Legislation for Internet Security: Panacea or Placebo?

Comment on *Sundt C. EURIM - IPPR Discussion Paper on Partnership Policing for the Information Society.*

Stuart Ritchie *and* Michael Barwise

> *KOKO ... (To Mikado.) It's like this: When your Majesty says, "Let a thing be done," it's as good as done-- practically, it is done-- because your Majesty's will is law. Your Majesty says, "Kill a gentleman," and a gentleman is told off to be killed. Consequently, that gentleman is as good as dead-- practically, he is dead-- and if he is dead, why not say so?*
> *MIKADO. I see. Nothing could possibly be more satisfactory!*
>
> W S Gilbert. The Mikado, 1885.

Summary

- The paper by Sundt[1] appears to advocate stronger legislative controls that will further criminalise malicious acts against Internet-facing technologies. We consider this to be ill-advised.
- Before we can devise solutions to supposed problems we must first correctly identify those problems, determine our real objectives in solving them, and confirm that our proposed solutions are likely to be effective.
- We submit that:
  - current political and legislative thinking on Internet threats and security is based on vast body of assertion, but little verifiable fact.
  - legislative solutions to technical problems are generally ineffectual both in theory and in practice.
  - legislation in the areas of security and intellectual property has so far tended to promote technical insecurity,[2] while simultaneously reducing competitiveness.[3]
  - law enforcement agencies increasingly lack the resources to police complex issues that are not life-threatening.
  - over-regulation can exacerbate many of the anti-social behaviours that contribute to the Internet threat.
  - if real solutions are to be found we must overcome the "tick box mentality" currently prevalent in much policy-making.

- Supposing there is a genuine desire to address security on the Internet, we submit that there is a significant risk of legislating unadvisedly.
- We suggest that the proper initial emphasis should be the creation of a credible, properly researched body of evidence that addresses the proximate causes of the perceived threats. From the resulting knowledge base, we should then and only then develop policy that improves our chances of addressing the real underlying issues by means of:
  - information and guidance at all points on the product life cycle from developer to user.
  - standards that specify auditable and realistic criteria for efficacy as well as compliance.
  - education to inculcate ethical concepts in young people. This cannot be accomplished in "cyber-ethics" classes independently of the wider social context.
  - validation mechanisms that can prove whether the above are being accomplished.
- These controls should not be implemented in any coercive regime, but by means of appropriate incentives.

[1] Sundt. C. EURIM - IPPR Discussion Paper on Partnership Policing for the Information Society.

[2] Barwise M, Bjergstrom N, and Ritchie S, "*Hacker's Charter? Legislative Enshrinement of Software Insecurity*", Information Security Bulletin (July 2003 in press), also EURIM-circulated.

[3] Ritchie S, "*European Database Right: Innovation Enabler or Disabler?*", Hertfordshire Law Journal, autumn 2003 (forthcoming)

- Only secondarily should legislation be used as a control, to address specific issues that have proved themselves not to be amenable to other solutions.

Discussion

Sundt[4] says: *'Effective consultation is not cheap. It is, however, less expensive than bad law'.*
This is an excellent point, for which we may modify the legal maxim: Hard technology cases make very bad law. And we might add that bad policy is potentially just as damaging as bad law, and even easier and cheaper to create.

Identification of the problems

Sundt states that *'Government, industry, law enforcement and education must work together to prevent the "script-kiddies", who vandalise the Internet, from deterring ordinary users.'*[5]

"Script kiddies" or entry-level hackers do indeed present a security threat, but it is only one of a number of threats, the relative significance of which depends as much on the nature of the target as on the intent of the perpetrator. Notwithstanding, by far the greatest contribution to malicious activity on the Internet is currently made by the continued presence of readily exploitable vulnerabilities in Internet-facing technologies, than is made by failures of, or gaps in, public policy or law enforcement . To defeat all these perpetrators we should be building higher fences, instead of merely criminalising those who climb over them. Legislative solutions are appropriate only to problems that cannot be dealt with in simpler and more proportionate ways.

