuals from their public social media profiles, and aggregating that information in *Les Pages Jaunes*' online directory service. The CNIL found the processing unfair (*déloyal*) because data subjects were not sufficiently informed that their public profiles would be collected by *Les Pages Jaunes* and were not given an opportunity to grant informed consent.[28] The CNIL's finding was confirmed by the French Council of State in 2014.[29] In the French *Pages Jaunes* decision, the concept of 'fairness' seems linked to the level of information provided to the data subject.

Under French consumer protection law, an 'unfair' practice is defined as '*commercial conduct that is contrary to the requirements of professional care and that modifies, or may modify, in a significant manner the economic conduct of a consumer*'.[30] The consumer protection code further subdivides unfair practices into 'misleading' practices and 'aggressive' practices.[31] Finally, the consumer protection code prohibits 'abusive contractual clauses' that create a significant imbalance between the parties.[32] Clauses that violate France's data protection law have been held to be abusive and therefore unenforceable under France's Consumer Protection Code. The concept of abusive contractual clauses is a transposition of Directive 93/13/EEC on unfair terms in

25 Data Protection Act 1998, Schedule 1, Part 2.

26 *British Gas Trading v Data Protection Registrar*, Data Protection Tribunal (1998) DA98 3/49/2, available at <http://webarchive.nationalarchives.gov.uk/+/http:/www.dca.gov.uk/foi/bgtdec.pdf>, accessed 8 July 2015.

27 *Johnson v Medical Defence Union*, High Court of Justice, Case N° HC03C00538, 3 March 2006, affirmed, Court of Appeal [2007] EWCA Civ 262.

28 CNIL decision n° 2011-203 of 21 September 2011.

29 Conseil d'Etat, req. n° 353193, 12 March 2014.

30 Article 120-1, French Consumer Protection Code.

31 Articles 121-1 and 122-11, French Consumer Protection Code.

32 Article L 132-1, French Consumer Protection Code.

consumer contracts.[33] Directive 93/13/EEC defines as unfair any contractual provision that, contrary to good faith, causes significant imbalance in the rights and obligations of the parties. The two cumulative elements of unfairness under the Directive are 'contrary to good faith' and 'significant imbalance in the rights and obligations of the parties'.

The French panel on unfair contract clauses identified 46 types of contractual provisions that are presumed unfair in contracts for use of social media services.[34] Many of the relevant provisions identified by the panel relate to excessive or non-transparent use of data. This shows a trend that is likely to increase in Europe: that consumer protection law will increasingly supplement data protection law as a source of regulation. The approach to 'fairness' under consumer protection law is likely to influence how fairness is considered under data protection legislation.

To summarize:

- Under the current Data Protection Directive, the concept of fair processing is linked principally to transparency, i.e. the level of information given to the data subject.
- Under Convention 108 and the European Convention on Human Rights, fairness means more than just transparency. Fairness requires that the data controller go beyond what is legally required, if doing so is necessary to protect a legitimate interest of the data subject.
- The Proposed General Data Protection Regulation refers to lawful, fair, and transparent processing, again suggesting that fairness goes beyond simple transparency and requires a good faith consideration of the interests of the data subject. This is consistent with the ICO's current definition of fair processing in the UK.
- Good faith and a significant imbalance in the party's rights and obligations are key considerations when determining whether a contractual term in a consumer contract is unfair under European law. The concept of fairness under consumer protection law in Europe is increasingly likely to influence how fairness is interpreted under data protection law.

