

Policing the Internet

Democratically accountable partnerships or self-protection groups?

A contribution to debate at the
Internet Governance Forum 2006

www.eurim.org.uk

THE EUROPEAN
INFORMATION
SOCIETY GROUP

EURIM



1 Who are we?

EURIM is a UK based Parliament-Industry Group. It brings together politicians, industry and officials to identify and progress realistic consensus-based policies in areas that are not well addressed elsewhere - usually because they cross political and organisational boundaries. This leads to fragmentation of initiatives and confusion over objectives and responsibility for action as well as over what is practical. Debate over the need to greatly improve the safety and security of the Internet goes back more than a decade to when it first began to be used for business and consumer purposes. EURIM has been looking at the issues for over five years and its papers and recommendations to date are available at www.eurim.org.uk. The scene has however changed in recent years. The proceedings of the Oxford Internet Institute conference *Safety and Security in a Networked World* (summary attached as an appendix) provide an excellent snapshot of the state of debate last year. Since then, however, the incidence of malware and cost of e-crime have escalated sharply. This paper focuses on the contribution that the Internet Governance Forum and its participants could make and the actions it should take.

2 The scale and nature of the problem

The Internet is a great force for good, but like all great forces it can also be misused. Over 10% of mankind is now on line, but so are at least 10% of the world's criminals. The scale and sophistication of malpractice, using the Internet to automate the identification and exploitation of prospective victims over the converging media (fixed and mobile, voice, data and video) is increasing dramatically. So too is the use of the Internet and mobile communications at every level of anti-social behaviour. From teenage gangs to international terrorism, from text-bullying, on-line paedophile grooming and cyber-stalking through impersonation, fraud and extortion to sophisticated attacks on critical infrastructures (especially payment systems), delinquents and criminals appear well ahead of law enforcement in their use of new technology. In some countries the majority of all investigations, including those into traditional physical crime, may entail securing and analysing potential digital evidence, on the computers, personal organisers or mobile phones of victims and suspects, or from surveillance camera footage that might have covered relevant locations.

The actual impact of e-crime is unknown, because it is so hard to report incidents to anyone who will take notice, but the impact of phishing and spam and the growing publicity for the consequences of fraud and abuse, harms confidence in the Internet as a safe place to do business, let alone for our children to learn and play. Those who wish to promote and enhance the socially inclusive use of the Internet for all mankind must take the issues very much more seriously lest inaction leads to a collapse of confidence, whatever the actual incidence of harm. But we must also guard against over-reaction and displacement activity that diverts time and effort from that which is worthwhile and can do more harm than good.

3 The disparity of Public-Private Resource

Business computer users are spending billions to protect their systems and those of their customers. By contrast few nations budget more than a couple of tens of millions for all their computer crime prevention and investigation operations, including child protection and anti-terrorism, added together. The computing, communications and financial services industries employ tens of thousands of electronic security experts to protect themselves and their customers. At the same time law enforcement services around the globe have barely a couple of thousand officers and support staff with experience of digital investigations in total. Meanwhile training, funding and career issues mean that in some nations more former policemen with experience of running major computer crime investigations are now working for industry than in their law enforcement agencies.

Those tasked with protecting the most vulnerable and with enforcing the law are playing catch-up. They are overwhelmed by the scale of criminal and anti-social activity that may require computing or digital evidence skills to investigate. There is confusion as to how (and to whom) on-line incidents should be reported and a reluctance to make it easier to report, lest the result distorts police performance targets, whether or not the latter are in line with public needs and expectations.

Responsibility at the national level for educating, advising and supporting those at most risk crosses departmental and agency boundaries and authority over budgets, courses and curricula is fragmented. At the international level there is much talk but little action, except between those who have met and trust each other, despite the processes they have to use. Meanwhile on-line criminal activity indicates significant co-operation across national and cultural, let alone “family” or “gang”, boundaries.

Industry (both users and suppliers) is beginning to co-operate, including with the formation of national and international professional groupings to educate and assess those who can be trusted. The time has come for similar co-operation across law enforcement boundaries (local, regional and national agencies as well as international) with the aim of also greatly improving co-operation with those in the private sector who are working to protect their customers as well as themselves.

4 Crime Prevention

Electronic security is a multi-billion pound global industry, albeit with much fragmented and duplicated effort plugging vulnerabilities after the event or responding piecemeal to the global attacks of a limited number of criminal groupings and their hangers-on. It should be possible to give users, large and small, far better protection for the same spend by enabling and encouraging co-operation between currently competing suppliers. It is said that the “technical reasons” that ended the attempt of the Internet Engineering Task Force to transform the security of the Internet with greatly improved end-over-end authentication services, were to do with conflicts over the licensing of Intellectual Property Rights not problems at the technology level.

