DOI: 10.1007/s10272-011-0391-6

Ralf Boscheck*

Internet and Consumer Privacy: Considering the FTC's "Do Not Track" Proposal

The digital economy relies on the collection of personal data on an ever-increasing scale. Regulations have to be found which can provide an optimal balance between consumers' interest in privacy and the benefits from innovations that rely on the largely invisible collection, retention and sharing of consumer data. The following article discusses current US reform proposals and their relevance for the ongoing debate in Europe.

Commentators of the projected overhaul of the European Data Protection Directive (DPD)[1] often compare the Commission's initiative with similar US reform proposals. They typically find differences in terms of the intended comprehensiveness of rules, the anchoring of fundamental concepts such as "privacy" or "consent" in human rights versus a consumer bill of rights, or the preferred method of regulatory or self-regulatory enforcement.[2] While some take pride in the fact that Brussels can build on an established body of law, others point out that its legal foundations are antiquated and its conceptual apparatus utterly out of touch with current technological realities – let alone potential future developments. All dread the challenge of transposing the final directive into 27 member state rules. Conversely, some analysts applaud Washington's desire to introduce an apparently *novel* online privacy protection legislation but tend to overlook the fact that the relevant US case law related to "privacy" preceded European initiatives by more than 120 years and that federal regulations were at the forefront in developing the by now universal fair information practice principles (FIPPs). But focusing on differences between the two systems not only causes selective representation of the facts; it also blurs the view of how either one, in its own context, attempts to tackle a common challenge – the creation of a set of efficient rules able to minimise the sum of both enforcement costs and the cost of taking wrong decisions.

Taking a step back, this article identifies the fundamental regulatory concerns and, complementing the ongoing European policy debate, presents various elements of the US perspective. Future comparative analyses seem appropriate when regulatory directions on either side of the Atlantic are more clearly defined and, given the indeterminacy of information flows, to the extent that they enable the necessary discussion about a set of global regulatory standards.

Background

On 1 December 2010, the US Federal Trade Commission (FTC) invited comments on a new framework to balance consumers' interest in privacy with the benefits from innovations that rely on the largely invisible collection, retention and sharing of consumer data.[3] Realising that industry self-regulation has always been too slow and too ineffective in providing adequate protection, the FTC's proposal is to inspire future public policies as well as business standards governing privacy and is likely to have a global impact. Central to the report is the suggestion of a "Do Not Track" mechanism – a permanent setting of computer browsers that offers their users the choice or whether to allow the tracking of their online activities – or not. For some commentators, this "Do Not Track" option represents a clear example of "internet exceptionalism", i.e. an interference in business that would not occur outside the realm of the internet.[4] For others,

* International Institute for Management Development (IMD), Lausanne, Switzerland.

1 For the initial announcment and the four guiding principles see the statement by EU Vice President and Commissioner for Justice, Fundamental Rights and Citizenship, Viviane Reding: The Review of the EU Data Protection Framework, EU Press Release, 16 March 2011.

2 See the comments by Hannah Evershed on behalf of Mindshare at http://www.wpp.com/NR/rdonlyres/D4087988-AFD9-45F3-B76E037AB6976DED/0/mindshare_eu_privacy_directive.pdf or the comparative assessment by Omer Tene for the Center for Democracy and Technology at http://www.cdt.org/blogs/privacy-european-commission-must-be-innovative.

3 Federal Trade Commission: Protecting Consumer Privacy in an Era of Rapid Change, December 2010, at www.ftc.gov/os/2010/12/101201privacyreport.pdf.

4 E. Goldman: The Third Wave of Internet Exceptionalism, in: B. Szoka, A. Marcus (eds.): The Next Digital Decade: Essays on the future of the Internet, 2010, nextdigitaldecase.com/ndd_book.pdf.

it threatens to expand "the notion of personal privacy" and, as a result, "undermines the implicit bargain that underwrites the internet".[5] The following puts these arguments into perspective.

We shall first discuss the notion of privacy in general and in the context of a fast evolving information technology environment before positioning the FTC's current proposal *vis-à-vis* its own previous and other regulatory initiatives. Finally, we evaluate the criticism brought against the "Do Not Track" proposal.