The difficulties of conducting a cost–benefit analysis for data protection regulation

The FTC's fairness test relies explicitly on a cost–benefit analysis, which requires a comparison of the aggregate harm caused by a given practice with the aggregate benefits of the practice. Where the aggregate harm outweighs the benefits, the practice is unfair. Where the aggregate benefits outweigh the injury, the practice is presumably fair and should be allowed. This approach reflects the traditional law and economics approach to tort law, based on the so-called Hand formula.[35] Under the Hand formula, a person should expend costs on preventing injury in an amount '*B*' which is equal to the amount of the injury '*L*' multiplied by its probability '*P*'. When calculating '*P*', the injuring party can assume that the victim will take reasonable steps to avoid injury. Under this approach, not all injuries are prevented, only a reasonable level of injuries. This approach comes as close as possible to a negotiated outcome if there were a perfect market for buying and selling risks and injury prevention measures.[36] The total costs of injury plus the total costs of injury prevention spent by the injuring party and the victim are minimized, thereby achieving an efficient outcome from a welfare economics standpoint.

The European approach to fairness focuses not on a cost–benefit analysis, but on the level of information provided to the data subject, the data subject's legitimate interests, and the ability to exercise his or her individual autonomy. Europe's focus on individual autonomy is grounded in the recognition of privacy and data protection as fundamental rights.[37] The FTC's approach is a welfare economics approach, taking into account not only the harms but also the benefits associated with the relevant practice. The European approach is an individual rights approach, which does not take into account—at least not explicitly—the benefits of the relevant practice. These two approaches are not necessarily incompatible, although the subject is hotly debated.[38]

Let us put aside the complex debate on whether a rights-based approach is compatible with a welfare economics approach, and focus on the particular problem

33 Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts, O.J. L 095, 21 April 1993, pp. 29–34.

34 French Commission on Abusive Contractual Clauses, Recommendation n° 2014-02, relating to contracts proposed by providers of social media services.

35 R Posner, *Economic Analysis of Law* (8th edn., Aspen/Wolters Kluwer, New York, 2011).

36 RH Coase, 'The Problem of Social Cost' (1960) 3 JLE 1.

37 *See*, Articles 7 and 8, European Charter on Fundamental Rights, Article 8 European Convention for the Protection of Human Rights and Fundamental Freedoms. For an insightful comparison of the US and European approaches to privacy, *see* JQ Whitman, 'The Two Western Cultures of Privacy: Dignity Versus Liberty' (2004) 113 Yale L.J. 1151.

38 L Kaplow and S Shavell, *Fairness Versus Welfare* (Harvard University Press, Cambridge, 2006); M Geisfeld, 'Efficiency, Fairness, and the Economic Analysis of Tort Law', N.Y.U. School of Law, Law & Economics Research Paper n° 09-21 (2009).

of conducting a cost–benefit test in data protection. Alessandro Acquisti[39] and Adam Thierer[40] explore this difficulty. Thierer's focus is on conducting cost–benefit analyses in the context of regulatory proposals, following the US rules on good regulation.[41] However, Thierer's considerations would also apply to a cost–benefit analysis conducted by a regulator in the context of a 'fairness' test.

Acquisti and Thierer point out that privacy is an intangible—and in many cases immeasurable—right, similar to the right to pursue happiness. Privacy is often based on consumer emotions, not economic considerations, making economic evaluation difficult. Individuals say that privacy is important, but traditional economic tools, such as willingness to pay (WTP) and willingness to accept (WTA), show that individuals in fact attach a low value to privacy in practice. There is a considerable gap between what people say and how they actually behave when given a choice to acquire (or forego) privacy protection in exchange for a price.[42] This paradox may lead to an under-valuation of privacy harms, if the harms are measured solely using the traditional WTP tests.

In some cases, privacy violations can lead to measurable harm, such as when a company loses credit card records. A loss of credit card information requires banks and consumers to take steps to avoid fraud. Those steps create costs that can be measured. The receipt of unwanted spam also creates harm that can be quantified, as does the loss of data that might facilitate identity theft. Even if an actual case of identity theft cannot be traced to a given data breach, the data breach increases the probability of identity theft, and that probability can be estimated. Moreover, the increased risk of identity theft may require that consumers take preventive action to address the increased risk, and the cost of those measures can be quantified.