If correct, that is an indictment of those responsible and of the system that enabled this to happen. But we cannot wait for reform of the global IPR regimes. Instead we should use a mix of commercial, political and moral carrots to ensure fair rewards, both recognition and financial, for those who contribute to the thinking and innovation necessary to make the Internet safe for use by ordinary human beings, plus sticks for those who do not, or who actively prevent progress, beginning with public exposure by their peers.

Equally we do not need to wait for the re-engineering of the Internet with new generations of routers, browsers, operating systems and addressing systems in order to make serious progress in internet safety, security and crime prevention. Improving the quality and relevance of the advice and guidance on offer could make a massive difference. Most ordinary human beings are baffled by the documentation and “help” routines currently on offer. These move rapidly from the simplistic and patronising to that which requires Masters Degrees in Information and Computer Science to locate and understand. And even then the tools that users are expected to install and trust appear to spend much of their time fighting for supremacy within the system - identifying each other as threats to be removed and expecting the user to adjudicate.

We need much greater co-operation to identify and promote the best practical advice available, in language that ordinary human beings can understand, and to ensure that reputable security products and services recognise each other and co-operate. That process includes giving much greater priority to computer security and Internet safety in mainstream ICT education and training at every level, from schools through further and higher education, as well as adult courses on the use of IT, to the design, implementation, operation and support of systems in ways that reduce opportunities for abuse.

It is almost certain that crime-prevention awareness and education is an area where incentives will be very much more effective than penalties. The core task is to persuade security suppliers to put at least 10% of their current marketing spend and major users to put a similar proportion of their security budgets into co-operative ventures to transform awareness and competence at every level – including among their public sector customers and partners who are often among the most complacent and vulnerable.

One of the best ways of promoting such co-operation is almost certainly a series of awards for “best of breed”, to give the oxygen of publicity to good practice and encourage others to join in or do better.

ACTION: the Internet Governance Forum should organise and promote awards for:

- co-operation between law enforcement, industry and others in organising crime reduction and prevention partnerships to support and serve Internet communities, including on a non-geographic basis;
- producing, promoting and distributing advice and guidance for target audiences (children, parents, teachers, small firms, end-user staff in large organisations etc.);
- products and services with plain language, intelligible and useable documentation, websites and help processes related to what the user experiences (technical merit, innovation and excellence are not enough);
- individual contributions to making the Internet a safe and secure environment.

5 Non-Geographic Reporting

The near impossibility of reporting incidents to someone who will accept the report, let alone help the victim obtain redress, means reported losses due to e-crime are minimal even though surveys indicate massive costs. A consequence is regular proposals for new reporting mechanisms to replace those that are not working. Most of these look set to be a waste of effort because they do not address the root cause of failure. No one has any incentive to report incidents other than to those who will help them handle the consequences or to obtain redress or retribution. Meanwhile few wish to receive reports to which they can respond only by admitting ignorance or inability to help.

Individual phishing attacks may not justify the use of scarce investigative resource but analyses by the leading global private sector monitoring organisations indicate that a large proportion of malpractice originates from a relatively small number of loose-knit criminal networks, many of whose members could be tracked, traced, removed and blacklisted (the e-death penalty) by the main communications operators for breach of service conditions. There is a need to bring the current proliferation of fragmented local and national reporting operations together into international reporting networks that cross public-private boundaries and collate and route information to those who are in a position to take action.

ACTION: the IGF should call for proposals for new regional law enforcement reporting agencies to be replaced by proposals for secure international information exchange. These should involve reputable private sector communications monitoring operations to enable (for example) collated analysis of phishing and malware incidents to be passed rapidly to those able to block attacks and blacklist the perpetrators for breach of conditions of service - not just to record data for use in next year's budget submission.

6 Non-Geographic Policing

Law enforcement lacks the capacity to respond effectively to more than a fraction of currently reported incidents. The Internet has been described as the Wild West without six guns. Law and order was brought to the Wild West by gunmen hired by the railways, banks and citizens' committees to protect themselves, their customers and their communities. A great many agencies claim to regulate content over the Internet but most effective action against malpractice is organised by the major internet service, e-commerce and on-line banking and payment providers - to combat their common enemies and to protect and re-assure their shared customers. They need to be further encouraged and enabled to act rapidly and decisively, in co-operation with law enforcement agencies, to protect the small firms and consumers whose confident use of on-line transactions and information services is essential to the growth of e-commerce and e-government.

