

Ensuring Respect for Privacy on the Internet

Dr. Lee A. Bygrave*

Associate Professor
Norwegian Research Centre for Computers & Law (N.R.C.C.L.)
Faculty of Law
University of Oslo

Introduction

In my presentation, I shall give some brief reflections on how best we can build up, and build in, norms for protecting privacy with respect to Internet transactions. I shall first consider traditional legal rules – particularly those in data protection legislation. Thereafter, I shall consider other rule types such as “netiquette”. Finally, I shall consider educational strategies to inculcate privacy norms in young persons. My basic point is that improvements can be made on all these fronts in order to *prevent* – as opposed to seek to remedy – privacy violations on the Internet.

Application of law to Internet

In the past, not so long ago, it was fashionable in some circles to claim that the Internet was a realm beyond the reach of traditional laws. This claim is facetious and has rightly been consigned to the history books as one of the myths of “digital libertarianism”.

For the Internet may be vast, it may be relatively new, it may be challenging for traditional values and norms, but it is and never has been beyond the reach of the law. Of course, some laws have been drafted in a manner that makes their application to the Internet difficult, but much law is sufficiently technologically neutral in its formulation as to permit application to new forms of technology and communication.

Hence, the basic question when assessing the applicability of laws to the Internet is usually not: do laws apply to the Internet? It is rather: how do they apply?

The latter question breaks down into several other questions:

- Do the laws apply with sensible results?
- Do they result in a desirable balancing of interests?
- Are the results unexpected? Unforeseen? Awkward?
- Do the laws give sensible guidance as to what online activity is permitted and what is not permitted?

* Associate Professor, Faculty of Law, University of Oslo; Research Associate, Baker & McKenzie Cyberspace Law and Policy Centre, University of New South Wales; Barrister of the Supreme Court of New South Wales.

As intimated, the main international instruments on data protection have been drafted sufficiently broadly so as to apply to the Internet. However, most of them have been drafted with little, if any, account taken of the digital environment. This is so with the EU's general Directive on data protection (Directive 95/46/EC – DPD). It is also the case with the 1981 Council of Europe Convention on data protection, along with the 1980 OECD guidelines and 1990 UN guidelines on the same topic.

The one notable exception is Directive 2002/58/EC on privacy and electronic communication (DPEC). The Directive covers some important ground and some controversial areas with respect to the online world – e.g., use of cookie mechanisms, logging and use of traffic data. Yet the Directive applies only to e-communication service providers (i.e., those who facilitate transmission of content), not content providers. Hence, it has relatively little to say about the appropriate conditions – from a privacy perspective – for development and application of, e.g., Digital Rights Management Systems (DRMS), as such systems are largely focused on provision of content. Somewhat surprisingly too the DPEC does not directly tackle several other key definitional issues in an online context, such as the scope of the “personal data” concept with respect to e-mail addresses, Internet Protocol (IP) addresses and attached clickstream data. It also leaves in the air the status of electronic agents, i.e., software applications which, with some degree of autonomy, mobility and learning capacity, execute specific tasks for a computer user or computer system.

The judiciary to the rescue?

The uncertainty surrounding the way in which data protection laws apply to the Internet is exacerbated by a paucity of clarifying case law. Court decisions treating in detail the provisions of data protection legislation in an offline context are few and far between; decisions that consider these provisions in the online context are almost non-existent.

Fortunately, we now have a landmark decision by the European Court of Justice (ECJ) dealing precisely with the application of data protection norms to processing of personal data on the Internet – more specifically, the applicability of Directive 95/46/EC to certain website-publishing activities of a Swedish woman. I refer here to the ECJ judgment of 6th November 2003 in Case C-101/01, *Bodil Lindqvist*. Many of you will be familiar with the ruling. It has attracted widespread public attention principally on account of its relevance for the increasingly large number of people who, in an ostensibly private capacity, set up personal “homepages” from which information about other persons can be spread.

In my view, the decision of the Court is a sensible one. It helps clarify the application of DPD Articles 3(2) and 25 in the context of website publishing. Nevertheless, it leaves a range of important questions unanswered. One such question is: When may a webpage with personal data be sufficiently private to fall within the ambit of Article 3(2)? It will be recalled that the second indent of Article 3(2) states that the Directive does not apply to data processing by a natural person “in the course of a purely personal or household activity”. Using recital 12 in the preamble to the Directive as a point of departure, the Court tersely held that this exception “must ... be interpreted as relating only to activities which are carried out in the course of private or family

life of individuals, which is clearly not the case with the processing of personal data consisting in publication on the internet so that those data are made accessible to an indefinite number of people” (paragraph 47 of the judgment). This is an eminently reasonable standpoint. However, the Court gave no guidance as to whether a lesser degree of accessibility (e.g., by a smaller and definite number of people) may make a website private for the purposes of Article 3(2). Concomitantly, it failed to provide guidance as to what mechanism might be sufficient to limit accessibility and thereby make a website private. Would, for instance, a password mechanism be sufficient? A host of further questions arise with respect to other parts of the Court’s judgment – particularly those parts dealing with the applicability of Article 25 to website publishing – but I do not have time to deal with these here.

The risk of regulatory overreaching

The application of data protection laws in an online context will not always produce entirely sensible or desirable results. A good example in point is provided by DPD Article 4(1)(c), which provides that the data protection law of an EU state may apply outside the EU in certain circumstances, most notably if a data controller, based outside the EU, utilises “equipment” located in the state to process personal data for purposes other than merely transmitting the data through that state.