The most difficult harms to quantify are those associated with the feeling that certain data practices are 'creepy'. Creepy is something that causes people to feel nervous and afraid.[43] Another way of looking at 'creepy' data practices is to call them practices that go beyond what a consumer would reasonably expect. In those cases, the harm can be linked to inadequate information provided to the data subject. Lack of information reduces consumer choice and is a frequent justification for privacy regulation. Solove and Hartzog examine several cases where the FTC has based its unfairness findings on inadequate information to consumers, including cases involving non-obvious default settings in software.[44]

After looking at the costs, and if possible quantifying them, regulators must look at the benefits of the relevant practice. Benefits of a potentially unfair practice are equal to the costs associated with stopping or regulating the practice. To measure these costs, regulators must consider two situations: a situation where the practice is unregulated and a situation where the practice is regulated or prohibited, and compare the two situations. The difference between these two situations is the cost of the regulation, or put differently, the benefit of no regulation. Like privacy harms, benefits are difficult to quantify. Widespread use of advertising cookies generates increased advertising revenues through targeted advertising, which in turn brings more free services and information to consumers. Goldfarb and Tucker attempted to measure the effect of the EU cookie regulation on the effectiveness of online advertising. They found that Europe's opt-in rule for cookies had a significant adverse effect on the online advertising market:

> First, privacy protection will likely limit the scope of the advertising-supported internet. However, it also crucially suggests that the types of content and service provided on the internet may change. In particular, without the ability to target, website publishers may find it necessary to adjust their content to be more easily monetizable. Rather than focusing on political news, they may focus on travel or parenting news because the target demographic is more obvious. Furthermore, without targeting it may be the case that publishers and advertisers switch to more intentionally disruptive, intrusive, and larger ads.[45]

Goldfarb and Tucker also argue that privacy regulation has an effect on innovation, which should be considered in any cost–benefit exercise. Thierer points out that privacy regulation can also affect other individual liberties, such as freedom of expression.[46] Like harm to

39 A Acquisti, 'The Economics of Personal Data and the Economics of Privacy', OECD Background Paper n° 3, Joint WPISP-WPIE Roundtable (2010).

40 A Thierer, 'A Framework for Benefit-Cost Analysis in Digital Privacy Debates' (2013) 20 Geo. Mason L. Rev. 1055.

41 President of the United States, Executive Order n° 12866 of 30 September 1993; Office of Management and Budget Circular A-4, Regulatory Analysis, 17 September 2003.

42 European Network and Information Security Agency (ENISA), 'Study on Monetizing Privacy – An Economic Model for Pricing Personal Information', 27 February 2012.

43 Merriam-Webster Dictionary, <http://www.merriam-webster.com/dictionary/creepy>. For a discussion of 'creepy' in the data privacy context, *see* O Tene and J Polonetsky, 'A Theory of Creepy: Technology, Privacy and Shifting Social Norms' (2013) 16 Yale L.J. & Tech. 59.

44 Solove and Hartzog, above, n 9.

45 Goldfarb and Tucker, above, n 18.

46 Thierer, above, n 40.

innovation, harm to freedom of expression is difficult to quantify. But the existence of these harms should be considered, at least from a qualitative standpoint. Alternative proposals should be compared with regard to their relative impact on other rights and interests.

Ideally, a cost–benefit test of this kind should be performed for any proposed new privacy regulation.[47] The European Commission[48] and the UK government[49] conducted regulatory impact assessments with regard to the proposed General Data Protection Regulation, but those assessments did not go into this level of detail.

In summary:

- The FTC's methodology on fairness requires an attempt to balance the relative benefits and harms associated with a given practice.
- Measuring harms associated with poor data protection is difficult, because traditional 'WTP' and 'WTA' methodologies show that consumers do not value privacy very much when given concrete choices.
- The benefit associated with a given practice (and the associated harm of regulation) is measured by the difference between the situation existing without a regulatory prohibition and the situation existing with a regulatory prohibition. Goldfarb and Tucker applied this methodology to the EU cookie regulation.
- Better regulation methodology in the USA and the EU both require cost–benefit analyses, including an examination of the effect of various regulatory alternatives on hard-to-measure rights such as privacy.