We should have no illusions as to who will contribute the majority of effort and resource. Recent high profile investigations of international paedophile networks show how the resource available to law enforcement can be swamped by the capacity of e-crime to generate very large numbers of incidents and information. The only way of handling the load is to involve industry staff and civilian volunteers, working to standards and procedures commonly recognised across public and private sectors, including internationally, as part of joint crime prevention, reporting and investigation operations.

There are many models around the world for such operations: from police "reserves" and "special constables" through accredited security firms and specialist units to industry-funded police forces, such as the British Transport Police. The challenge is to create frameworks that enable local and national operations to co-operate across jurisdictional boundaries, including with nations where the security and probity of law enforcement cannot be taken for granted. This places limits on the ability to use official channels. The routines established by the insurance companies for handling piracy on the high seas and by the financial services and freight forwarding industries for handling international "disputes" are therefore apposite.

ACTION: the IGF should call for a significant proportion of the funds currently being allocated for "research" into the scale and nature of e-crime or into security technologies to be used for documenting and publicising current processes for organising co-operation across local, regional and national boundaries and how these might be applied in the on-line context.

7 Child Protection as an Example

The partnership routines being established by the Virtual Global Task Force provide a model for what can and should be achievable. These have greatly improved not only the ability of children to report what is happening to them to someone who will understand and take notice but also the ability of law enforcement to rapidly track, trace and identify would-be predators. The task force would, however, be very much less effective without the contributions of the industry "partners": from the "Report Abuse" buttons on widely used websites to technology support for reporting systems and investigation, including tracking and tracing

communications. Such partnerships need to be imaginative as well as quality controlled. Thus the UK partners include the Football Association as well as Microsoft, AOL, BT and Vodafone.

The result is far more effective education and protection than can be seen in nations that talk about child protection and seek to extend legislation covering television advertising to the Internet, under the guise of regulating video-streaming as a TV like service. It is interesting that some of the latter have rigid divisions preventing co-operation between law enforcement and industry in parallel with outbreaks of public concern (from press campaigns to mass demonstrations) over the supposed cover-up of widespread child abuse.

ACTION: the IGF should call for national governments (especially those of the G8) to facilitate national and international co-operation between law enforcement and the Internet community, especially the commercial providers who provide services to the majority of users, to protect on-line communities from criminal behaviour and abuse, using lessons from the formation of the Virtual Global Task Force.

8 The role of government(s)

There is much talk today of cross-border co-operation but debates within regional groupings like the European Union over applicable law, including "country of origin" versus "country of destination", indicate that little more progress is likely over the next decade than has been achieved at the inter-governmental level over the past century. If one then looks wider at the clashes between Roman, Common, Islamic and Asiatic legal traditions, let alone cultural and political differences, that lack of progress become less surprising. Meanwhile the private sector has had routines for international co-operation for over a thousand years.

The best selling book and subsequent film, "The Da Vinci Code", were largely inspired by the mythology around the break up of one such network: that which enabled the Knights Templar, the Venetians, the Byzantines and the Arab/Jewish networks of the Middle East to co-operate in safely transmitting funds from the Orkneys to Jerusalem, until the King of France reneged on his debts. Today such routines are not only global but have evolved via routines to handle piracy on the high seas or accidents in space, with adjudication under whichever law and in whichever location the relevant service contract(s) state.

The global financial services, international payment and freight forwarding operations of today have evolved similar routines for handling cross-border transactions between customers operating under very different legal and regulatory systems. Some of these are already integrated into seamless on-line networks, operated from a handful of regional hubs, with local access under the legal and regulatory regime of the nation from which access is being made: country of destination.

The Internet has a different tradition with regulation largely based on country of origin and remarkably little interference from the government of the nation that, until very recently, originated most of the traffic. Other governments around the world are, however, loath to leave the policing of the Internet to a cartel of global commercial players operating under the governance of ICANN, the Internet Engineering Task Force or W3C, let alone the ITU, IPU or other international bodies. But if that is to be replaced by something better, not mere anarchy, they must greatly increase the resources they provide to their domestic e-crime law enforcement operations and develop very much more efficient routines for cross-border co-operation - using the expertise of the major commercial players in working with and through local law enforcement around the world.

This will not be easy and those in the West who argue that such routines must be democratically accountable should remember that some of Cicero's greatest speeches on republican virtue and civil liberties were actually in support of the tyrants and organised crime bosses of his day. Inter-government agreement on anything that is effective and meaningful is unlikely other than between states that share political, cultural and legal traditions. Even then it cannot be taken for granted.