Privacy, Media and Consent

Privacy denotes one's ability to isolate oneself from others and their views. To have no privacy means to be exposed, out of control and possibly open to coercion. People guard against encroachment and back away from those that would tap their phones, read their mail or search their rooms. Even if they had nothing to hide and others were guided by benign motives, they would find such intrusions humiliating.[6] Of course there may be limits to privacy if others are affected by concealed actions that they cannot assess or adequately prepare for, or if transparency would create an otherwise unobtainable, overcompensating value to society. Privacy concerns are therefore hardly clear-cut and they often arise in the context of publishing and the means for making information available to a wider audience.

As early as 1890, Samuel Warren and Louis Brandeis discussed the impact of portable cameras and advances in printing technology on privacy as the "right to be left alone," and in 1928, US Supreme Court Justice Brandeis restated his position when dissenting from a ruling that permitted wiretaps without warrants.[7] Since then, judicial and legislative initiatives around the world have tried to keep up with rapid increases in computing speed and analytics, data storage capacities and the scale and widespread use of information networks that make it impossible for individuals to know, let alone control, the information that others may have about them.[8] And yet while some common principles have emerged to limit the collection, access and use of data, regulatory actions are constantly outpaced by technological advance or new patterns of individual media use. New analytics, for instance, have just proven capable of re-identifying anonymised data that will place even early records at risk.[9] Similarly, internet use itself is not only altering the way individuals balance their needs for privacy and disclosure[10] but also the reliability of "rules of thumb" that they use in granting information access. Two cases illustrate the need to establish and secure user consent.

From 2005 to 2010, Facebook changed from a policy under which a user's data was only available to other Facebook users belonging to groups that the user specifically chose to a policy under which those same data elements were available to people without Facebook accounts.[11] In the words of the Electronic Frontier Foundation (EFF), a civil liberties group focusing on digital media and its use, "as Facebook grew larger and became more important, it helped itself and its advertising and business partners to more and more of its users' information, while limiting the users' options to control." Facebook's changes in its privacy policies clearly conflicted with users' privacy expectations, and by the end of 2009 about 35% of them had revisited and customised their privacy settings.[12] Such a reaction requires awareness, but internet users often do not realise the extent to which their privacy is already compromised.

In July 2010, the Wall Street Journal examined the 50 most popular websites in the USA, accounting for nearly 40% of US page views, to count the number of "cookies", "beacons" and other trackers installed on a visitor's computer by each site.[13] In total, the 50 sites placed 3,180 tracking files on a test computer used to conduct the study; only the encyclopedia Wikipedia.org installed none. Twelve sites, including IAC/InterActive Corp.'s Dictionary.com, Comcast Corp.'s Comcast.net and Microsoft Corp.'s MSN.com, embedded more than 100 tracking tools apiece. Google, Microsoft and Quantcast stated that they did not track individuals by name and offered internet users the option to opt out of their tracking networks. Dictionary.com installed 168 tracking tools that did not allow users to opt out and 121 tools that, according to their privacy statements, did not rule out col-

5 D.T. Rockey: Will the FTC's 'Do Not Track' Proposal Spell the End of Free Internet Content?, in: BNA Insight, Vol. 16, No. 4, 2011, pp. 164-167.

6 See S. Bok: Secrets: On the ethics of concealment and revelation, New York 1982, Pantheon Books.

7 S.D. Warren, L.D. Brandeis: The Right to Privacy, in: Harvard Law Review, Vol. IV, No. 6, 1890, pp. 193-210.

8 For a review see OECD: The Evolving Privacy Landscape: 30 years after the OECD Privacy Guidelines, OECD Digital Economy Papers, 2011, No. 176, at http://dx.doi.org/10.1787/5kgf09z90c31-en.

9 A. Narayanan, V. Shmatikov: Myths & Fallacies of Personally Identifiable Information, in: Communications of the ACM, June 2010, Vol. 53, No. 6.

10 In fact this idea predates the internet. See A.F. Westin: Privacy and Freedom, Atheneum, 1967.

11 Kurt Opsahl: Facebook's Eroding Privacy Policy: A Timeline, 28 April 2010, https://www.eff.org/deeplinks/2010/04/facebook-timeline/.

12 2nd Federal Trade Commission Information Roundtable, Remarks by Tim Sparapani, Transcript pp. 121-23, 28.01.10.