'Principles-based' versus 'rules-based' regulation

The debate between 'principles-based' versus 'rules-based' regulation is not new.[50] In the law and economic literature, the debate is generally framed in terms of 'rules versus standards'.[51] Standards are general principles, such as the prohibition of 'unfair' practices, or the requirement that processed personal data not be 'excessive'. Standards require interpretation and judgment to determine whether a given practice complies with the standard. Rules require less interpretation than standards. The EU rule that personal data may not be transferred outside the EU unless the recipient has signed standard contractual clauses is an example of a rule. Crystal clear, the rule requires almost no interpretation.

This of course is an over-simplification. Most legal provisions are somewhere in between general standards and precise rules.[52] Depending on where they are situated on spectrum, the provisions will require varying levels of interpretation.

The existing EU Data Protection Directive contains both general standards (eg 'fair and lawful') and detailed rules (eg no transfers outside the EU unless an exception applies). The proposed General Data Protection Regulation will change this balance by increasing the level of detail when compared with the 1995 Data Protection Directive. The draft regulation contains over 90 articles, including provisions governing issues such as data portability, profiling, data transfers, and de-referencing of individuals' data. Koops has argued that the proposed regulation is too detailed and prescriptive.[53] Some of the proposed regulation's provisions are precise rules, such as the requirement that consent be given in a manner distinguishable from consent to other matters.[54] Other provisions attempt to apply general principles to specific kinds of processing, such as *'automated processing intended to evaluate certain personal aspects relating to [a] natural person or to analyse or predict in particular the natural person's performance at work, economic situation, location, health, personal preferences, reliability or behavior'*.[55] These provisions are aimed at new forms of digital processing.

The difference between general standards and detailed rules has been studied at length elsewhere.[56] A standard is more likely to stand the test of time, because courts or regulatory authorities can interpret the standard in light of new technological developments and fact situations. A regulatory authority can apply the 'unfair and deceptive', or the 'fair and lawful' standard, to almost any situation that might arise on the Internet, and the standard will never be outdated. The disadvantage of a standard is that it can create an unpredictable environment for stakeholders, who will have to guess in advance whether their own conduct violates the standard. Standards are also more costly to enforce. Determining whether a given data processing operation is 'excessive' will require

47 European Commission Better Regulation Guidelines, 19 May 2015. OMB Circular A-4, above, n 41.

48 European Commission, Impact Assessment on the proposal for a General Data Protection Regulation, SEC(2012) 72 final, 25 January 2012.

49 UK Ministry of Justice, Impact Assessment for the proposal for an EU Data Protection Regulation, 11 November 2012.

50 For a general discussion of 'principles-based regulation', *see* J Black, 'Forms and Paradoxes of Principles Based Regulation', LSE Law, Society and Economy Working Paper 13/2008, SSRN abstract n° 1267722.

51 L Kaplow, 'Rules Versus Standards: An Economic Analysis' (1992) 42 Duke L. J. 557; Posner, above, n 35, p. 747.

52 Black, above, n 50.

53 Koops, above, n 2.

54 Proposed General Data Protection Regulation, above, n 1, Article 7.

55 Ibid, Article 20.

56 Kaplow, above, n 51; S Breyer, *Regulation and Its Reform* (Harvard University Press, Cambridge, 1982).

a fact-intensive inquiry, whereas determining whether a data controller has made a required data protection filing can be determined simply by verifying the data protection authority's registry.

To address the uncertainty surrounding vague standards, regulatory authorities, such as the FTC in the USA or the Article 29 Working Party in the EU, issue guidelines. In addition to guidelines, enforcement actions, court decisions, and settlements provide signals to market actors. This is how regulation occurs in traditional tort law: courts apply general standards such as 'fault' or the 'reasonable man', and economic agents learn from those court decisions and adapt their conduct accordingly.