ACTION: instead of lobbying for global legal frameworks the IGF should support the successful work of groups like UNCITRAL in producing model laws for piecemeal adoption and consider a UN Treaty on Technical Assistance to enable smaller states and organisations to make better use of the legal routines already well established for handling international trade disputes.

9 Getting our priorities right

The creation of effective frameworks for global co-operation, using the contractual terms of the Internet service suppliers to protect paying customers and remove miscreants, should have a higher priority than the creation of new regulatory and governance routines. Unless well judged, the latter not only divert resource from addressing known malfeasance but can create more vulnerabilities than they remove. For example one of the largest insider dealing operations in a western nation was only possible because new regulatory rules had enabled a compliance officer to bring together staff from across the internal security boundaries of the organisations involved. Meanwhile Sarbanes-Oxley mandates not only expensive paper-chases that would not have prevented Enron but also anonymous whistle-blowing routines of the type made illegal in France after World War 2 because they had cost so many lives at the hands of the Gestapo and Milice. Requirements to give regulatory or law enforcement staff the ability to cross the security barriers of financial services players or to demand the retention of vulnerable data, are obvious examples of how well-intentioned initiatives can cause responsible organisations to move key functions outside the jurisdictions concerned. The cost of ill judged regulation is not just money but can be increased risk, personal as well as financial, if it makes it harder for reputable service providers to provide realistic protection for their customers.

ACTION: the IGF should call for all proposals for new regulatory regimes, national or regional (e.g. EU) to be subjected to full systems review and impact analysis to check how they will achieve the objectives stated and at what cost to legitimate business, given current and prospective technologies and business models.

Much is said about the need to build trust between those who have never met. But even the most primitive tribesman knows better than to trust someone who wants to know his name or take his photograph for no obvious reason or benefit. Current research, albeit mainly from the United States and Canada, is that Internet users may not like their bank but they trust it. Meanwhile they trust the on-line security of their government nearly as little as that of their Internet or E-Commerce service provider.

Well-publicised stories of the theft of files of personal details from both public and private sector to aid impersonation and fraud and the current plagues of phishing and spam mean that consumer trust in on-line transactions is fragile and needs reinforcement. The European E-Commerce directive requires those trading over the Internet to also provide physical contact details. Many trading sites not only fail to do so but the registration details obtained by a "whois" enquiry are, if available at all, often those of the service supplier who built or sold the site.

Given the growing use of the Internet for consumer and political research of all types, it is surprising how little consumer research has been done into what Internet Service providers' customers expect, would like, or are willing to pay for. There is a common attitude that the Internet is too complicated for customers to understand and decisions should therefore be left to industry or government. But many consumers wish to receive anonymous e-mails no more than they wish to receive anonymous letters or phone calls. Why should they not be able to ask their Internet Service provider to automatically return these to sender? The consequences are profound, but has the time not come for Internet service providers to listen to their customers?

We urgently need more open, inclusive, balanced and focussed debate, leading to relevant and effective action to close the cyber-community policing gaps of today. That debate must include current and potential victims, not just self-appointed experts of industry and academia, let alone law enforcement officers and politicians seeking to protect the past from the future.

ACTION: the IGF should call for more consumer research into what Internet users (business as well as consumers) actually want and from whom: including by way of trade-offs between price, facilities and security before calling for government intervention, if at all.

But time is not on our side and the one topic on which there appears to be global consensus on the need for effective action is that of child protection, including protecting children from each other as well as from adult predators. It therefore provides the ideal point of leverage for opening up debate at the political level, focusing on that which will actually help educate and protect those most vulnerable and at most risk.

ACTION: the IGF should test the effectiveness of mechanisms for international co-operation to enhance confidence in the Internet as a safe place to work, learn and play by supporting programmes to educate children, parents and teachers in the safe use of the Internet and to track and trace child abusers.

Appendix

Safety and Security in a Networked World: notes from the Oxford Internet Institute conference on Balancing Cyber-Rights and Responsibilities

Introduction

This is a quick attempt to summarise the discussion at an international conference which brought together players from academia, industry, regulators and law enforcement, from around the world, for a holistic debate, looking at issues of Internet safety and security together. The author does not agree with all the points made but has attempted to prevent his own prejudices from distorting the accuracy of the summary (including the paragraph below).

New challenges required a level of sophistication in users that they do not yet possess. Many questions remain, including what level of risk is acceptable to various categories of users, how users use the technology, and what combination of enforcement and empowerment is most likely to increase safety and security. Much activity is under way that has not yet led to action. There are significant disconnects (priorities and understanding) between software and service providers, their customers (whether corporate or consumer) and governments (whether politicians, regulators or law enforcement).