13 J. Angwin, T. McGinty: Sites Feed Personal Details To New Tracking Industry, in: Wall Street Journal, 30.07.10.

lecting financial or health data. In general it was thought that tracking would not violate anyone's privacy as data was not linked to people by name and the activity was disclosed in privacy policies. But surveys show that many consumers believe that the term "privacy policy" on a website means that the site protects their privacy, and information theory suggests that "only 33 bits of information are needed to uniquely identify a person out of the entire world population. Knowing that a person lives in a hometown of 100,000 provides already 16 bits of entropy about him – only 17 bits remain"[14] – enough reason for regulators to challenge the notion of informed consent.

Privacy Governance and the FTC Report

Already in the late 1960s, the application of new information technologies to the processing and sharing of personal data most importantly within and among governmental authorities raised concerns about how to safeguard the privacy and civil liberties of citizens. The resulting regulatory initiatives in most OECD countries ultimately converged in the concept of "fair information practices"[15], often supported by dedicated data inspection boards or privacy commissioners. In the USA, legislative responses were enacted in the 1966 Freedom of Information Act, the 1970 Fair Credit Reporting Act and the 1974 Privacy Act. They also provided the basis for the FTC's early consumer privacy initiative.

The Commission characterises its respective efforts as being guided by two approaches:[16] the "notice and choice model" relies on consumers making informed choices based on privacy notices that detail a given company's practice with regard to information collection and use; the "harm-based model" aims at avoiding specific harms, i.e. physical security, economic injury or unwanted interference with daily life. Both approaches significantly advanced the goal of protecting privacy. Since 2001, the Commission has brought 29 cases against companies that allegedly violated posted privacy policies, did not dispose data properly or allowed customer data to be shared with unauthorised third parties. Companies were ordered to implement thorough information security programmes, submit to third-party audits and provide sizeable monetary relief. During the same time, the Commission also brought 96 cases involving unwanted spam, 15 spyware cases and 15 cases against companies collecting personal information from children without parental consent. Since 2003, the FTC's Do Not Call rule has been enforced to shield consumers from unwanted telemarketing calls; currently the registry includes more than 200 million telephone numbers. As of 2008, the FTC's work on behavioural advertising has prompted industry to launch a variety of self-regulatory initiatives to ensure transparency, consumer consent and control. Respective enforcement actions recently involved a complaint against Sears[17], with the Commission claiming that the retailer had deceived consumers about the extent to which it tracked their online activities and a charge against Twitter[18] for failing to honour their users' choice to designate certain "tweets" as private. And yet, the FTC has realised the limits of its two-pronged privacy approach.

On the one hand, privacy policies too often reflect the need to limit a company's liability rather than to inform consumers. Increasingly long, legalistic and barely comprehensible disclosures offer consumers a limited choice and force them to bear the burden of protecting their privacy. Similarly, the harm-based approach typically neglects much wider concerns for reputational harm and the fact that new harms may result from the use of data that had not been envisioned when it was originally collected. On the other hand, consumers benefit from unprecedented connectivity, instant information access and choice, all of which is funded, in part, by targeted advertising and the use of consumer data. To balance both considerations, the preliminary FTC report of December 2010 outlines three principles: privacy by design, greater transparency and simplified choice.

"Privacy by design" means building privacy protection into everyday business practices, i.e. collecting only data that is needed for a specific and clear business purpose and retaining it only as long as necessary to fulfil that purpose. "Greater transparency" requires clear, standardised and therefore comparable privacy notices,

14 See Federal Trade Commission, op. cit., on consumer surveys and A. Narayanan, V. Shmatikov, op. cit., on "33 bits".

15 A 1973 report by the US Department of Health, Education and Welfare (HEW) entitled "Records, Computers and the Rights of Citizens" formulated the following principles of "fair information practice": (1) There must be no personal-data record-keeping systems whose very existence is secret. (2) There must be a way for an individual to find out what information about him is in a record and how it is used. (3) There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent. (4) There must be a way for an individual to correct or amend a record of identifiable information about himself. (5) Any organisation creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data. Quoted from OECD, op. cit., p. 8.

16 FTC, op. cit.

17 *In re Sears Holdings Mgmt. Corp.*, No. C-4264 (31 August 2009), http://www.ftc.gov/os/caselist/0823099/090604searsdo.pdf (consent order).