Detailed rules are easier to understand and enforce than standards. A regulator does not generally have to conduct a fact-intensive balancing test to determine if a company has violated a rule. Rules create a more predictable environment for stakeholders, because they will not be left guessing what kind of conduct violates the rule. A rule requires less information to understand and enforce. A rule contained in a statute reflects a balance struck by elected officials after a democratic debate. Such a rule benefits from legitimacy compared with the guidelines created by a regulatory authority that is not directly accountable to citizens. But a rule can quickly become obsolete and can open unintended loopholes. A rule can also impose a form of conduct that is not well adapted to given situation, thereby leading to inefficient outcomes. A classic illustration is a rule requiring that pedestrians cross a street using the crosswalk. The rule is easy to understand, and its purpose is to reduce pedestrian injuries. However, there are situations where is it more dangerous to use the crosswalk than to cross in the middle of the block. A rule does not have built-in flexibility.

In summary, detailed rules adopted by the legislature have the advantage of having a high level of political legitimacy, and being predictable. But they run the risk of becoming obsolete, and in some cases, they can lead to inefficient outcomes. A general standard will better stand the test of time, will in theory lead to the optimum level of conduct, but will create uncertainty for stakeholders and require significant information to enforce.

As noted above, most legal provisions fall somewhere in the middle. They are more detailed than a general standard but less precise than a detailed rule. The distinction between standards and rules should be viewed as a continuum, not as a binary alternative. What is interesting for our purposes is to see that the FTC has been able to apply the 'unfair and deceptive practices' standard in a way that achieves outcomes similar to those required by more detailed EU data protection provisions, which are closer to the 'rules' side of the spectrum.[57] The FTC has imposed the principle of obtaining affirmative express consent from the data subject before using geolocation information,[58] an outcome identical to the rule imposed by the European E-Privacy Directive.[59] The FTC has punished the collection of users' detailed browsing information without clear disclosure of the practice, a measure designed to address the same harm as the EU cookie rule.[60] The FTC held that material retroactive changes in privacy policies are unfair[61] and that inadequate security measures are unfair.[62] The FTC's standard for information security probably surpasses that of many data protection authorities in Europe. Through its settlement agreements, the FTC has been able to impose 20-year-long data protection compliance programmes on large Internet companies, including Google, Facebook, and Twitter. These compliance programmes include obligatory training, audits, and ongoing reporting obligations to the FTC. These measures go beyond what certain data protection authorities in the EU are currently able to impose.[63] The French CNIL, for instance, currently does not have statutory power to negotiate undertakings in the context of sanction procedures. The FTC's experience shows that general standards in privacy are not necessarily inferior to more detailed rules.

Standards and rules can also have different effects on internal compliance attitudes. Bamberger and Mulligan studied how companies build privacy compliance into their corporate organization and operations.[64] They found that the FTC's privacy activism had prompted companies to build internal compliance programmes with trained privacy professionals to implement the programmes. These privacy professionals view themselves not just as compliance officers, but also as 'norm entrepreneurs'. For Bamberger and Mulligan, overly prescriptive privacy rules would weaken this internal norm entrepreneur function:

57 Solove and Hartzog, above, n 9.

58 *Aspen Way Agreement & Order*, n° C-4392, 25 September 2012.

59 Directive 2002/58/EC on Privacy and Electronic Communications.

60 *In re Sears Holdings Mgmt. Corp.*, n° C-4264, 31 August 2009.

61 *In re Gateway Learning Corp.*, 138 FTC 443 (2004).

62 *FTC v Wyndham Hotels*, Civ. Action n° 13-1887, Dist. Ct. N.J., 7 April 2014.

63 W Maxwell, 'Global Privacy Governance: A Comparison of Regulatory Models in the US and Europe, and the Emergence of Accountability as a Global Norm' in C. Dartiguepeyrou (ed), *The Futures of Privacy* (Fondation Telecom, Paris, 2014).