1) The Secure Future of the Internet and how to stop it (first keynote)

- The Internet Engineering Task Force principles were:
- keep it simple: leave everything complicated to applications
- keep it open: do not presume to predict what can/will be practical in the future
- decisions by consensus of a technical meritocracy (hum not vote)
- assume people are reasonable
- assume people are nice

But these principles have been overtaken by a fight between intellectual anarchy and property rights owners as commercial billionaires seek to sell “killer applications” to mass market consumers. In consequence the IETF has had to give up on trying to address security and we are reliant on the forbearance of the spammers to do no harm while they borrow our spare processing capacity and bandwidth for their own purposes.

The possible solutions are

- more alert users: but is this tenable “when the Pinkertons (i.e. competing security products and services) start fighting each other on your machine”?
- more alert PCs: handing control to a third party who will decide what you can run
- more limited PCs: including the new generations of Internet appliances
- a more alert Internet: but the concept of deciding what traffic can be carried for whom (e.g. quarantining supposed zombies) is anathema to the Internet traditionalists

There is a need to separate the Internet ethos from Internet governance and enable users to decide what software they trust via a representative Internet community that is capable of also handling the issues of competition and anti-trust

2) Achieving a balance: National priorities, International problems (first panel)

46 nations have so far adopted the Council of Europe Convention on Cybercrime (including Canada, Japan, South Africa and the USA). The UNICTRAL model laws on E-Commerce and E-Signatures are equally successful (e.g. 10 members of ASEAN have adopted them though only two are members). Problems of identity/authentication and validity/enforcement are because of the need to operate across both hierarchies and webs of trust.

Progress is because organisations like the World Bank and EBRD have funded experts not only to attend meetings but also to help poorer nations implement the results. Success is driven by economics and reaction to need. Attempts to predict what will be needed (e.g. certification regimes) have killed progress where they have been tried.

Surveys of political elites indicate that parents place action on child pornography as the top Information Society priority in Europe, second in the US and third in Asia. The disagreement is on how to respond. The traditional Internet view is to leave it to parents. Most of the world believes that "government should..." In the US there is a view that "anyone but government should". Across the EU there is the adoption of "co-regulation" to head off government intervention. The convention on the rights of the child has 132 signatures (more than any other) but not that of the US, which has different priorities and the First Amendment. Only 144 of the 35,000 US customers of Landslide Productions have been charged (mainly via sting operations, because delay had made it impossible to legally examine their systems for evidence). Different legal processes enabled over half the 7,200 UK customers to be arrested.

The US has rules. The EU has guidelines. China bans what it does not like. Singapore has discovered the value of "regulatory arbitrage" to attract those who wish to do business in all parts of the world. ID theft has cost 20 million Americans over \$50 billion. Internet usage is growing but so is the proportion of users switching off (8% in 2005). Bad experiences and fears over safety and security are a prime reason.

3. Balancing privacy and security (break out)

The supposed anonymity afforded by pre-paid mobile phones may not be achievable in practice. If so, registration to avoid anonymity is unnecessary and policy debate might be more fruitfully directed towards wider concerns about the use and disclosure of communications traffic data from call detail recording and various forms of circumstantial evidence, such as CCTV footage'. The use of digital evidence was illustrated by a murder in Sweden, where the convictions relied on SMS messages. The attempts by the Trusted Computing Group to resolve the antagonisms around privacy, first amendment rights and innovation relies on trusting that the state, ICT industry and corporate interests who develop the trusted hardware have the user's best interests in mind.

4 Experiences of self and co-regulation (break out)

Who should it apply to, how should we allocate accountability and should we have different regimes for different applications? The Australian model is the most developed, driven by the need to head off political intervention. The government provides the framework, the industry (200 companies) drafts the rules and the regulatory authority approves the rules and ensures compliance. ISPs must provide filter tools, notice, information and newsgroup takedown, age limits, notifications to the police and a safety button link to consumer information. The ACMA receives complaints, which are evaluated and used to update lists supplied to filter companies. The use of filters by parents is optional. Less than 20% use them. Filters only block accidental access. Those seeking material change route or communicate by peer to peer.

