

Stewardship of Cyberspace: Duties for Internet Service Providers

Melissa E. Hathaway¹

John E. Savage²

Abstract

In today's interconnected world, the Internet is no longer a tool. Rather, it is a service that helps generate income and employment, provides access to business and information, enables e-learning, and facilitates government activities. *It is an essential service that has been integrated into every part of our society.* Our experience begins when an Internet Service Provider (ISP) uses fixed telephony (plain old telephone service), mobile-cellular telephony, or fixed fiber-optic or broadband service to connect us to the global network.³ From that moment on, the ISP shoulders the responsibility for the instantaneous, reliable, and secure movement of our data over the Internet.

Introduction

ISPs come in many forms and sizes and go by many names: the phone company, the cable company, the wireless company, etc. They are the Internet stewards: planning and managing resources, providing reliable connectivity, and ensuring delivery for traffic and services. And while the communications infrastructure security as a whole is generally believed to be robust, recent trends suggest that the networks and the platforms on which Internet users rely are becoming increasingly susceptible to operator error and malicious cyber attack. Therefore, in 2012, should we ask the question, do ISPs *have additional duties to ensure the reliable delivery of an essential service?*

In this article, we expose the gap between ISPs written responsibilities and the unwritten, yet expected ones. Specifically, we define eight ISP duties:

- A. Duty to provide a reliable and accessible conduit for traffic and services
- B. Duty to provide authentic and authoritative routing information
- C. Duty to provide authentic and authoritative naming information
- D. Duty to report anonymized security incident statistics to the public
- E. Duty to educate customers about threats
- F. Duty to inform customers of apparent infections in their infrastructure

¹ President, Hathaway Global Strategies LLC

² An Wang Professor of Computer Science, Brown University

³ Services include: Public-switch Telephone network (dial-up); Digital Subscriber Line (DSL) (usually copper), Asymmetric Digital Subscriber Line (ADSL); broadband wireless; cable modem (cable Internet); Fiber to the Premises (FTTx) (optical fiber); Integrated Services Digital Network (ISDN) (transmission of voice, video, data, and other network services over the traditional circuits); frame relay (wide-area network); Ethernet; Asynchronous Transfer Mode (ATM); satellite Internet access; and synchronous optical networking (SONET) (using lasers over fiber)

- G. Duty to warn other ISPs of imminent danger and help in emergencies
- H. Duty to avoid aiding and abetting criminal activity

The latter duties are helpful in calibrating threats and funding responses to them.

It is important to note that the Internet is radically different from the plain old telephone service (POTS) that has provided voice communication since the 19th century. POTS established a “circuit” or path through the telephone network that remained constant during the communication session. The telephone network operated according to a strict, regimented, set of processes and technologies that provided a highly reliable service, but adapted to change slowly. It did not have an application programming interface (API) to allow for third party access and experimenting with telecommunication services was discouraged.

The Internet operates much differently. Long messages are decomposed into packets that move from source to destination following potentially different paths through the network. This is called packet switching. The Internet also provides a simple interface to communication networks that make it easier for third parties to create innovative communication-based products to connect and access the Internet and providers to introduce a new generation of value-added services and applications. Yet, the *Internet and the communications and services that ride on it, rely on the integrity of routing and naming infrastructures*. These two critical functions are essential to the proper functioning of the Internet.

Routing

The Internet is a *network of networks*. Networks consist of end systems, called *hosts*, and intermediate systems, called *routers*, connected via communication channels. Information travels through a network on paths chosen by a routing process that is implemented by routers. These paths automatically change many times a day, as congestion on one network might make an alternate path more attractive, or if a network has downtime – either intentional or not – so a new path is needed until the preferred path is restored.

Unfortunately, the technology in use today to ensure the Internet is operational is based on trust; it cannot give adequate guarantees that the expected network configuration is the one in place. As a consequence, one ISP can issue an update to another, whether by accident or by design, that will send Internet traffic to the wrong destinations. This lack of trust has resulted in major disruptions of Internet routing and can enable malicious activity, such as monitoring traffic, identity theft, and disruption of commerce.

Naming

ISPs provide naming services to both their customers and other Internet users. Domain names are human-friendly names that are translated into Internet-working Protocol (IP) addresses, for example www.acme.com is a domain name, and 216.27.178.28 is its IP address. People like to use domain names and routers like to use IP addresses. Therefore, a system that converts one to the other was needed. It is what is called the Domain Name System (DNS).

The DNS is the “telephone directory” for the Internet which does this translation. This “telephone directory” is implemented as a hierarchical collection of “servers.” The DNS system was not designed to be inherently secure. When a request comes in to translate, a series of

queries and responses occur until a mapping is found for the domain name in question. When a request is made, the requestor accepts the first response that it receives, and then uses it. Imagine asking a question to a room of strangers, and whoever answered the question first (regardless of accuracy), is assumed to be truthful. This is what the DNS essentially does and this vulnerability can and does often result in end users being misdirected to fraudulent websites on the Internet.

The Domain Name System Security Extensions (DNSSEC) is a set of extensions to the underlying DNS protocol suite that was designed to address this problem, but has not yet been widely implemented by ISPs. DNSSEC uses cryptographically signed messages to authenticate the sender, which ensures that only “authorized” entities can resolve a name to an IP address or answer the question.⁴

The Role of ISPs

Approximately twenty-five ISPs carry as much as eighty percent of all the Internet traffic.⁵ They own and operate a critical infrastructure that facilitates the delivery of essential goods and services. As intermediaries and stewards of this infrastructure, they have an important role to play in fostering security.