Policing Policy in respect of trans-national "crimes"

Sundt asks '*How should we police that part of cyberspace over which the UK might claim jurisdiction, so that others will work with us when the location of the criminal is elsewhere or unknown?*'[6]

Before we rush into such policing we should investigate international jurisdiction and legal classification issues. We should be extremely cautious about this. For a start, there is no part of cyberspace over which the UK (or any other individual nation or state) can claim supremacy. Jurisdiction (and equally choice of law) cannot make a lot of sense in the context of the Internet.

Johnson and Post[7] argue that *"Because events on the Net occur everywhere but nowhere in particular, are engaged in by on-line personae who are both 'real'…and 'intangible'…, and concern 'things'…that are not necessarily separated…by any physical boundaries, no physical jurisdiction has a more compelling claim than any other to subject these events exclusively to its laws."*; and *"Cyberspace radically undermines the relationship between legally significant (online) phenomena and physical location".*

Likewise the *Gutnick*[8] case , in which a person domiciled in Victoria, Australia, successfully sued, in the Victorian jurisdiction, a US publisher for internet defamation. On one view at least the tort was committed within the jurisdiction of New Jersey where the servers were located. About this Swinson and Galvin[9], trying to keep a straight face, say *"…if a US court is ever asked to enforce an Australian*

[4] Sundt, *op cit*, p 1.

[5] *ibid.*

[6] *ibid.*

[7] D Johnson and D Post, *Law and Borders – the Rise of Law in Cyberspace* (1996) 48 Stanford Law Review 1367 and www.cli.org/X0025_LBFIN.html

[8] Gutnick v Dow Jones & Co Inc (December 2002 unreported)

[9] J Swinson and B Galvin, case comment, Computer and Telecommunications Law Review

judgment obtained in circumstances similar to the Gutnick case, the US court will likely reconsider the question of the Australian court's jurisdiction.”. The point here is the ancient problem underlying international law: recognition and enforcement of judgements.

Our argument is that we should start from the supposition that there is probably no general solution to the problem of jurisdiction, then be prepared to work hard towards potentially very small achievements.

Law Enforcement and Harmonisation

The history of British moral censorship consistently shows how difficult it is to legislate in areas of subjective judgement, and all the more so across jurisdictional boundaries.[10]

We should have learned from these experiences to be particularly wary of introducing legislation that is difficult or impossible to enforce. Precisely because internet crime is not predicated on the presence, domicile or even residence of “criminals” in that jurisdiction, internet “crime” cannot be stopped even momentarily by criminalising certain internet activities in a single or even many jurisdictions. Harmonisation would need to take place in all jurisdictions. As the history of mutual extradition treaties shows, this would be extraordinarily difficult.

Sundt[11] suggests: “*A major need is, however, for more effective co-operation across jurisdictional boundaries. The harmonisation of penalties with regard to denial of service and computer misuse across EU member states may help but is only part of the problem*.”

Such co-operation as has been achieved so far is not a panacea. Burnstein[12] says: “*The multifactor tests of the Second Restatement and the Rome Convention do little to solve the choice of law problems in cyberspace, especially when the factors relied upon are geared toward and suited for a real-space world of easily drawn political boundaries*.”. Further, across the world only limited harmonisation is practicable, as discussed above.

Harmonisation is never as simple, or effective, or even sustainable in law, as it may seem, due to cross-cutting issues with other harmonisations. For example, the Privacy Directive,[13] and implicitly its offspring such as the UK’s Data Protection Act, may themselves violate international law, as pointed out in the US by Perritt and Stewart.[14]

The major classification problem remains. What counts as a crime? So long as there remain significant areas of disagreement, and so long as the rules of evidence likewise vary between relevant jurisdictions, effective international co-operation is very difficult and its development perforce must proceed slowly and carefully.

Security Begins at Home

Sundt[15] states: “*Industry has a major part to play in educating its customers but Government also needs to encourage good security practice as part of its social inclusion, promotion and awareness campaigns to encourage the take-up of on-line products and services, including its own. It also needs to*

[10] Travis A. Bound and Gagged. London, Profile Books. 2000.