64 K Bamberger and D Mulligan, 'Privacy on the Books and on the Ground' (2011) 63 Stan. L. Rev. 247, 314.

> A decision to redirect privacy regulation towards more rule-bound governance, for example, might diminish the need for corporations to rely on high level internal privacy experts, and in turn reduce their capacity to embed privacy into corporate culture and business operations.[65]

Bamberger and Mulligan identify a paradox that may not have been fully considered by European policymakers. Prescriptive rules might favour a formal check-the-box compliance attitude, whereas general standards might be more conducive to principles-based data protection governance programmes.

In summary:

- General standards are more flexible than detailed rules. Detailed rules are easier to understand and to enforce than general standards but can miss their mark and become quickly outdated. Most legal provisions are somewhere in the middle, between general standards and detailed rules.
- The proposed General Data Protection Regulation contains 90 articles, introducing considerably more detail than what exists in the existing Data Protection Directive. Several of the proposed provisions create detailed rules (eg rules on consent) and target new kinds of electronic processing (profiling).
- The FTC's application of the 'fair or deceptive' standard has in many cases permitted the FTC to achieve the same outcome as that achieved in Europe. Bamberger and Mulligan speculate that the existence of general standards is more likely to encourage 'norm entrepreneurship' within corporations, as opposed to 'check-the-box' compliance attitudes.

Suggested methodology for regulatory restraint

New digital platforms and markets raise new privacy challenges that are often difficult to evaluate. Some of the risks are potentially significant, but the probability of the risk occurring and the ability of the market to deal with the risk without regulatory intervention are unknown. Policymakers will have a tendency to conclude that the new risk requires a new regulation. The creation of a government regulatory solution to address a poorly understood risk creates costs of its own. As pointed out by Howard Shelanski, regulatory solutions often miss their targets in fast-moving technological markets.[66] What policymakers considered to be a significant market failure at the time they enacted the regulation may turn out to be a non-issue given market and technological developments. Shelanski concludes that in the field of regulating digital markets, the cost of 'Type I' errors, ie enacting a regulation when in fact no regulation was necessary, is much greater than the cost of 'Type II' errors, ie failing to regulate when in fact a government regulation should have been adopted. In the case of 'Type I' errors, Shelanski points out that the market can often self-correct. By contrast, the government regulation that misses its mark will create costs that the market cannot correct.

In spite of this, politicians have a natural bias to enact a regulation in order to address the new but ill-defined risks in digital markets. This is understandable: In the market for political decisions,[67] a regulator or politician who announces that he or she is going to take measures to address potentially grave new risks posed by digital markets will be perceived as proactive and courageous. A politician who says that it is better to wait before doing anything will be perceived as weak and complacent. The costs of the 'Type I' error will generally not be borne by the politician or regulator who sponsored the original proposal. Consequently, the regulator or politician will have a natural bias in favour of enacting new regulation as opposed to relying on existing laws, even if regulatory restraint would have been the superior choice.

The discussion of fair processing shows that general principles can sometimes go a long way towards regulating new digital markets. That is not to say the new rules are never necessary. In some cases, there may be an enduring market failure that requires the adoption of specific rules, and the reliance on existing principles will not be sufficient. However, the need for a new regulatory solution should be verified before new rules are enacted.

The European framework for regulating electronic communications contains a methodology that could be extended to other cases of digital regulation.[68] The regulatory framework for electronic communications is focussed principally on competition-related market failures, but there is no reason why the methodology could not be extended to cover other kinds of market failures in digital markets. The methodology flowing

65 Ibid, p. 314.

66 H Shelanski, 'Information, Innovation and Competition Policy for the Internet' (2013) 161 U.Pa.L.Rev. 1663.

67 For a discussion on the market for political decisions, *see* G Stigler, 'The Theory of Economic Regulation' (1971) 2 Bell J. Econ 3; Posner, above, n 35, p. 731.