When a new ISP⁶ connects to the Internet it implicitly agrees to certain terms concerning the transmission of packets, sharing of routing information, resolution of domain names, reporting on the status of the Internet, and handling emergencies. Until now these understandings were not made explicit. There should be an explicit *duty* to comply with technical aspects of Internet participation. Given the rapid rise in the complexity of the Internet and the critical role it has come to play in the global economy, *providers should be obligated to be stewards of the global enterprise*. We can no longer be one-click away from an infection, disruption, or worse yet, no service.

Duties Incumbent on ISPs

The major telecommunications providers and ISPs, collectively, have unparalleled visibility into global networks, which enables them, with the proper tools, to detect cyber intrusions and attacks as they are forming and transiting towards their targets. Today, some ISPs limit spam, notify

⁴ Cryptographic signing is a digital guarantee that information has not been modified, as if it were protected by a tamper-proof seal that is broken if the content is altered.

⁵ Sriram Vadlamani. “The Top 25 Telecom Companies in the World, Based on Brand.” Asian Correspondent.com. 12 April 2009. [<http://asiancorrespondent.com/515/top-25-telecom-companies-in-the-world-based-on-brand-value/>] The Cooperative Association for Internet Data Analysis (CAIDA) show that the top 20 Autonomous Systems account for the majority of the IPv4 prefixes and addresses. [<http://as-rank.caida.org/>] Also, DoubleClick AdPlanner for April 2011 show that the largest 25 of the top 1000 properties accounted for 80 percent of web traffic globally.

⁶ A network that is under the administrative control of one organization is called an *autonomous system* (AS). There are approximately 40,000 ASes operating today. For the purposes of this paper, we treat the acronym ISP as a synonym for either ISP or AS. Routing within an AS is called *intra-domain routing* whereas routing between ASes is called *inter-domain routing*.

customers of botnet⁷ infections, and partner with law enforcement to deny the distribution of child pornography. Internationally, this collection of autonomously administered networks already adhere to common protocols, enable seamless, global connectivity, and collaborate to ensure 24x7 uninterrupted service. If nations work together to define codes of conduct that all ISPs agree to follow, it will result in a more secure Internet infrastructure and service. Below we propose duties to which ISP might subscribe.

A. Duty to provide reliable and accessible conduit for traffic and services

The Internet is considered a basic, ubiquitous, and essential communications tool for all of society. Governments around the world are adopting policies to facilitate citizen access to the Internet via a fast, reliable, and affordable Information Communications Technology (ICT) infrastructure. This vision is reflected in Organisation for Economic Co-Operation and Development's (OECD) Internet Economy; Europe's Digital Agenda; the United States' National Broadband Plan; and in the International Telecommunications Union (ITU) initiatives.⁸ Economic progress, citizen access, and infrastructure quality are measured in terms of price, bandwidth, speed/quality of service, skills, content and language, and applications targeted to low-end users.⁹ Progress is being made and these global initiatives are bringing faster broadband Internet access for every citizen, to facilitate our information society needs and global e-commerce demands.

For example, Finland passed a law in 2010 stating that every one of its citizens will have the right to access one megabit per second (Mbps) broadband connection, obligating twenty-six telecommunications companies to provide that quality of service.¹⁰ Finland went on to *amend their constitution* to make broadband access a constitutional right. Separately, the United Kingdom promises to have a minimum connection of two Mbps to all homes by 2012.¹¹

Government efforts to provide universal access to consumers at lower cost have been underway for decades. Telecommunications liberalization brought the promise of global income gains (economic growth) by making access to knowledge easier. The General Agreement on Trades and Tariffs (GATT) Uruguay Round (1986-1993) began the discussion among nations. It was further codified in the Marrakech Treaty in 1994, where the General Agreement on Trade in Services (GATS) principles called for transparency, access to, and use of public telecommunications transport networks (PTTN) and services "on reasonable and non-discriminatory terms." This included obligations for interconnection to PTTN (including private networks) as well as safeguards for public-service responsibilities (*duty to warn*) and to protect the technical integrity of the network (*reliable service*).

⁷ A Bot is a malicious form of software that could use your computer to send spam, host a phishing site, or steal your identity by monitoring your keystrokes and responds to issues relating to spam, virus-infected computers, and other security-related issues. Infected computers are then controlled by third parties and can be used for cyber attacks.

⁸ The International Telecommunication Union (ITU) is the United Nations specialized agency for information and communication technologies.

⁹ International Telecommunications Union. Measuring the Information Society, 2011. Geneva Switzerland.

¹⁰ Finland Ministry of Transport and Communications. Press Release. 29 June 2010.

[<http://www.lvm.fi/web/en/pressreleases/-/view/1169259>]

¹¹ "Government Reveals Super-Fast Broadband Plans". BBC News, 6 June 2010.

[<http://www.bbc.co.uk/news/technology-11922424>]

In 1997, the World Trade Organization (WTO) adopted a Basic Telecommunications Agreement (BTA) to liberalize facilities-based international service and to allow foreign entities to own a majority interest in facilities used to provide international voice and data service.¹² Examples of the services covered by the agreement include voice telephony, data transmission, telex, telegraph, facsimile, private leased circuit services (i.e. the sale or lease of transmission capacity), fixed and mobile satellite systems and services, cellular telephony, mobile data services, paging, and personal communications systems.

In addition to the basic agreement, 55 governments agreed to value-added services (or telecommunications for which suppliers “add value” to the customer’s information by enhancing its form or content or by providing for its storage and retrieval, such as on-line data processing, on-line data base storage and retrieval, electronic data interchange, e-mail or voice mail). The World Trade Organization Director-General, Mr Renato Ruggiero, stated that “information and knowledge, after all, are the raw material of growth and development in our globalized world.”¹³

The rapid adoption of technology and growing migration of essential services to be delivered on Internet-based infrastructure demands a re-examination of whether ISPs should be classified as non-discriminatory. That is, must they treat all customers equally in terms of service or can they “discriminate?” Can we really say that the Internet or those that provide information services over the Internet deserve some degree of explicit responsibility as those assigned to “telecommunications service providers?”

