

Privacy-Enhancing Technologies – Caught between a Rock and a Hard Place¹

[Published in *Privacy Law & Policy Reporter*, 2002, volume 9, pages 135–137]

Lee A Bygrave

Introduction

In this presentation, I intend to focus on the difficulties facing the development and – more importantly – application of privacy-enhancing technologies (PETs). These difficulties are considerable though not necessarily insurmountable. We need to take full account of them in any future reform of privacy/data protection rules. The underlying argument I want to advance is that, because of these difficulties, PET initiatives are struggling and need, amongst other things, greater legal support – particularly from EU/EC instruments.

PETs are not pets

Privacy-enhancing technologies are still far from being as pervasive part of our everyday lives as are household pets; neither are they as friendly and comprehensible (at least in the eyes of their ‘owners’). For the vast majority of people, PETs tend to be unfamiliar, poorly understood, alien to everyday life.

Of course, we do have a variety of commonly used technological-organisational platforms that have privacy-enhancing effects (eg, traditional systems for cash payment and telephony), though these arguably lie outside the ambit of the PET concept as they have not been set up with the conscious aim of enhancing privacy. In my opinion, the term PET should be reserved for technological (and, to some extent, organisational) systems that are *intentionally* developed to promote the privacy of persons.

While on the issue of definitions, we should also distinguish PETs from, respectively, security-enhancing technologies or ‘SETs’ (ie, mechanisms aimed primarily at ensuring the confidentiality, integrity and/or availability of data/information, though not necessarily in order to promote personal privacy) and from patterns of mere behaviour (eg, keeping one’s e-mail address confidential), though there are considerable overlaps.

That PETs tend still to play a marginal role in everyday life is due to a multiplicity of factors.

¹ This is the edited text of a speech presented at the EC Commission Conference on Implementation of Directive 95/46/EC, Brussels, 30th September 2002. The speech was given as part of Workshop 2 (‘Developments in the Information Society: Internet and Privacy-Enhancing Technologies’).

PETs do not pay

Perhaps the most acute factor hampering PET initiatives is economic. Unfortunately, many PETs don't pay. PET development over the last decade is a trajectory strewn with the burnt-out hulks of commercially failed initiatives. PETs tend to have remained not just technologies in search of an application – as are a great many privacy-invasive technologies (PITs) – but rather technologies in search of commercial viability. So far, it appears that the amount of investment required to kick-start and maintain in the marketplace PET applications has often far exceeded financial returns. Exacerbating this disproportionality is the recent burst of the 'dot.com' bubble and the concomitant flight of capital out of the ICT sector generally.

PETs are not pop

Part of the economic problem facing PET initiatives is lack of broad consumer take-up of PET applications. This lack of consumer take-up is itself due to a complex array of factors. It is partly symptomatic of little consumer awareness of the availability and functionalities of PETs. Yet it is also symptomatic of the unfortunate but inescapable fact that while public concern about privacy is often high in the abstract, it is rarely translated into concrete actions costing money. In this respect, the observation of a former US Congressman is apt: 'privacy is an issue in which public concern is a mile wide and an inch deep'.²

Mass take-up of PETs is hampered too by certain characteristics of PETs themselves and the way in which they are marketed. An individual PET tends to have a narrow field of application (eg, encryption of e-mail or blocking of 'cookies') such that a consumer who is seriously interested in safeguarding his/her privacy interests across many contexts has to learn about and acquire multiple PETs from multiple organisations. In terms of marketing, there is a paucity of readily available and non-technical information about many of the products concerned and their developers. This information gap is particularly problematic in light of the relatively high degree of complexity of many of the products, along with the fact that some of the basic PET functionalities – especially those of pseudonymity, anonymity and authentication – are relatively difficult for laypersons to properly grasp. With a few exceptions, national data protection authorities appear to have done little to bridge the information gap.

PETs have also received little real nurture from politicians and other major policy-makers – apart from occasional rhetorical flourishes of support. Indeed, governments will tend to look upon strong PETs with scepticism if not antipathy when the latter threaten interests of national security and crime prevention. The events of '9-11' and the ensuing 'war on terrorism' have undoubtedly made the political climate even less PET-friendly. As for PET initiatives that do not obviously threaten national security or crime control, these

² Glenn English, quoted in WH Dutton & RG Meadow, 'A tolerance for surveillance: American public opinion concerning privacy and civil liberties', in KB Levitan (ed), *Government Infrastructures* (New York: Greenwood Press, 1987), pp 147, 148.

risk being dumped by politicians for the same sorts of reasons that deny PETs mass-market appeal.

