

Trust in the Internet

1. Introduction

Nominet is keen to develop and enhance the reputation of the .uk domain name space, so that it remains a domain in which people have confidence and trust. Following a public consultation in 2006, Nominet adopted a strategy of raising industry standards, to work with registrars, to advocate models of self- and co-regulation, to monitor the wider regulatory environment, and to identify potential regulatory issues.

The purpose of this paper is to review recent developments in the wider environment and consider what implications they have for trust in the Internet and ultimately trust in .uk.

In the following paragraphs, we present a summary of the recent House of Lords report on Personal Internet Security, elements of the Government response to that report and the Byron review. In addition to these external forces, recent work by Nominet to support the aims of the Internet Governance Forum led to the development of messages from the UK, which identified Internet security as the key challenge facing us at present.

The PAB is invited to consider a set of questions which may inform the development of Nominet policy in this area.

2. House of Lords Report on Personal Internet Security

In July 2007 the House of Lords Science & Technology committee published its report on Personal Internet Security. The report is published in full at http://www.parliament.uk/parliamentary_committees/lords_select/internet.cfm

The Committee highlighted the threat to the future of the Internet posed by e-crime. It argued that the Government must do more to protect individual Internet users.

The Chairman of the House of Lords Committee, said: *'We are firm believers in the Internet. It is a huge force for good. But it relies on the confidence of millions of users. At the moment it seems that the Internet is increasingly perceived as a sort of 'wild west', outside the law. People are said to fear e-crime more than mugging. That needs to change, or else confidence in the Internet could be destroyed.'*

The Committee concluded that many organisations with a stake in the Internet could do more to promote personal Internet security: the manufacturers of hardware and software; retailers; Internet Service Providers; businesses, such as banks, that operate online; the police and the criminal justice system.

The Committee upheld the general principle that well-targeted incentives are more likely to yield results than formal regulation. It urged the Government, through a flexible mix of incentives, regulation, and direct investment, to galvanise the key stakeholders. It also hinted that if these incentives and attempts were to fail, it would have no hesitation recommending that they were backed up by the possibility of direct regulation.

2.1 Recommendations and key issues contained in the report

The House of Lords refutes the Government's continued insistence that the responsibility for personal Internet security ultimately rests with the individual.

It identifies actions for the government to undertake, a selection of which are summarized here under four main categories:

Areas for research:

- Help develop a leading reputation for academic research on IT Security. (Report Finding 2.36)
- Research into alternative network architectures to inform the incremental improvements to the existing network that will be necessary in the coming years.

ISPs:

- Engage with the network operators and Internet Service Providers to develop higher and more uniform standards of security within the industry. (3.67)
- Remove the 'mere conduit' immunity once ISPs have detected or been notified of the fact that machines on their network are sending out spam or infected code. (3.69) (VoIP excluded 3.7)

Protection of personal data:

- Reconsider the tariffs for the whole of the data protection regime, while also addressing resources and enforcement procedures as well. These should include the power to conduct random audits of the security measures in place in businesses and other organisations holding personal data. (5.57)
- The steps currently being taken by many businesses trading over the Internet to protect their customer's personal information are inadequate. The refusal of the financial services sector in particular to accept responsibility for the security of personal information is disturbing, and is compounded by apparent indifference at Government level.

Action for other regulators:

- For Ofcom, not only to co-sponsor the Get Safe Online project, but to take responsibility for securing support from the communications industry for the initiative. (6.47)
- For the Home Office, without delay, to provide the necessary funds to kick-start the establishment of the Police Central e-crime Unit, without waiting for the private sector to come forward with funding. (7.78)

2. Government response

The following points are selected from the Government reply to the House of Lords Report on Personal Internet Safety.

Research:

The Engineering and Physical Sciences Research Council (EPSRC) and the social and economic aspects to the Economic and Social Research Council (ESRC) have already established links to encourage, and mechanisms to fund, multidisciplinary research. The joint research programme will enable UK industry, universities, local authorities and

other research and technology organisations to work in collaboration to address key research challenges in ensuring privacy and consent in next generation systems.

The scale of the activity is dependent on the outcome of the current Spending Review.

ISPs:

The Government accepts that the ISPs have an important role in preventing security problems for users. ISPs cannot remove all their problems but there are things they can do to both optimise the ability of their networks to filter bad traffic – accepting that there are technological limitations to this – and have a relationship with their users that promotes responsible behaviour.

There are many ISPs that have shown innovative and committed approaches to solving these problems but the government have agreed that there is a need to both look for a way of identifying what a customer has a reasonable right to expect and ensuring that ISPs who meet that expectation can clearly indicate it. This work will clearly need to consider preventing the transmission of bad traffic from customer machines into the ISPs' networks.