Internationally, most nations do not distinguish between basic services (traditional modes of communications) and enhanced services (Internet-based services). However, the United States has made that distinction. The Telecommunications Act of 1996 created separate regulatory regimes for companies providing voice telephone service, cable television service, and providers of information services (broadband). The law did not necessarily envision the convergence of voice, data, and video services and infrastructures. A year after this law was enacted, the United States agreed at the WTO to treat both value added services (Internet) and traditional communications (voice) in a non-discriminatory manner. The Federal Communications Commission (FCC) or Congress should clarify this contradiction. Why? Because the rapid adoption of technology and growing migration of essential services to be delivered on Internet based infrastructure demands that broadband and other Internet-based services be classified as core telecommunications services that obligates the providers to deliver a reliable service that contributes to the stability and resiliency of the global communications infrastructure.

The United States and other countries are pursuing deeper integration of critical infrastructures with Internet based technologies, like the “smart grid,” a computerized network that facilitates electricity and information flows between homes and electrical suppliers; computerized health records; public safety alerts (Voice Over Internet Protocol); and next-generation air-traffic management. These essential services may not be built to the same standards for which the traditional voice telephone system was built. Broadband network reliability and resiliency are

¹² Federal Communications Commission. “Report on International Communications Markets 2000 Update” Prepared for Senator Ernest F. Hollings, United States Senate Committee on Commerce, Science, and Transportation. 4 May 2001. Page 3

¹³ World Trade Organization. Paper 16. “WTO Telecom Talks Produce Landmark Agreements.” 15 February 1997 [http://www.wto.org/english/res_e/focus_e/focus16_e.pdf]

vital for all services that traverse a network, including traditional communications services. Our reliance on the dependable operation of communications networks is growing. Therefore, it may be necessary to expand existing communications reliability and resilience programs, including best practices and associated outage reporting, as these services transition from traditional modes of communications to Internet-based technologies. Outage reports and other reliability data collected by regulators provide insight to the overall health of communications reliability and security of the critical infrastructure and, where necessary, enables regulators to work with individual entities or the industry as a whole to bring about improvements.¹⁴

The FCC realizes that it "needs a clear strategy for securing the vital communications networks upon which critical infrastructure and public safety communications rely."¹⁵ Europe is already moving forward with streamlining its regulatory process as part of the Digital Agenda for Europe. Europe recognizes that compliance monitoring and enforcement of a non-discrimination policy allows for more choices, at affordable prices, underpinned by a higher standard of service.¹⁶

Many nations have recognized that it is in their national economic interest to enhance access to and participation in the Internet. ISPs provide an essential citizen service – the Internet – and they also provide the conduit upon which other essential services depend (e.g., Smart Grid). Therefore, it is their *duty to serve as reliable and accessible conduits* to Internet traffic and services

B. Duty to provide authentic and authoritative routing information

Inter-domain routing (from ISP to ISP) is done primarily using the *Border Gateway Protocol* (BGP).¹⁷ BGP has become a standard because of its simplicity and resilience. Under BGP, *announcements* are made by each ISP of destinations that can be reached via it and the paths that packets will take to these destinations. (Think of this as a message that says I am open for business, I can route your information and if you send it to me, it will pass through these ISPs.) These announcements propagate to neighbors and eventually to all routers on the Internet. BGP relies on trust among the operators of gateway routers, routers between ASes, to ensure the integrity of Internet routing information. However, this trust has been compromised on a number of occasions, revealing fundamental weaknesses in this critical Internet utility and service.

When BGP vulnerabilities are exploited, Internet traffic can be misdirected and misused. For example, in February 2008 Pakistan Telecom was ordered by the Pakistan telecommunications ministry to prevent its users from viewing certain YouTube addresses. Announcements of short

¹⁴ United States Department of Energy, Office of Inspector General. "Audit Report: The Department's Management of the Smart Grid Investment Grant Program." OAS-RA-12-04. January 2012.

¹⁵ The United States Federal Communications Commission. Connecting America: The National Broadband Plan. 16 March 2010.

¹⁶ European Commission. "Commission launches public consultation on the application, monitoring and enforcement of non-discrimination obligations in electronic communications." 28 November 2011. [http://ec.europa.eu/information_society/policy/ecomm/library/public_consult/non_discrimination/index_en.htm]

¹⁷ "A Survey of BGP Security Issues and Solutions," K. Butler, T.R. Farley, P. McDaniel, and J. Rexford, Procs. IEEE, Vol. 98, No. 1, January 2010.

paths to these addresses were designed to draw traffic from within Pakistan to this provider who then proceeded to discard the traffic. Unfortunately, these announcements leaked from Pakistan and made portions of YouTube inaccessible to about two thirds of all Internet users for about two hours.¹⁸

On April 10, 2010, BGP users received an alert regarding a possible prefix hijack by China's largest ISP, China Telecom. For approximately fifteen minutes, this ISP generated approximately 37,000 unique prefixes that were not assigned to them.¹⁹ This is what is typically called a prefix hijack and while the hijack had modest to minimal impact on total Internet traffic volumes, it should be noted that China was 10 times more affected than the United States. Yet, this event underscores the vulnerability of the BGP routing infrastructure and reminds us that if intentional, the criminal could store, alter or just be throw away the traffic.²⁰

In this last case, given the brevity of the incident and the fact that no traffic was known to have been lost, the redirection may have been an accident. However, as was shown a few years ago, it is possible for an ISP to create path announcements that can deliberately move traffic to a particular ISP where a man-in-the-middle attack can be perpetrated. In such an attack, packets can be read, modified or destroyed.²¹

The only way to solve the BGP trust problem is to develop and administer a system that allows each step in the process to be signed and certified. Routers should be able to affirm with high confidence that each routing announcement has not been modified in transit and that the sender is authorized to make such an announcement.