PETs can be PITs

Somewhat paradoxically, PETs are occasionally attacked by privacy advocates. ‘PETs are not always our pets’, the advocates claim. Concern is expressed about the level of privacy permitted by the particular tool (eg, does the PET promote pseudonymity when anonymity is arguably viable?; does it reflect the standards of the EC Directive on data protection or less stringent standards?). Privacy advocates are further concerned about the pedigree of the PET developers and about the character of the standards-setting process (eg, how open and transparent is that process?). Finally, they are concerned about the context in which PETs are applied and the ultimate effect of the application (eg, is the PET being applied in a process that enhances organisational power to the detriment of individuals?; is the PET being introduced as a palliative for the introduction of a PIT?).

Legal factors

Further frustrating PET development are legal factors. The first and most obvious of these are the numerous rules laid down in statute or case law which mandate disclosure of personal identity in various contexts. Another factor is that legal rules are often too diffuse to be effectively translated into mandatory PET standards. This applies even in privacy/data protection legislation, where it would be most natural to expect fairly direct backing for PETs. The 1995 EC Directive on data protection (Directive 95/46/EC) is a case in point. The closest the Directive comes to mandating PET usage is in Article 17 along with recital 46 of its preamble, but these provisions are concerned *prima facie* with security measures. Put somewhat simplistically, the Directive seems to be aimed more at controlling PITs than encouraging PETs. Of course, controlling PITs can indirectly encourage PETs, yet the problem remains that the Directive provides little guidance – indeed little vision – for PET development.

The current weakness of EU/EC legislative support for PETs is to be contrasted with the strong legislative support recently introduced for copyright-protective technologies in Articles 6 and 7 of the 2001 EC Directive on copyright (Directive 2001/29/EC). The contrast here is ultimately a reflection of the differences in the respective lobbying strengths of privacy advocates on the one hand and copyright-holders on the other.

At the same time, attempts to bolster PET usage through the introduction of more PET-specific rules into legislation, risk running into conflict with generally accepted regulatory principles. One such principle is that legal rules should be technology-neutral. Another principle is that legal rules should not distort marketplace competition. Finally, there is the danger of ‘legislating on a metaphor’ – to quote the words of Jon Bing.

Some light on the PET front

Not all is dark on the PET front. It is likely that PET development will get significant leverage off the growing popularity of ‘e-democracy’. Systems for online voting and the like are attracting increasing government support. If the hitherto strong emphasis in Western democracies on the need for anonymous voting is to be continued into the online world, provision will have to be made for development and application of PETs.

Another positive development is the newly adopted EC Directive on privacy and electronic communications (Directive 2002/58/EC). This instrument represents a move towards more direct and active encouragement of transactional anonymity and thereby usage of PETs to facilitate such anonymity. We see this most significantly in recital 30 in the preamble to the Directive which states that ‘[s]ystems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum ...’.

The Directive also breaks to some extent from the regulatory principle that legal rules should be technology-neutral: see, eg, recital 24 in the preamble (mentioning, *inter alia*, ‘spyware’ and ‘web bugs’) and recital 25 (mentioning ‘cookies’).

PETs need a pat

These points of light notwithstanding, PET development risks continued marginalisation unless it receives more encouragement from legislators. The issue then becomes: what form should such encouragement take? Should it mainly come in the form of non-binding recommendations (set down in, eg, a Commission Communication)? Should it come in the form of rules in a revamped Directive and if so, what sort of rules – provisions in the preamble or substantive provisions? Numerous alternatives present themselves.

While I do not wish to preempt the discussion on this issue at the workshop, it is my belief that we need to bolster PET usage by introducing legally binding rules. I say this because of the very considerable difficulties facing PETs and because I believe that PET usage is a necessary, though not sufficient, precondition for the effective maintenance of privacy and related interests. Moreover, I believe that, if drafted carefully, the sorts of rules that I am calling for do not need to break with regulatory principles on technology-neutrality etc. The rules could be formulated so that they primarily stipulate the goals to be reached (eg, of anonymity and/or pseudonymity), and their specification of the means for reaching these goals (eg, in terms of systems development) could be done without singling out and promoting a specific PET.

Fortunately, several models for such rules exist already. In addition to recital 30 in the preamble to the Directive on privacy and electronic communications, we have Article 17 of the general Directive on data protection which could be easily modified to extend to PETs. Another model is to be found in German legislation – most notably section 3a of the *Federal Data Protection Act* as recently amended. Finally, it is worth keeping in mind

the 2002 OECD *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. While these are primarily concerned with security rather than privacy, they are instructive for future work on drafting rules dealing specifically with the quality of information systems. For ultimately, the discussion about legislative support for PETs must be seen as part of a broader discussion about how to achieve a more systems-active regulatory policy for privacy/data protection; ie, a policy which integrates the concerns of privacy/data protection with the development and functionalities of ICT.