[11] Sundt, *op. cit., p 7.*

[12] M Burnstein, “*Conflicts on the Net: Choice of Law in Transnational Cyberspace”*, 29 Vanderbilt Journal of Transnational Law 75

[13] Council Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 24 October 1995

[14] H Perritt and M Stewart, “False Alarm?”, (1999) 51 Federal Communications Law Journal 811, and www.kentlaw.edu/perritt/professorperritt/falsealarm9.html

[15] Sundt, *op. cit.*, pp 4-5.

encourage the use of established reporting mechanisms for product and service problems to ensure that trust in electronic services, and thus in e-government, is not lost."

This is a good suggestion. However, Government itself does not have an unblemished record in the security arena. An already proven and pro-active organisation such as the Office of Government Commerce might be expected to take on responsibilities in this sphere, but even OGC needs to become more expert in some areas such as risk definition before it could safely be given the necessary broad overwatch powers to "police" security policy and implementation.

There is already a large community of independent not-for-profit researchers into security vulnerabilities and their solutions. However, this community faces considerable opposition from vendors, and is being progressively criminalised by legislative provisions designed to protect commercial IPR.[16]

User Education

Sundt[17] has suggested a "Green Cross" code. This is an excellent idea in principle, but what should such a code contain, and how would it be developed and deployed? It is patently insufficient to offer mere lists of technical procedures. This has been demonstrated by the failure of school sex education to reduce teenage pregnancy. Current cultural attitudes are a fundamental contributor to the formation of behaviours. The "cool" hacking activities of a school child do not occur in isolation from a wider social context, but once in place, they will accompany that child into adulthood and potentially into escalated modes of Internet abuse.

Apart from active abuses, the largest contribution to Internet insecurity across the board is the casual attitudes of staff of commercial organisations to even well-identified threats. Inappropriate activities range from opening of potentially malicious e-mails without proper precautions to the downloading of pornography and other offensive material. We might think *prima facie* that severe penalties enshrined in formal policies can control such abuses. Mars,[18] however, has shown that much counter-productive risk-taking behaviour in the workplace stems from frustration at already excessively restrictive regimes. In such cases, over-regulation may exacerbate the problem, or at best have no significant positive influence.

Sundt[19] also recommends "*Government (including DTI, DCMS and DfES as well as Home Office) to work with industry (suppliers, retail outlets, ISPs, content providers etc) and with learning and content providers to encourage the use of more secure products and services and teach good practice (both self-protection and behaviour towards others) at all levels, from schools and colleges to workplaces and lifelong learning centres*."

This also is an excellent idea. However it presupposes the existence of such secure products. Currently this is not the case.[20]

[16] Barwise M, Bjergstrom N, and Ritchie S, "*Hacker's Charter? Legislative Enshrinement of Software Insecurity*", Information Security Bulletin (July 2003 in press), also EURIM-circulated.

[17] Sundt, *op. cit.*, p 5.

[18] Mars G. Cheats at Work. Allen & Unwin. 1982.

[19] Sundt, *op. cit.*, p 5..

[20] Schneier B and Shostack A. Judging Microsoft. Information Security Bulletin. 7.3. 2002.

Nevertheless, Sundt has correctly identified the way forward for security education. It must involve non-educationalist practitioners if the results are going to be of any service, as has recently been demonstrated by the mis-targeting of teacher ICT training under the NOF initiative.[21]

Practitioner Education and Responsibilities

Sundt says little of the well-recognised need for higher standards in the production and deployment of Internet-facing technologies. The law cannot help here, but fostering a culture of educated demand for improved security could be a major driver.

Sundt's suggestion[22] that "*... there is evidence that market forces are encouraging development of more secure products*..." is open to challenge. There is in fact substantial contrary evidence,[23] that vendors are not unduly interested in developing inherently secure products, as this is an arduous and expensive undertaking with little direct financial return in the current marketplace. However, were user security awareness to be enhanced, the market might eventually better support such efforts. The necessary awareness is thus a prerequisite, and can only be accomplished by education.

A discussion of qualifications and an example examination format for information security practitioners is offered in Appendix 2.