Of the many proposals have been made to meet the trust requirements, Secure BGP²² (S-BGP) is the most secure. Unfortunately, it has not been deployed, possibly because at the time the proposal was made, it was considered to be computationally demanding and its implementation requires a global public key infrastructure (PKI). Although the situation has changed, adoption of S-BGP will be challenging due to the large number of routers now in operation globally. Through simulation and analysis, Gill *et. al.* have made a convincing argument that by seeding large ISPs with S-BGP and having them provide attestations for stub ASes (85% of all ASes are stubs), profits will drive ISPs to adopt it.²³

Packets can still transit from IP to IP without the DNS.²⁴ However, without BGP, packets can't move at all. Regulators around the world have begun discussions with industry regarding the adoption of secure routing procedures and protocols based on existing work in industry and the

¹⁸ Declan McCullagh. "How Pakistan Knocked YouTube Offline." CNET News. 25 February 2008.

[http://news.cnet.com/8301-10784_3-9878655-7.html]

¹⁹ BGP.mon blog. [<http://bgpmon.net/blog/?p=282>]

²⁰ BGP.mon blog. <http://bgpmon.net/blog/?p=323>

²¹ <http://arstechnica.com/security/news/2008/08/inherent-security-flaw-poses-risk-to-internet-users.ars>

²² See <http://www.ir.bbn.com/sbgp/>

²³ "Let the Market Drive Deployment: A Strategy for Transitioning to BGP Security," Gill, Schapira, Goldberg, Procs. SIGCOMM'11, August 15-19, 2011..

²⁴ Joel Hruska. "Gaping Hole Opened in Internet's trust-based BGP Protocol". ARS Technica (online). [<http://arstechnica.com/security/news/2008/08/inherent-security-flaw-poses-risk-to-internet-users.ars>]

above-mentioned research. ISPs need a process or framework for securing BGP announcements that includes specific technical procedures and protocols. The framework, if adopted by large ISPs (even the leading ten or fifteen companies), could go a long way toward making the Internet a more reliable, secure service.²⁵ Protocols and infrastructure are needed for everyday use of the Internet. ISPs have a *duty to provide authentic and authoritative routing information*. To us, this means they should adopt S-BGP or something equivalent.

C. Duty to provide authentic and authoritative naming information

As mentioned earlier, the Domain Name System (DNS) is the “telephone directory” for the Internet. The DNS system was not designed with security in mind. This directory is implemented as a hierarchical collection of “servers.” There are thirteen Root zone servers that contain the names of the top-level-domain (TLD) name servers associated with suffixes, such as *.mil*, *.edu*, or *.com*. Each of these servers contains the names of sub-domain name servers, such as *brown.edu*, which resolve or translate universal resource locaters (URLs) into IP addresses. The root zone, top-level, and sub-domain name servers are authorized by the Internet Corporation for Assigned Names and Numbers (ICANN) to provide name resolution. Thus, these servers are said to be *authoritative*.

For efficiency reasons, ISPs maintain DNS caches.²⁶ If a user asks for a translation that is not in the cache, the ISP finds it and inserts it into the cache. These entries have a time-stamp associated with them and are refreshed when the “time-to-live” limit is reached.

The DNS system was not designed to be secure. For example, when a computer or a DNS cache asks for the resolution of a domain name, a series of queries and responses to a root zone server, top-level-domain server, domain and sub-domain server occur, in that order, until a mapping is found for the URL in question. When a request is issued at each stage of the transaction, the initiator accepts the first response that it receives to its query. This provides an opportunity for a man-in-the-middle attack in which a malicious agent can insert a response, which directs the initiator to a non-authoritative server. The DNS also provides a key function for IP applications such as VoIP. In some cases, when a user makes a call with VoIP, the user’s machine will contact a DNS server to get the IP address of the called number. However, if the DNS cache is poisoned, the calls could be misdirected to somebody else who could then obtain your personal and confidential information.

Several dramatic abuses of the untrusted DNS system have occurred. Two recent examples demonstrate this vulnerability. In November 2011, the Federal Bureau of Investigation (FBI), working in cooperation with Estonian authorities and others, dismantled an international cybercrime ring that infected millions of computers worldwide by downloading a malicious piece of software (i.e, a Trojan) called DNSChanger.²⁷ This piece of malware changed the IP address of the DNS cache used by various computer operating systems so that instead of using a local, and presumably honest cache, it redirected the compromised machine to a compromised

²⁵ Ibid

²⁶ A cache is a file that hold copies of the mappings of domain names to IP addresses

²⁷ “Operation Ghost Click: International Cyber Ring That Infected Millions of Computers Dismantled,” FBI web site, Dated November 9, 2011, accessed February 5, 2012.

DNS cache. Not only would this Trojan evade the proscriptions of the recently introduced pieces of legislation of Stop Online Piracy Act (SOPA, H.R. 3261) and Protect Intellectual Property Act (PIPA, S. 968), it has misdirected users to sites where they participated, unwittingly, in click fraud. Clicks that appeared legitimate generated millions of dollars in income for the fraudsters.