68 Directive 2002/21/EC of 7 March 2002 on a common regulatory framework for electronic communications networks and services (Framework Directive).

from the EU framework on electronic communications is quite simple: before enacting a new regulatory obligation aimed at addressing the competition-based market failure, regulators must satisfy a three-step test. First, regulators must conduct a market analysis in order to precisely define the market failure that needs to be addressed and confirm the presence of enduring barriers to entry. Second, the regulator must explain why market and technological evolutions are not likely to address the market failure. Finally, the regulator must show why existing competition law is not sufficient to deal with the problem. If all three tests are satisfied, then the regulator may propose a new regulatory solution. The regulator's proposal is examined, however, by the European Commission who will ensure that the regulator has considered all the relevant options before proceeding. In addition, when the regulator chooses a remedy, the remedy must be the least burdensome alternative available to treat the market failure.

As noted above, this methodology is designed to address regulatory measures in the electronic communications market. The general methodology could be extended, however, to specific regulation designed to address privacy-related harms. In that case, the regulator would be required first to characterize the market failure that needs to be addressed. This characterization would necessitate empirical evidence that the harm actually exists, or if it does not yet exist, why the harm is likely to emerge. Second, the regulator would have to explain why it is unlikely that the market will bring its own solutions to the problem. In the telecommunications field barriers to entry are sometimes so high that it would be next to impossible for a competitor to enter the market, thereby making the emergence of market-based solutions unlikely. In the case of data privacy harms, the regulator would have to make a similar demonstration showing that it is unlikely that new technologies, service providers, or platforms would permit the relevant risk to be addressed by the market.

Lastly, and most importantly for this article, the regulator would need to ask whether existing law can provide a remedy for the identified harm. This would require that the regulator take stock of existing laws, including general principles contained in data protection and consumer protection legislation. In this context, the regulator would ask the question whether provisions such as those prohibiting unfair processing or unfair commercial practices would be sufficient to permit courts and regulatory authorities to address the new risk. If enforcement of existing legal provisions is inadequate, one option would be to improve enforcement rather than create new regulations.[69]

The *Google Spain v Costeja* case[70] is an example of a court using existing data protection principles to address a new risk, the so-called right to be forgotten. The European Court of Justice used the general principles of the existing Data Protection Directive to reach a result that many thought unreachable without new legislation. *Google Spain v Costeja* creates its own set of incongruities, which may ultimately have to be corrected through new legislation. However, the case shows that general principles should not be discounted too soon.

As noted above, reliance on general principles gives courts and regulatory authorities flexibility to apply a fact-specific analysis to fast-moving markets. A general principle can be applied flexibly in a manner that evolves with new technological and market developments. A detailed rule may lack this flexibility.

There may be cases where flexibility creates excessive costs. For example, when a general principle leads courts to adopt conflicting decisions, there may be a need to legislate in order to achieve consistency. Also, there may be situations where courts are powerless to apply the general principle to the new risk. In that case, courts will throw up their hands and state that the law as currently drafted does not permit them to address the problem properly. In that case as well, legislative intervention is necessary. However, these situations arise after several years have gone by, and it has been possible to observe the deficiencies of existing legal provisions. Many legislative proposals targeting digital risks do not respect this observation period.

Fair processing cannot treat all ills in a digital environment. However, this article has shown that fair processing and other existing data protection principles have more to offer than many would first assume.

In summary:

- Regulators are quick to see market failures in new digital business models, but premature regulation can create errors that are difficult to cure.
- The European framework for regulation of electronic communications imposes a methodology of regulatory restraint. The sponsor of a regulatory proposal must establish that there is an enduring market failure that is not likely to be addressed to technological or market evolution, and that competition law is insuffi-

69 European Commission Better Regulation Toolbox, 19 May 2015.

70 *Google Spain v AEPD and Costeja*, Court of Justice of the European Union, 13 May 2014, C 131/12.

cient to address the problem. This methodology could be extended to other fields of digital regulation, such as data protection.

- Before creating a new regulation, the application of existing laws should be considered, including where necessary improvements in enforcement of existing laws. In many cases, reliance on existing laws will be a lower-risk alternative than creating new regulations to address perceived market failures in complex and poorly understood digital ecosystems.

doi:10.1093/idpl/ipv013