18 *In re Twitter, Inc.*, No. 092-3093, 2010 WL 2638509 (FTC, 24 June 2010) (proposed consent order).

reasonable access to consumer data and the need to obtain affirmative and express consent before using data in a materially different manner than claimed when the data was collected. "Simplified choice" limits the need for obtaining consumer consent to not commonly accepted data practices, i.e. to those that are not essential for product and service fulfilment, internal operations or legal compliance. Here customers must be given clear and concisely stated options and be able to decide on the use of their data. The Commission suggests that "one way to facilitate consumer choice is to provide it in a uniform and comprehensive way. Such an approach has been proposed for behavioural advertising, whereby consumers would be able to choose whether to allow the collection and use of data regarding their online searching and browsing activities. The most practical method of providing such universal choice would likely involve the placement of a persistent setting, similar to a cookie, on the consumer's browser signalling the consumer's choices about being tracked and receiving targeted ads. Commission staff supports this approach, sometimes referred to as 'Do Not Track'."[19]

The FTC's request for comments ushered in a host of calls for clarification.[20] Obviously, principles need refinement in context – particularly when the context is continuously transformed by changes in technological capacities, patterns of media use or business models. A framework that is to apply to commercial entities "that collect or use consumer data which can be reasonably linked to a specific consumer, computer or device" is always in danger of under- or over-regulating. Remember, data that once was considered anonymous can now be traced back! Next, fast changing products and markets may require a flexible interpretation of what constitutes reasonable data retention or commonly acceptable data practices. Given that some tracking is nearly always necessary to complete an online transaction, it is a vital and acceptable practice, which from the outset limits the scope of the "Do Not Track" proposal. And yet, the most fundamental criticism of the FTC's plan relates to the alleged intolerable extension of consumer privacy and the incompatibility of the "Do Not Track" rule with the "implicit bargain underwriting the internet".

Reconsidering Privacy, "Do Not Track" and the Economics of the Internet

Critics argue that the "Do Not Track" proposal not only inappropriately extends the consumer's reasonable expectation of privacy, but in the process severely limits effective market communication and, as a result, the economic viability of the internet and its provision of free content. For one, while the FTC's "Do Not Call" and similarly the subsequent "Do Not Mail" rules protect the consumer's privacy against unsolicited calls or advertising mail, it is argued that "such privacy generally ends, when she chooses to venture out where she may be easily observed or overheard, or chooses to disclose information to third parties. ... Few would argue that an individual who enters a brick and mortar location should have the legal right to prohibit the owner from observing them, monitoring their movements within the building, or offering purchase suggestions."[21] The FTC's "Do Not Track" option, however, implies that consumers should be able to use the internet "surreptitiously and without being observed."[22] Next, eliminating the opportunity to track consumers' browsing behaviour would effectively do away with much of current behavioural advertising, which, relative to less guided forms of promotion, has proven to be at least twice as effective in transforming an interest into a purchase.[23] Finally, "Do Not Track" not only infringes on producers' right to speak but is apt to "put an end to this Golden Age of ad supported Internet content and services".[24] There is need of some clarification.

Figure 1 plots a two-dimensional media map. The vertical axis charts degrees of exclusivity of media access from "absolutely proprietary" to "free for all"; the horizontal axis represents various ways of media use, from one-way notification to two-way real-time communication. Together these axes provide a matrix of value creation opportunities with different prospects for value capture.

Moving from left to right, media usage changes from the transfer to the exchange, and ultimately the direct joint production and further development, of information;

19 FTC, op. cit., p. vi.

20 The following is not going to review the breadth of the commentary. For a presentation of the main technical issues see for example comments by the Electronic Frontier Foundation at http://www.eff.org/deeplinks/2010/12/ftcs-privacy-report-calls-attention-privacy, the US Public Policy Council of the Association for Computing Machinery at http://usacm.acm.org/PDF/FTCprivacyResponseFinal.pdf, the Network Advertising Initiative at http://naiblog.org/wp-content/uploads/2011/02/NAI_FTC_Comments.pdf, or Comments from Software & Information Industry Association at http://www.siia.net/blog/index.php/2011/02/siia-comments-on-ftc-privacy-report/.