A recent report states that DNSChanger continues to infect computers at half of the Fortune 500 companies and half of all Federal agencies.²⁸

A second example involves VeriSign, an American firm that operates two root servers, and three top-level domains (TLDs) namely the *.com*, *.net*, and *.name* domains. VeriSign announced that it had been repeatedly hacked in 2010 but that it does not believe that its DNS database servers were breached.²⁹ If their system was breached, trust in their management of key components of the DNS database will be seriously damaged.

The security extensions to DNS (DNSSEC) mentioned above were developed by the Internet Engineering Task Force (IETF) and are designed to address the vulnerabilities with DNS.³⁰ They rely on digital signatures to certify that the parties requesting updates to DNS mappings are authorized by a central trust anchor to make those changes. The bottom line is that DNSSEC is intended to improve data integrity on DNS connections through the authentication process. However in order for DNSSEC to work, it must be supported at every level of the DNS hierarchy, from root server to browser. A chain of trust must be established from the information producer to the information consumer. Without this unbroken chain of trust, opportunities for exploitation remain.

Today, most of the root servers are implementing DNSSEC and many of the TLDs are deploying DNSSEC. ISPs need to upgrade their systems and increase their technical knowledge to deploy DNSSEC to deeper into the infrastructure. Accelerating the deployment of DNSSEC will help eliminate BGP vulnerabilities and bring a higher level of quality of service to their customers. Customers need to be assured that their traditional voice, VoIP, email, video, or other service is going to get to its correct destination and maintain its integrity along the way. Therefore, ISPs have a *duty to provide authentic and authoritative naming information* as part of their service.

D. Duty to report anonymized security incident statistics to the public

A major impediment to calibrating scope and scale of security threats to the Internet is the paucity of public data. Some ISP customers are reluctant to have incident data concerning their enterprises or infrastructures reported out of concern for their reputations as responsible guardians of data might be tarnished.³¹ This lack of transparency limits the ability for the security

²⁸ Brian Krebs. "Half of Fortune 500s, US Govt. Still Infected with DNSChanger Trojan" Krebs on Security. February 2012. [<http://krebsonsecurity.com/2012/02/half-of-fortune-500s-us-govt-still-infected-with-dnschanger-trojan/>]

²⁹ VeriSign Annual 10-K Corporate Filing. See also, Joseph Menn. VeriSign Hacked: Security Repeatedly Breached at Key Internet Operator. Reuters. 2 February 2012.

³⁰ Internet Engineering Task Force overview of DNSSEC. [<http://www.dnsssec.net/rfc/>]

³¹ It should be noted that recent guidance published on 13 October 2011 issued by the Securities Exchange Commission (SEC), notes that all public companies have existing obligations to disclose material risks and events on their public filings. A risk or event is material if it is important for the average investor to know before making an investment decision. The clarifying guidance states that "material risks can include cyber risks and material

product industry to deliver products that perform with higher assurance levels. It also limits the research community's access to data that could facilitate idea creation and innovative solutions that increase security across the entire architecture.

ISPs should have a duty to report data sets, including but not limited to the (1) volume of spam seen in transit; (2) estimated number of compromised machines owned by customers of an ISP; (3) remediation steps proposed to customers by an ISP and actions taken by them; (4) frequency, intensity, sources and targets of distributed denial of service attacks; (5) location, frequency, and duration of network outages and route disruption; and (6) the frequency, source and target of cache poisoning attacks, to facilitate solution development. It would also be helpful if the ISP reported event data that exceeded predetermined thresholds similar to their responsibilities when there is a disruption of communications service.

Initially it may suffice for only the largest ISPs to report such data. They have more resources at their disposal and, as has been reported, they service the largest percentage of compromised machines.³² Reporting of incident data may either be encouraged by national or trans-national authorities or prohibited by law. For example, the European Parliament and Council of Ministers reached an agreement on pan-European telecommunications reform that is being transposed into national laws.³³ Section 13(a), "Security and Integrity of Networks and Services," of the Regulatory Framework for Electronic Communications in the European Union, outlines a number of duties for ISPs. Among them are the duty to "notify the competent national regulatory authority of a breach of security or loss of integrity that has had a significant impact on the operation of networks or services; and where appropriate, the national regulatory authority concerned shall inform the national regulatory authorities in other Member States and the European Network and Information Security Agency (ENISA)."³⁴ The directive goes on to say that the regulators can ask the ISPs to "inform the public when it determines that disclosure of the breach is in the public interest."³⁵ Finally, the directive requires that "once a year, the national regulatory authority concerned shall submit a summary report to the Commission and ENISA on the notifications received and the action taken in accordance with this paragraph."³⁶

events can include cyber breaches, including the theft of intellectual property/trade secrets, penetrations which compromise operational integrity, etc. See: <http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm>

³² "The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis Based on Spam Data", OECD Science, Technology and Industry Working Papers, 2010/05, van Eeten, M. et al state that in 2009 60% of all infected machines are in the top 200 of ISPs.

³³ European Parliament Council. "Regulatory Framework for Electronic Communications in the European Union." 2009. Specifically, see DIRECTIVE 2009/140/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 25 November 2009 that amends Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorization of electronic communications networks and services.

³⁴ European Parliament Council. "Regulatory Framework for Electronic Communications in the European Union." 2009. page 55.

³⁵ Ibid., Page 55.

³⁶ Ibid., Page 55.

On the other hand, in the United States, many attorneys interpret the Electronic Communications and Privacy Act of 1986, along with the Telecommunications Act of 1996, as limiting the ability of ISPs to share this data.³⁷ It should be noted that aggregate threat data is collected by commercial security firms, such as Symantec and McAfee, which make it available to customers for a fee.