Conclusions: Alternatives to legislation

Due to the international and ephemeral characteristics of transactions on the Internet, legislative control over acts performed in its space is fraught with problems of jurisdiction, parity, evidential quality and practical policing. Furthermore, any such control can only be influenced post facto, while it is increasingly clear that the problems to be addressed are the fundamental flaws in technologies and education that are leaving the doors unlocked and wide open to criminal activity.

We believe it is a hard problem with few or no real quick wins to accommodate all these issues in just proportion in a common legislative base. We consider the place of legislation in controlling cybercrime as secondary to that of education and research towards technical improvements in, and more informed use of, technologies to create a more secure environment within which to conduct legitimate business.

Legislation ought to be applied only in the event of failure of all other alternatives. Furthermore, any criminalisation of acts performed upon technologies or Internet infrastructure absolutely must take into account the motive for those acts. We cannot afford to define broadly categorised offences that disregard intent, and which encompass acts performed in the course of legitimate research into the security of technologies. Neither can we afford to confuse the commercial interest of vendors in their IPR with the interest of the public at large in improved security,[24] and in so doing engender for technology vendors a unique immunity from independent scrutiny of their products.

Before we commit to processes or policy, we need to take a much more rigorous look at the proximate causes of the security problems we face, and be prepared to bring a much wider range of expertise to bear on them than hitherto: involving cultural, educational and technical professionals, to ensure the solutions we create, if not panaceas, are at least not mere placebos.

[21] Barnes P. Personal Communication (attached as appendix 1).

[22] Sundt, *op. cit.*, p 4.

[23] e.g. Andy Cobbold, BMC, quoted in "Suppliers hit back over software quality", Computer Weekly 24/06/2003 p16, as saying the elimination of security flaws is uneconomic.

[24] R Wobst, "*The Golden Cage: TCPA, Palladium and Some Likely Market Consequences*", Information Security Bulletin, 8.3. 2003.

Appendix 1

Statement by Peter John Barnes
Teacher Training in IT under the NOF Initiative

During 2002 I worked as a contract IT Education Consultant for the Midland South East Consortium delivering IT training to school teachers as part of the Governments NOF initiative.
I taught both primary and secondary phase teachers generic and subject specific ICT modules.

It was with great interest I undertook this role.
As a qualified and experienced teacher now working in the IT industry with experience from technician through to consultant and director of an education services company, I valued the opportunity to work directly with teachers.
In my commercial role I have devised training for many leading IT and network technology companies, including Cisco, Siemens, Motorola, BT, Nokia, Marconi, Nortel, Ericsson.

My experience was that I had much to offer school teachers in all sorts of computer skills from basic to advanced level.

The NOF scheme, was not well received by the majority of teachers. It focussed too much on the pedagogy and best practice of using ICT in teaching. For most teachers this was inappropriate as they needed to understand the basic concepts and use fundamental skills in the utilization of ICT. In other words they needed to be much more familiar and practised in the use of computers and software before they could make affective use of incorporating ICT into their teaching for the purpose of enhancing the lessons and learning experience of the pupils.

All teachers should have been issued with laptops allowing them access to computer based resources wherever and whenever they needed to and to allow them the opportunity of maximum exposure to any on-line education initiatives.

It was stipulated that the training had to be carried out by qualified teachers. This meant the exclusion of ICT professionals from commerce who could have made a significant contribution

Here are some quotes from the end of module reports that I submitted to the MSEC.

“The training module was not particularly effective because it dealt with planning and implementing ICT and included the “best practice” of ICT in the classroom, but the majority of teachers had not mastered enough basic computing skills to cope with or appreciate the intentions of the module.”

“Whilst I found First Class (the on-line mentoring and email system) easy to use, the majority of teachers didn’t. Again this stemmed from their lack of knowledge and practice in the use of ICT , particularly the resources associated with First Class, including Web browsers, file types and sizes, applications such Word and PowerPoint, tools such as WINZIP, data transfer rates and so on.”

“Most of the teachers relied on the face-to-face sessions rather than the intended use of First Class. They didn’t logon between sessions.”