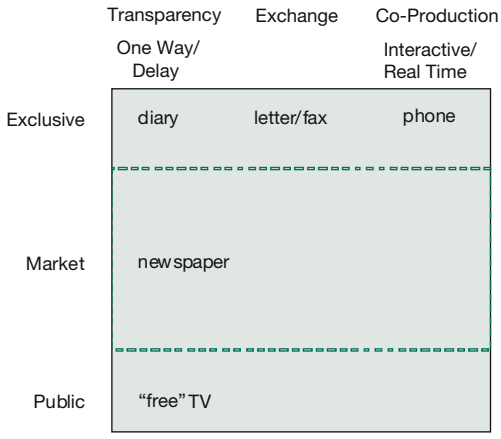
21 D.T. Rockey, op. cit., p. 165.

22 Ibid.

23 Howard Beales, a former Director of the Bureau of Consumer Protection at the Federal Trade Commission, suggests that behaviourally targeted advertising is more than twice as effective at converting users who click on ads into buyers (6.8 per cent conversion vs. 2.8 per cent for run-of-network ads). See H. Beales: The Value of Behavioural Targeting, 2011, at http://www.socialized.fr/wp-content/uploads/2010/08/beales-etude-sur-le-ciblage-comportemental-sur-internet-ppc4bible.pdf.

24 D.T. Rockey, op. cit. p. 166.

Figure 1
The Economics of Media



moving from top to bottom, the potential for economies of scale and scope in producing and consuming information increases exponentially. Commercial value capture – that is, the suppliers' ability to be paid for, and possibly in excess of, the costs of their services – is limited to the extent that consumption can be monitored and free-riders excluded; it is potentially largest where the benefits of transparency, exchange, and joint and real-time production can be exploited at the widest market, i.e. in the area just above the lower dotted line. Below that line, public goods are typically subsidised by the traffic they generate in a related and chargeable business model. Thus, newspaper sales are usually subsidised by advertising income, and a paper's attractiveness to advertisers is a function of its ability to reach clearly defined reader segments. The internet provides opportunities for operating across the entire matrix, creating the possibility of exclusive communication, market-based production and exchange as well as the generation of public goods. Yet, different from the newspaper, the internet initially is a pull and not a push medium, and it is in continuous interaction with the users who surf the web in search of content. Monitoring users' browsing behaviour provides valuable insights that are not available to print media and their advertising clients and allows for a targeted push. But it does so by breaking through the top barrier that separates the "market" from "exclusive" private media use.

Given that newspapers generate advertising revenue without excessively encroaching on readers' privacy, one may contend that with all the additional benefits the internet is offering, its viability does not rely on impinging upon privacy – no matter how much this would improve marketing effectiveness. But there is another angle to this. Tracking someone's browsing behaviour to match commercial offers not only improves sales, it also reduces the users' search costs and may create access to offers that otherwise would be missed. Put another way, tracking internet activities helps to speed up or complete the essential groping process of the market and thereby prevents market failures. Hence, the question is indeed one of privacy vs. efficiency.[25] The FTC's current proposal does not take a view but wants consumers to have a choice. Of course, that decision would be less concerning if the currently proposed blunt and universal opt-out could be replaced by a more fine-grained selection mechanism.

The extent to which privacy concerns need to be enforced by regulatory authorities largely depends on the degree of consumer awareness and the reliability of industry self-regulation. Already today, advertising opt-out tools such as AdBlock Plus and Do Not Track protection such as Mozilla's 2010 release of the Firefox browser are readily available. Also, Microsoft's Tracking Protection gives users the opportunity to fine-tune their opt-out decisions, and EFF's TOSBag page tracks changes in terms of services for a number of consumer facing websites such as Google, Netflix, Facebook and PayPal. With growing consumer awareness of the need to safeguard privacy, the question is whether tracking entities will respect consumers' clearly expressed intent. As usual, self-regulation can maintain market opportunities and reduce the risk of overregulation.

Conclusion

Realising that industry self-regulation has always been too slow and too ineffective in adequately protecting consumer privacy, the FTC's suggestion of a "Do Not Track" mechanism implies a trade-off between privacy and efficiency. US regulators want consumers to take informed decisions which could be improved if the currently proposed universal opt-out mechanism were to be replaced by more granular controls. Insistence on privacy does not undermine the viability of the internet. Realising its true potential requires a proper interplay between consumer awareness, industry self-constraints and regulatory control.

25 Obviously, one does not need to go as far a Richard Posner, who criticises privacy in employment relations as a means of covering up defects that ultimately reduce the efficiency of the labour market. See R. Posner: The Economics of Privacy, in: American Economic Review, Vol. 71, No. 2, 1981, pp. 405-9.