Because ISP customers are reluctant to have data on their enterprises released, their cooperation may require that safeguards be put in place, including keeping data private while allowing useful statistics based on the data to be computed. Such safeguards have been the holy grail of statistics since at least the 1970s.³⁸ In 2006, two papers emerged that provided a basis for showing that it is possible to give highly accurate responses to queries on statistical databases while minimizing the probability of identifying individual records.³⁹ The authors made a key observation, namely, that privacy comes from uncertainty. Using this observation they defined the concept of *differential privacy*, which is based on query functions that use random numbers to generate results.

A randomized query function is said to offer differential privacy if the *probability* that it produces an outcome when a single element is in the dataset is within a constant multiplicative factor of the *probability* that it produces the same outcome when the element is not in the dataset. Thus, a differentially private query function behaves approximately the same whether the element is in the dataset or not. Functions of this kind have been developed for a large number of useful queries.⁴⁰

If ISPs assumed the *duty to report anonymized statistics on security incidents to the public*, it would likely lead to the emergence of a standard of care or best practices for the all ISPs to follow. It would also spark the development of innovative solutions and the deployment of better capabilities for enterprise and infrastructure protection.

E. Duty to educate customers about threats

Most ISPs deploy advanced technologies that detect malicious and harmful activity. They have unique insights on the scope and scale of cyber threats and incidents affecting our homes, businesses, and infrastructures. As such, they also can play a unique role in educating their customers about the threats. Customers who are able to recognize the threat and are presented with user-friendly resources/tools are capable of enhancing their security, and as a result are

³⁷ The Telecommunications Act of 1996. Pub. L. No. 104-104, 110 Stat. 56. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986). Note, Lawyers for the ISPs interpret the ECPA to prohibit the voluntary provision of customer data.

³⁸ Tore Dalenius. "Towards a methodology for statistical disclosure control." *Statistik Tidskrift* (Statistical Review) Volume 15. 1977. Pages 429-444.

³⁹ Cynthia Dwork. "Differential Privacy." In *Proceedings of the 33rd International Colloquium on Automata, Languages and Programming (ICALP)*, 2:1-12 and Dwork, C., McSherry, F., Nissim, K., and Smith, A. (2006). *Calibrating noise to sensitivity in private data analysis*, In *Proceedings of the 3rd Theory of Cryptography Conference*, 265-284.

⁴⁰ Cynthia Dwork and Adam Smith. "Differential Privacy for Statistics: What we Know and What we Want to Learn," *Journal of Privacy and Confidentiality*, Vol 1, No. 2, 14 January 2009. Pages. 135-154.

better poised to protect themselves. Government and industry educational resources are emerging in every corner of the world many of which have an ISP as a critical component of the education campaign.

For example, in December 2011 a coalition of 28 service providers, network operators and equipment suppliers in the European market began working together to make a better and safer Internet for children (“Coalition”).⁴¹ The Coalition is a cooperative voluntary effort aimed at making it easier to report harmful content, ensuring privacy settings are age-appropriate, and offering wider options for parental control, reflecting the needs of a generation that is going online at an increasingly young age. European Commission Vice President Neelie Kroes said: “This new Coalition should provide both children and parents with transparent and consistent protection tools to make the most of the online world. The founding Coalition members are already leaders in children's safety online. Working together we will be setting the pace for the whole industry and have a great basis for fully empowering children online.”⁴²

In the United States, two projects have emerged worth noting. The first is a Web-wide partnership entitled GetNetWise.⁴³ It is a public service funded and developed by Internet industry corporations and public interest organizations to help ensure that Internet users have safe, constructive, and educational or entertaining online experiences. The GetNetWise coalition wants Internet users to be just “one click away” from the videos, educational materials, and other helpful hints they need to make informed decisions about their and their family's use of the Internet. The service is facilitated by the Internet Education Foundation, a non-profit organization dedicated to educating the public and policymakers about the potential of a decentralized global Internet to promote communications, commerce and democracy.

The second program is the National Cyber Security Alliance (NCSA). Its sponsors include AT&T, Verizon, Microsoft, Google, McAfee, Symantec, Cisco, ADP and many others. The organization’s purpose is to educate and therefore empower a digital society to use the Internet safely and securely at home, work, and school, protecting the technology that individuals use, the networks they connect to, and shared digital assets. It develops and disseminates educational materials for home, classroom, and business use.

Australia commissioned a study to understand the depth of education initiatives around the world. The research report by Galexia documents more than 68 different initiatives and highlights the different techniques used to educate consumers on the basics of cybersecurity.⁴⁴ The study notes that many of these initiatives help fight illegal and harmful online content and

⁴¹ Founding Coalition members are: Apple, BSKyB, BT, Dailymotion, Deutsche Telekom, Facebook, France Telecom-Orange, Google, Hyves, KPN, Liberty Global, LG Electronics, Mediaset, Microsoft, Netlog, Nintendo, Nokia, Opera Software, Research in Motion, RTL Group, Samsung, Sulake, Telefonica, TeliaSonera, Telenor Group, Tuenti, Vivendi, Vodafone.

⁴² European Commission. Press Release. “Digital Agenda: Coalition of Top Tech & Media Companies to Make Internet Better Place for Our Kids” 1 December 2011.

[<http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/1485>]

⁴³ <http://www.getnetwise.org/about/>

⁴⁴ Australian Communications and Media Authority. An Overview of International Cybersecurity Awareness and Educational Initiatives: A Research Report. May 2011.

[http://www.acma.gov.au/webwr/_assets/main/lib310665/galexia_report-overview_intnl_cybersecurity_awareness.pdf]

conduct while at the same time promoting the safer use of the Internet and other communication technologies.