There is an assumption in the report that ISPs do not take appropriate action against compromised machines that are serviced by their networks. The Government does not believe that this is completely true and, indeed, evidence to the Committee made clear that the leading ISPs set user terms and conditions that enable them to isolate machines identified or notified as causing problems. It is in the interest of the ISPs to take such actions. As said elsewhere in their response, the Government believes that the industry can do more to identify and aspire to best practice in this area. The Government believes that this holds out more prospects for innovative solutions than impractical solutions about changing liability models.

Personal data:

The Government believes that the current legislative and enforcement regime surrounding personal information is proportionate and provides a strong incentive to appropriate action by companies.

Other regulators:

Ofcom, the Home Office and other bodies will make full replies detailing their collaborations to enhance protection of the individual.

The Government would draw the Committee's attention to its recent initiative on establishing a Claims Tested mark which provides assurance to purchasers of security software and services that the claims made for the product in terms of functionality have been independently tested for their veracity.

3. Byron Review

In October 2007 the Prime Minister announced that the Government had asked Dr Tanya Byron to review evidence on child safety, to assess the effectiveness and adequacy of existing measures and look at how to enable families to manage the risks associated with, among other things, using the Internet.

The review is a cross departmental effort by the Department for Culture Media and Sport, Department for Children Schools and Families, Home Office and BERR. Its main features are:

- It will not be focused on broadcast media, but will look at all areas of games, user generated content, and all Internet access
- Volunteers are asked to come forward to contribute to the study
- There will be road shows for parents
- Stakeholders are invited to make their submissions by 30 November 2007

4. Internet Governance Forum

Nominet has been engaged in a number of initiatives this year to promote awareness and engagement in the IGF amongst UK stakeholders.

In October, Nominet offered workshops to draw out the opinions of a wide range of stakeholders on the four IGF themes: Access, Diversity, Openness and Security. The Security workshop, chaired by Lord Erroll, received an overwhelming level of response and was the most heavily subscribed.

Of the IGF themes, security was identified as the single-most important issue to UK stakeholders. Generally, the participants' view of the current situation was rather bleak. See appendix for a summary of the feedback from the security session.

Outcomes and feedback points will be available on the Nominet web site shortly.

At the same event, we announced the winners in our Best Practice Challenge. The aim of the Challenge was to recognise organisations, groups or individuals that have worked to deliver a safer, more accessible, diverse Internet experience.

We will be sharing these examples of best practice and the outcomes of our UK IGF stakeholder workshops with the international community at the IGF in Rio.

5. Relevant Policies

Nominet has a range of existing policies designed to build and enhance trust in the Internet:

- a. Raising Industry Standards (September 2006)
- b. Policy on Phishing (July 2007)
- c. Policy on illegal domain names (May 2005)

6. The PAB's views

In view of the comments contained in this paper, and the role Nominet plays in the management of the .uk domain name infrastructure, we present a set of general questions to develop Nominet's industry response:

1. What is the PAB's opinion of the statement "*confidence in the Internet could be destroyed*"?

2. What would be the impact on .uk, Nominet and its members' businesses in the event that there was a loss of public trust in the Internet?
3. What changes to the regulatory environment could have a significant impact on .uk, Nominet and its members?
4. What policy areas need to be investigated by the PAB that would enable Nominet to increase public confidence in the Internet in the UK?

In order to inform the debate further, we would like to invite Lord Erroll to present the view from the House of Lords Committee at the January 2008 PAB meeting.

Appendix: Feedback from the Security session, 11 October 2007

- The most important issue to UK stakeholders.
- Need to protect the network as an entity in its own right.
- Improve law enforcement collaboration (especially cross-border).
- Education of end users.
- Shared responsibility for security – not realistic to expect end users to do it all.
- Criminals believe that crimes committed on the Internet are risk-free.
- Law enforcement resources are limited.
- More effective authentication processes are required, but privacy needs to be protected.

Of our experiences in the UK, which would we like to share with the international audience?

- Role of ISPs in the security of the network, and the information that travels over it.
- Need to develop effective trust relationships that are soundly based.
- How do we reconcile fundamentally different national approaches (e.g. notions of privacy and acceptable behaviour)?
- Don't just focus on technological answers.
- Resist pressure for "irrational" action.
- The UK should take a stand – and a lead?
- Examples of UK "best practice" to take to the world.

In the area of security, what would make the IGF magic or tragic?

Magic?

- An organisation like a "digital Interpol".
- IGF should be a meeting point for people & organisations seeking to address criminal problems faced by the Internet.

Tragic?

- The UN takes over governance of the Internet. Any attempt to remove the flexibility of the network.