5 Protecting Children: evaluating new initiatives (break out)

The Internet constitutes a 'new virtual reality' with its own rules and language, which provides a 'supportive context in which the child abuser is no longer a lonely figure but part of a larger community that share the same interests'. Children do not necessarily apply their 'stranger danger' awareness in the real world to this cyberworld, making a distinction between 'strangers' and 'virtual friends'. The most 'extreme, aggressive and reprehensible' types of Internet behaviour are found in P2P facilities. The criminal law supports victims of cyberbullying if the threats are seen to have an impact in the real world but wary of opening up a flood of legal action in cyberspace. Most cyber-bullies have themselves been bullied in the real world and about 80% of cyber-bullies know their victims. The close link between real and cyber-bullying has important implications for schools.

6 Security in cyberspace: room for a new legal tool set (break out: papers on web)

Five botnets generate 90% of phishing attacks. Denial of service attacks take up 25% of the time of the NHTCU in the UK. Those creating and managing them are said to be off-shore and/or not worth suing. Given the inability of law enforcement to address the problem, those affected might consider using civil law (most of the participants in this session were from US law schools) to sue the zombie-owner, ISP or the provider of the vulnerable operating system/browser etc

There is a lack of incentive for users to patch their systems to prevent them being hi-jacked and a lack of willingness on the part of ISPs to notify and/or quarantine customers whose systems had been taken over. An attempt to do so in the US had sparked a vitriolic response. Many security routines are unfit for purpose (e.g. instructions to turn-off the firewall in order to download ... thus enabling your systems to be infected even if they were not already) and the software suppliers should be sued instead.

The IETF exercise to improve security and authentication was abandoned because of irreconcilable clashes over intellectual property rights (including licensing availability and charges) not technology problems. It was therefore suggested that the political threat of anti-trust legislation or compulsory licensing might be more relevant than further research. Either way the implications are profound.

7 Terrorism, online extremism and the role of ICTs (break out)

The considerable technical expertise within terrorist groups is backed by a sophisticated use of the technology for propaganda, luring new recruits, fund raising, information provision and other communication activities. Groups like the Tamil Tigers have been using the facilities of Western (US and UK) universities to run web-based recruitment and publicity operations for over a decade. Their techniques for attracting and influencing segmented audiences (including journalists) are more sophisticated than those of many government departments. For example, the Tamil Tigers have a site in English which is relatively sanitised, but a more full-blooded one in Tamil. Some groups have developed 'anti-terrorist' websites to fight back and public websites can be a point of vulnerability for terrorist groups: but the terrorists are fully aware of this and feel the risk is worth taking.

8 NGO experiences of promoting safe use of the Internet (break out: papers on web)

Many NGOs now have great expertise in ICTs and its implications in their specialist areas. However, those most concerned about the impact of the technology often have to compete hard for attention and resources in competition with other priorities in their areas.

9 Making enforcement work on the national and International Scale (plenary)

The police are in the process of moving from absolute ignorance, through arrogance to the beginning of understanding. Operation Ore was a turning point. The NCS SPOC for Ore is still receiving 300 new cases a month. The Internet is now seen as "just another public space" to be policed. It is an uncomfortable space because there are no boundaries and "big egos" have to be persuaded to forgo sovereignty/control, but it needs overt policing, including via the Global Task force. This has acted on 85 of the 100 reports received to date. The UK centre is multi-agency with a multi-national dimension supported by AOL, BT, Microsoft and Vodafone and has four faculties:

- Information: collation of reports and profiling
- Harm reduction: media teams, BECTA, DfES etc.
- Operations: targeting known predators
- Partnership: including "Child Education Tracking System"

IWF appears to have succeeded in almost wiping out UK hosted websites of child abuse material. The problem is now primarily to block access to those outside the UK. Microsoft's decision to close its chat-room rather than to try to improve safety was unfortunate because the children migrated to less safe spaces. The Irish ISP code for harmful material is the most comprehensive but there is considerable commonality of approach internationally, whether the complaints are channelled via the ISP, an ISP association or an independent hotline.

10 The challenges of rolling out e-government (break out: papers on web)

While 24% of the UK population has now carried out at least one e-Government transaction this was usually only to obtain information. The usage of UK government websites is half that of the Netherlands, Canada, Australia or the USA and a third that of the private sector. UK users were less likely to use the Internet (as opposed to other sources) to find information on government and more unlikely to trust it for a transaction. Ten years ago the UK had a number of well-signposted on-line information services. These were then restructured around life episodes so that, for example, you could only obtain a list of local GPs via the route for "having a baby". Government departments lack motivation to provide on-line services that will increase demand. Both usability and security compare unfavourably with most of the private sector. There are signs that some Government initiatives are driving a change in the nature and scope of citizenship, and in Government-citizen relations, e.g. strong e-authentication using the Government Gateway. How might the involvement of credit reference agencies as trusted intermediaries affect access to e-Government services? Internet safety and security needs buy-in at the policymaking level. While there is increasing recognition that secure data sharing is necessary for added value, citizens need reassurance that obligations to safeguard privacy will be honoured, perhaps involving some form of consent. Cyber-rights and responsibilities also need to be balanced, perhaps requiring citizens to sign up to a compliance regime.