Other innovative activities include the fielding of video games to educate the public. In the United States there is a partnership between i-SAFE (a non-profit organization dedicated to educating and empowering youth (and others) to safely, responsibly and productively use Information and Communications Technologies (ICT)) and Carnegie Mellon University. They are integrating an on-line game entitled, “MySecureCyberspace” into thousands of K-12 programs across the United States.⁴⁵ Children play the game in a digital city and learn to secure the key infrastructures and critical services. Children become aware of online security and privacy issues as they interact with the Carnegie Cadet characters in a virtual world. Similarly, the United Kingdom has launched an on-line virtual reality game entitled “Smokescreen” that guides teenagers through dangers of social networking.⁴⁶ The game has over thirteen missions that place teenagers in situations that force them to ask themselves, what would I do if it happened to me? What if ISPs promoted innovative educational materials like these? In a secondary educational campaign, the Ministry of Defense aired a number of television commercials alerting citizens of their responsibility for on-line security. The commercials present scenarios where, criminals, terrorists and predators review personally posted data on YouTube, Twitter, Facebook, etc., to achieve a purpose.⁴⁷

The cybersecurity problem space is growing faster than the solution space. If ISPs undertake the *duty to educate their customers about the threats*, then our respective government leaders will be able to engage in a broader conversation about all of the solutions that can be brought to bear to address the problem comprehensively.

F. Duty to inform customers of apparent infections in their infrastructures

Media headlines throughout the past year have been rife with high profile cybercrime events, confirming that insecure computers are being infected every day. Criminals have shown that they can harness bits and bytes with precision to deliver spam, cast phishing attacks, facilitate click-fraud, and launch distributed denial of service (DDoS) attacks. The increasing frequency of these events in recent years and the scale of those affected have been alarming. Some estimates suggest that, in the first quarter of 2011, almost 67,000 new malware threats were seen on the Internet every day. This means more than 45 new viruses, worms, spyware and other threats were being created every minute – more than double the number from January 2009. As these threats grow, security policy, technology and procedures need to evolve even faster to stay

⁴⁵ Carnegie Mellon University. “Cyber Education.”

http://www.carnegiemellontoday.com/pdfs/news_pdfs/CMSecurity_CyberEducation.pdf and the game is accessible on the Web at www.mysecurecyberspace.com

⁴⁶ The game is accessible on the web at: <http://www.smokescreengame.com/> and “Smokescreen - A New Resource for Promoting Safty Online. [<https://blogs.glowscotland.org.uk/glowblogs/ISRU-News/2010/05/06/smokescreen/>]

⁴⁷ United Kingdom, Ministry of Defense Online Security Campaign. See: <http://www.youtube.com/watch?v=hpKiIrYDLxg>; <http://www.youtube.com/watch?v=-UziYBdnQhk>; <http://www.youtube.com/watch?v=1UyWN0uREfk>; and <http://www.youtube.com/watch?v=qXZSzs-P2kQ>

ahead of the threats.”⁴⁸ A recent Symantec report suggests that these the trends will continue.⁴⁹ From 2010 to 2011 the differences were discouraging. In fact:

- There were 286 million unique variants of malware that exposed and potentially exfiltrated our personal, confidential, and proprietary data;
- Each data breach exposed, on average, 260,000 identities;
- There was a 93% increase in Web-based attacks (compromised/hijacked websites where if visited, you would become infected);
- The underground economy paid anywhere from \$.07 to \$100 for our stolen credit card number; and
- Realizing that mobile payments and mobile platforms (e.g., smart phones, iPad™) would be the newest vector of technology adoption, there was a 42% increase in mobile operating system vulnerabilities and subsequent exploitation.

While consumer education is necessary, recent efforts have shifted toward having the ISPs act as the intermediary or control point for impeding the spread of infection and eradicating the malicious activity.⁵⁰

Australian ISPs are showing the world that industry can organize and implement a consistent approach to help inform, educate, and protect their customers in relation to cybersecurity.⁵¹ Thirty leading ISPs serving over 90% of the Australian market have opted-in to providing a four pronged security service, including: (1) a notification/management system for compromised computers, (2) a standardized information resource for end users, (3) a comprehensive resource for ISPs to access the latest threat information, and (4) a reporting mechanism to CERT Australia to facilitate a national high level view of threat status. Australian customers are notified about suspicious activity, their ISP assists them stopping the infection, and if need be, the ISP quarantines them so that the computers cannot browse the wider web until they have been repaired. “The Australian experiment has been stunningly successful,” said Michael Barrett, chief information security officer for PayPal. “We will see more countries adopting this model.”⁵² The Australian model is now promoted by the OECD, which found that ISPs represent nearly 87% of the total market (service) in 40 nations.⁵³ They also recognize that peer pressure among the ISPs is an important incentive that contributes to security and opting-in to an overall program.

⁴⁸ United States Department of Commerce, Internet Policy Task Force. Cybersecurity Green Paper. June 2011. Page ii.

⁴⁹ Symantec Internet Security Threat Report: Trends for 2010, Volume 16. April 2011

⁵⁰ A recent report by the OECD defines Internet intermediaries as follows: “Internet intermediaries bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet- based services to third parties.” See: OECD (2010). The Economic and Social Role of Internet Intermediaries. OECD. Available online at www.oecd.org/dataoecd/49/4/44949023.pdf.

⁵¹ Internet Industry Association (Australia). “Internet Service Providers Voluntary Code of Practice for Industry Self-Regulation in the Area of Cyber Security.” 1 June 2010. [\[http://iia.net.au/images/resources/pdf/iia_cybersecuritycode_implementation_dec2010.pdf\]](http://iia.net.au/images/resources/pdf/iia_cybersecuritycode_implementation_dec2010.pdf)

⁵² Joseph Menn. “US starts to tackle hacking curse” Financial Times. 12 October 2011.