“The teachers wanted more training in basic IT skills and the confidence to incorporate IT into lessons. Furthermore they wanted help with the type of resources and environments specific to their school. They did not want to spend time discussing pedagogy, which this module seemed to be based on. In other words they already new how to teach and there main problem was not adapting teaching principles to implementing ICT but rather familiarity with ICT itself and access to equipment.”

"I think there was something of a mismatch between the actual needs of teachers and what the module was designed to achieve. The teachers wanted skill in ICT, whereas the module dealt with the skill in planning for ICT."

"I can't see that a programme like this could ever be about supporting teachers effectively. Effective on-going support would almost certainly necessitate site visits. Whilst the opportunity was always there for on-line mentoring, this didn't prove to be a vehicle that teachers wanted to, or perhaps could easily, use."

*On the subject of motivating teachers: "*I think this could only ever be fulfilled in part through the NOF training……… the key motivator was to dispel their scepticism about the NOF training by providing them with instruction and resources at a level with which they could cope and was meaningful for their ability and teaching circumstances, whilst at the same time working towards the expected outcomes. Other than that I believe that an effective and lasting motivation can only be achieved by actually working alongside teachers in schools to skill them and help implement ICT into their subject teaching areas."

In summary teachers need:

- *Greater understanding of basic IT concepts*
- *To acquire comprehensive skill in the use of computer technology*
- *Access to equipment and in particular the use of a personal computers*
- *Education and training programmes written by experts in the IT field in association with educationalists (the material used in the NOF training was predominantly devised by the university schools of education, whose forte is teaching practice not the use of IT).*
- *Training by ICT experts.*
- *ICT trainers to work more closely with teachers in schools over longer periods of time.*

Peter John Barnes, BA Hons, PGCE, MIITT
Director, Lorikeet-IT

July 2003

Appendix 2

Statement by John Sherwood (© 2003, John Sherwood)
Information Security Practitioner Qualifications

Types of Formal Qualification

There are four distinct levels at which an overall education and training programme can be aimed for the purposes of professional development:

Awareness
This type of education is specific to the industry sector and the organisation. It would not be appropriate to address this need with a formal external qualification.

Technician
The vendor community is best placed to provide specific training and certification of technician skills with regard to specific technologies and products. An independent formal qualification would be difficult to maintain since technology moves so quickly.

Professional
This area is where there is currently a gap in the market. The CISSP attempts to address this area, but lacks the substance and hence the respect that such an external formal qualification requires.

Academic
There are several successful MSc programmes run by universities that address this area.
The Needs for a Professional Level Qualification
The objectives for a qualification at this professional level are:
To provide an external, independent benchmark against which professional practitioners of information security can be educated and examined
To be respected[25] across the international professional community as being a real test of professionalism, knowledge and experience.
To provide a realistic and attractive goal towards which information-security professionals can direct their personal professional development efforts and feel satisfaction once having achieved the qualification.
To provide a measure that can be used to assess the professional skill level of an applicant for a professional post.
To provide a measure that can be used to assess the competence of an information-security professional offering client services in the market place.

Components of the Qualification

Knowledge
A common body of knowledge with which a candidate must demonstrate an acceptable level familiarity and fluency

Experience
A measurement of the practical on-the-job experience acquired by the candidate.
Professionalism
Demonstration that the candidate understands a common code of ethics and professional practice and applies these in his/her professional work

Integration
Demonstration by the candidate that s/he can bring all the three above components together to deliver an all-round level of professional service

[25] *Footnote by Sherwood.* The main problem with the CISSP is that many regard it as a 'Micky Mouse' qualification that addresses only the 'knowledge' component and not the 'professionalism' or 'experience' components.

Components of the Examination
In order to examine the suitability of a candidate for award of the professional qualification, the following components are needed:

Formal Examination
To demonstrate theoretical knowledge against a published syllabus (to include ethics and professional practice)

Portfolio of Work
To demonstrate experience

Sponsorship
By two professional referees already of qualified standing who personally recommend the candidate

Peer Panel Interview
A panel of three peers who interview the candidate in depth to demonstrate integrated professionalism

John Sherwood
14th July 2003