11 Weighing up the risks and benefits of children's use of the Internet (break out)

The 'UK Children Go Online' www.children-go-online.net research findings about issues within families, was a central discussion focus. Other studies in the UK, Spain and Greece of the attitudes of parents and children to Internet risk concluded that much Internet safety advice to children does not take sufficient account of the emotional context in families and is likely to be ignored by children who feel that an area of independence is being thwarted.

12. The challenges of cross-border transgressions and enforcement (break out)

Underlying political, cultural/philosophical and institutional differences between the US and Europe determine outcomes from transatlantic negotiations over privacy and trans-border data flows. Compromise was reached on the 'Safe Harbor' e-commerce guidelines but no compromise was reached on Terrorism and Passenger Name Records (PNRs) requirement resulting from the US Aviation and Security Act. The different outcomes can be understood only by understanding the broader contextual issues. Any global identity system should be based on a 'cybersecurity banner' that reads: "maintaining the freedom of our society is our first priority". The Internet has opened opportunities for moving from a 'reactive' law enforcement model to one that privileges risk management over detection and punishment. and involves a mix of public and private organisations.

13 Cybersecurity and the New World Enterprise (key note)

Security is everyone's responsibility, and without security, there can be no guarantee of privacy. However, security software is too complex to install, update, understand and operate for many users, and good practice conflicts with easy access to the Internet and associated services. 50,000 zombies in a single attack is now "proven". 840 million Internet users world-wide in 2004, now estimated to be over a billion – a lot of 'open doors'. Major issues on security, including with biometrics. How do you revoke a thumb? Two-factor authentication and a good business model will enhance security, but we need secure code to minimize vulnerabilities.

14 Privacy, Trust and Security (plenary)

The cost of security includes inconvenience and lost transactions (too complex so gave up) and is rising because of a mix of government/regulatory creep, consumer luddism and ICT self-interest. Who invades my privacy (inquisitive friends, loyalty cards, press, government, criminals etc.) and why? Who will pay for security and privacy? Law enforcement wants its security to be unbreakable but to be able to break that of others. The codemaker has a strong advantage over the codebreaker, but a system might be broken through a management fault. Most voters would compromise on the Ben Franklin position that those who would sacrifice liberty for security deserve neither. But where on the slippery slope would they wish to stop?

There is a consequences matrix:

	Desirable/Intentional	Undesirable/Intentional
	Desirable/Unintentional	Undesirable/Unintentional

Only 0.6% of consumer complaints to OTELO (one of the two UK Communications disputes resolution services) have been about privacy, and even these reflected suspicion about the provider rather than civil rights or criminal activity. Fraud perpetrated using mobile phones and organisers is expected to increase, in large part because consumers do not understand the capabilities of the technology, or the associated risks. Education may work better than regulation for some problems, but many services and products are unfit for purpose.

15 Broadening our understanding of online risks for minors (break out: papers on web)

The mainstream approach to safety over the Internet appears to be, at best, irrelevant and, at worst, counter-productive. Those who are timid in their use of the Internet are at little risk. As understanding of the Internet increases they become more confident, take more risks and place themselves in greater danger: including by producing and exchanging explicit material (sexual and/or violent) featuring themselves and their peers, cyberbullying or joining chat-rooms that exist to encourage suicide/fasting and abuse between children of different ages. 95% of adult predators do not falsify their age. Children's attitude to risk is very different to that of adults. Is the Internet accelerating problems that part of "normal" teenage life (physical or fantasy)? One of the virtues of Internet use is that it *can* make it easier to identify those at risk and also those from whom they are at most risk.

Those most likely to seek out “undesirable” content over the Internet are teenage males, alienated from parents, school and religious community. Most of what they find is via groups of friends, unmonitored chat-rooms and peer to peer, using a variety of increasingly mobile media. Filtering what is accessed via the home or school PC is of limited relevance.

16 Securing Networks (break out: papers on web)

We need security against intrusion from the State, and from the ‘bad guys’. Privacy-enhancing technology is one way in which we can protect ourselves, by balancing privacy and security. Intrusion detection techniques could also reveal patterns of illegal behaviour generated by both manual operation and machine. However, the weakest link in any system often resides in policymaking, which can also often result in unintended consequences.