This provision gives an impression that the EU is, in effect, legislating for the world. However, the provision is motivated in large part by the desire to prevent circumvention of EU data protection norms by data controllers based in third countries. That is, of course, a reasonable motivation. Nevertheless, implementation of the provision carries a distinct risk of regulatory overreaching in the sense that EU member states’ data protection laws are given so broad a field of application that there is little realistic chance of enforcing them. This risk looms particularly large in the online environment where, e.g., routine use of cookies mechanisms by website operators in third countries may involve utilisation of “equipment” in an EU state (assuming that the cookies are properly to be classified as personal data). Is it, for instance, realistic to expect a website operator in China that puts cookies on the browser programs of website visitors from the EU, to comply with EU member states’ privacy norms? Is it realistic to expect such an operator to be even aware of this compliance duty? The ultimate problem here is not so much one of regulatory overreaching but the fact that such overreaching may make a mockery of the law. Accordingly, greater thought should be given to amending Article 4(1)(c) – and the corresponding provisions in national laws – in order to ameliorate the risk of regulatory overreaching in the online environment.

Legislative support for PETs

Most data protection laws contain little direct support for the use of Privacy-Enhancing Technologies (PETs). The DPD is a case in point. Certainly there are provisions in the Directive which come close to mandating PET usage – see particularly Article 17 along with recital 46 in the preamble. Yet these provisions are concerned *prima facie* with *security* measures.

At the same time, we must not forget that any attempts to introduce more direct legislative support for PETs risk conflicting with generally accepted regulatory mores of today, such as the principle that legal rules should be technology-neutral and not distort marketplace competition. These difficulties, though, are surmountable. Rules encouraging PET development and usage could be drafted so that they simply stipulate the goals to be reached (e.g., greater allowance for anonymity and/or pseudonymity) and then specify the means for reaching these goals in fairly general terms only (e.g., in terms of systems development). German legislation provides an instructive model for such rules. I refer here particularly to section 3a of the *Bundesdatenschutzgesetz*. Moreover, it would not be difficult to modify DPD Article 17 so that it more clearly embraces PETs.

Role of “soft law”

Our attention should not be directed solely at refining and extending the privacy norms found in legally binding instruments. Netiquette, industry codes of conduct and other “soft law” instruments have also an important role to play in fostering privacy in the online environment. They have several ostensible advantages over traditional legal instruments. First, they often permit more flexibility. Secondly, they engender a greater degree of user “ownership” of the norms they promote. Thirdly, the language they employ is often simpler than the terminology of legislation.

Nevertheless, it would be wrong to claim that such schemes are without problems. They do not necessarily give greater prescriptive guidance than legislation: their apparently simple language can often harbour considerable ambiguity, and uncertainty frequently arises over the extent to which their dispute resolution outcomes create binding or influential precedent. They tend also to be relatively transitory. A case in point is Norway’s *nettnemnda* (Net Tribunal). This was established in early 2001 with sponsorship from the Norwegian ICT industry, and was probably the first scheme in the world to offer both a set of “Ethical rules for the Internet” and a workable dispute resolution procedure. It is now – just three years later – operationally defunct. There appear to be few other equivalent schemes in long-term existence.

The basic point I want to make is that hard law must be supplemented by soft law; “top-down” legislative action must be supplemented by “bottom-up” code making. In other words, we need to encourage co-regulation in the privacy field. Self-regulation by itself is insufficient. Experience indicates that self-regulatory initiatives will usually only work fruitfully in the face of a sustained threat by government to “cover the field” through legislation. Unfortunately, there seem to be few, if any, co-regulatory privacy schemes currently working with respect to the Internet industry. Australia’s Internet Industry Association Privacy Code of Practice, which arguably embodies the most ambitious plan for such a scheme, has not yet been officially approved by the Australian federal Privacy Commissioner.

Another point that is important to consider concerns the involvement of Privacy Commissioners and other data protection authorities in the development of basic Internet architecture; i.e., their involvement in the development of “code” (in Lessig’s terms) or “lex informatica” (in Reidenberg’s terms). My hunch is that data protection authorities rarely participate in the forums which spawn or shape Recommendations

for Consideration (RFCs) and other Internet standards. If my hunch is correct, then we are faced with a serious shortcoming on the part of privacy officialdom. It means essentially that the privacy authorities have not learned the basic lesson offered by Lessig, Reidenberg and others in their analyses of “code” and “lex informatica”. That lesson needs to be learned if we are to have a realistic chance of preserving the privacy-friendly characteristics of extant Internet architecture.

Education in schools

These references to learning dovetail neatly with the thrust of my final message. This message is that we need more education of the general populace about the importance of privacy and related values. At the same time, such education needs to be directed to a much greater degree than it has been in the past at young persons. Courses on “information ethics”, embracing data privacy issues, should be made a compulsory part of the school curriculum. There is much work to be done in this respect. Focus hitherto has largely been on getting more ICT into schools; relatively little focus has been directed at teaching youth about the ethical ramifications of using ICT. The privacy ramifications of this imbalance in priorities are now increasingly manifest with the growing number of children who have mobile phones with cameras and ready connection to the Internet.

It would be most natural to introduce such educational measures in secondary schools, but I wonder if primary school pupils also could be sensibly targeted. Learning about basic data protection norms is, after all, a natural extension of learning about bodily integrity and respect for others. We teach very young children to say “please”, “thank you”, “excuse me” etc. And we teach them about the importance of their bodily integrity and space. Might we not also sensibly teach them about basic manners on the informational plane?

There would seem to be increasing interest on the part of secondary and primary schools for appropriate teaching materials on data protection, but few such materials are available. The Office of the Information Commissioner in the United Kingdom has developed some useful and innovative educational packages (e.g., the “Protecting the Plumstones” CD-Rom which it sent out to some 30,000 UK schools in 2002). And the Norwegian Department of Education is also sponsoring development of a secondary schools’ course on data privacy. Such initiatives must be augmented. Data protection authorities can play an important role in developing course materials and should get more resources to do so.