The number of interfaces, and therefore opportunities for illegal access, increased dramatically when the PC supplanted the mainframe. Hackers now have a vast number of targets, but are unlikely to face any punishment, and targets have come to accept the inevitability of attack. Meanwhile, the threat spectrum is changing from ‘script kiddies’ increasingly to organised crime, and the escalating spiral of hacker attack and reactive defence needs to be broken. This inequality of accountability requires the introduction of the principle of redress, and a change of thinking, replacing the ‘arms race’ spiral by ‘network forensic readiness’ which will collect credible digital evidence. The ‘good guys’ must work together to solve the problem, not just work independently from their own perspective.

17 Developing prevention and enforcement against a backdrop of international difference (break out)

‘Child pornography’ has been defined in different international and national legal and regulatory contexts. The problem of child sexual abuse has led to a tendency ‘to stretch international standards and national criminal laws to capture increasingly marginal material’, which could ‘undermine the consensus on the appropriateness of laws prohibiting child pornography or diminish the force of criminal sanctions’. A greater focus on core serious offences about which there is common international agreement, such as images of criminal sexual assault, is therefore recommended.

The US i-Safe programme included assistance for an event on Intellectual Property Rights addressed by the US Attorney General in Los Angeles. The DOJ Press Release is at:

http://www.usdoj.gov/opa/pr/2005/April/05_ag_221.htm

The Court TV version ☺

http://www.courtvtv.com/choices/activate_your_mind/?sect=2

And the story as told by the LA Times was: *Students Do Not Share Gonzales' View on Piracy.*

<http://www.latimes.com/business/la-fi-piracy29apr29,0,3250364.story>

In break-out sessions those students whose parents worked in Hollywood claimed that their parents supported piracy because the more their work is viewed or heard, the more famous they will be. They did not wish to see an end to their current freedoms on the Internet but agreed that compromise was going to be necessary to ensure those freedoms.

18 Whose Responsibility? (plenary)

The possible approaches include:

- Using criminal law
- Imposing duties on users
- Imposing duties of software suppliers
- A security commons approach involving users, software suppliers and ISPs
- An EU Directive extending the cybercrime convention
- Rewriting the Internet

The more IT literate encounter more risk by being more adventurous

85% want tougher laws on pornography

59% want stricter regulation

75% want more advice for kids

67% want more advice for parents

- The Australian approach is Government/Regulator + Industry + Community
- Violence is a more serious problem than sex
- Software vendors bear a heavy responsibility for rushing products to market with insufficient testing and should be responsible for “egregious holes”.
- The US “total information awareness” exercise was an example of centralised vulnerability with the harm from false positives and consequent delays, diversions and overload resulting in more harm than good.
- Over half of any automated selection is false (negative or positive) therefore human contacts (e.g phone calls) are needed to check. That may be practical for credit transactions but for national security ...

19 Ways forward (plenary)

- If ISPs are to remain “mere conduits” then filtering and making “possession” illegal are the way forward
- Filtering is “so 2003”
- Politicians will interfere. We can therefore expect the growing nationalisation (rather than internationalisation) of the Internet.
- Abusers should be disconnected. If connection is a right then it also has responsibilities
- Rewriting the Net itself (a filtering Internet) may be a key part of the way forward
- The Internet is not fit for children, it was designed for the military and for academics, but it is now a mass market therefore ...
- How do you regulate a cloud?
- Burning the house to roast the pig?
- Proposals must be evidence based (where is the data), modelled and assessed for practicality and likely consequences meanwhile policy makers and parents will muddle through (as they always have).
- What matters most: soft targets (representation) or harmful behaviour (identifying physical abusers)?
- Civil remedies for negligence should be explored more thoroughly (but by whom?), including the activities of “rampant bounty hunters” and the right of self-defence.
- There is a need for much greater co-ordination and accountability of the main players
- Consumers/users are very different and they are usually undemocratic therefore policy must be set for them by an informed elite of professionals, regulators and academics.
- There is a public demand for less vulnerable products and services and if suppliers will not provide these then the causes need to be investigated (? anti-trust)

20 Conclusions

- The entrance to a good University should carry the warning sign: “Beware Dangerous Ideas”: over a Skull and Crossbones.
- There are multiple players, issues and possible responses mixed with emotive responses. Is this a swamp or a fertile area for research?
- We have overcome the resistance to putting cybersafety and security together, now we must move from awareness to education
- How would the people with whom you disagree use your proposed legislation?

Drafted by Philip Virgo, 17th September 2005.

Visit <http://www.oii.ox.ac.uk/microsites/cybersafety/?view=home> for details of who said what.