⁵³ Organisation for Economic Co-operation and Development, Directorate for Science Technology and Industry. *The Role of Internet Service Providers in Botnet Mitigation: An Empirical Analysis based on Spam Data*. [STI WORKING PAPER 2010/5], 12-Nov-2010. Page 41.

In Japan, more than 70 Internet service providers, representing 90% of the customer base have assumed the duty to inform their customers of infections. ISPs notify consumers if their machines appear to be part of a botnet infection and offer government-funded tools offered through Cyber Clean Center (CCC) to clean the computers.⁵⁴ This voluntary program has shown remarkable reduction of infection rates. From 2007 to 2011, ISPs have reduced the rate of botnet infection from about 2.5% of personal computers to just 0.6%.⁵⁵

In the Netherlands, Dutch ISPs signed the Anti-Botnet pact and jointly launched an initiative to fight malware-infected computers and botnets. The efforts involves 14 ISPs and represents 98% of the consumer market. ISPs are sharing information to obtain better coverage and reduce response times. They have accepted the responsibility to notify their victimized users and quarantine the infections until assistance can be provided.⁵⁶

In Germany, the German Federal Office for Information Security (BSI) has mandated that its ISPs track down infected machines and provide advice to users on how to clean their computers.⁵⁷ Telefonica has taken this initiative further. It recently launched customer protection insurance against online fraud at a cost of five euro per month. "The customer and up to six family members are covered against data misuse, fraudulent online payment practices and theft or damage of the Telefonica Germany DSL router, modem or surf stick. Telefonica claims to be the first network operator to offer a customer protection insurance."⁵⁸

And in the United States, Comcast is a market leader and early adopter of the duty to inform and protect its customers. Through its service known as Constant Guard, Comcast proactively contacts its customers via an email "Service Notice" if Comcast believes one or more of its customer's computers is infected with malicious software (e.g., it is a bot). Comcast's efforts in this regard have received the attention of the Federal Communications Commission (FCC).

Service providers, network operators, and equipment suppliers are working together as part of the FCC's Communications Security, Reliability and Interoperability Council's (CSRIC) to propose a set of agreed-upon voluntary practices that would constitute the framework for an opt-in implementation model for ISPs to conduct botnet remediation.⁵⁹ This initiative is modeled after the Australian iCODE Project and, if widely adopted in the United States, could make a significant difference in ensuring the health of their Internet backbone

These examples show that ISPs are already assuming the *duty to inform customers of apparent infections in their infrastructures* principle. Some ISPs might participate strictly for business purposes - to reduce fraud, infections, and unnecessary bandwidth use. Others may engage for

⁵⁴ European Network and Information Security Agency (ENISA) Botnets: Detection, Measurement, Disinfection & Defence. 2011. page 98.

⁵⁵ Joseph Menn. "US starts to tackle hacking curse" Financial Times. 12 October 2011.

⁵⁶ Gadi Evron. "Dutch ISPs Sign Anti-Botnet Treaty." *Dark Reading*. 29 September 2009. [<http://www.darkreading.com/blog/227700601/dutch-isps-sign-anti-botnet-treaty.html>]

⁵⁷ John Leyden. "German ISPs team up with gov agency to clean up malware." The Register. 9 December 2009.

⁵⁸ "Telefonica Germany Offers Internet Insurance." TelecomPaper (online). 9 February 2012. [<http://www.telecompaper.com/news/telefonica-germany-offers-internet-insurance>]

⁵⁹ CSRIC mission is to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.

more altruistic purposes; they may wish to assume responsibility for the safety of the Internet and their users, perhaps at their own expense. Either way, "it is important that ISPs collectively battle this problem and protect their customers as well as prevent nuisance to the rest of the Internet," says Albert Vergeer, director of Internet for KPN, XS4ALL, and Telfort.⁶⁰

G. Duty to warn other ISPs of imminent danger and help in emergencies

ISPs have unique visibility of the malware and activity transiting their infrastructure. They also have a responsibility to provide uninterrupted service to their customers. As we see more organized and semi-organized groups disrupt services and infrastructures in support of the "cause of the day" using DDoS or similar malware, it may demand that the ISPs adopt and practice Good Samaritan behavior.

Good Samaritan laws more typically apply in countries in which the foundation of the legal system is English common law.⁶¹ In many countries that use civil law (i.e., the legal system inspired by Rome) as the foundation for their legal systems, the same legal effect is more typically achieved using a principle of duty to rescue.⁶² Perhaps one of the best internationally recognized of these laws is the use of the SOS.⁶³ When a threatened party uses SOS, it triggers a duty to assist (DTA) that marshals available resources to help victims avoid or recover from harm. Similar duties to assist exist in both domestic and international contexts, such as a nuclear accident or a pilot's Mayday call. Duncan Hollis has called for the creation of an e-SOS, a duty to assist in the case of cyber emergencies.⁶⁴ Even the North Atlantic Treaty Organization's (NATO) has Article 4, which is a consultation and information sharing arrangement that activates when a member nation perceives its territorial integrity, political independence, or security is threatened.⁶⁵ Even the Telecommunications Act of 1996 contains a Good Samaritan provision to protect ISPs from liability when they act in good faith to block or screen offensive content hosted on their systems.⁶⁶

To effectively defend the information infrastructure requires that private and public parties identify threats quickly and mitigate their impact effectively. As at sea, the timing and scale of some cyber threats can overwhelm the most sophisticated individuals, groups, and even states. For example, in July 2009 the United States and South Korea fell victim to a DDoS attack

⁶⁰ Gadi Evron. "Dutch ISPs Sign Anti-Botnet Treaty." *Dark Reading*. 29 September 2009.

[<http://www.darkreading.com/blog/227700601/dutch-isps-sign-anti-botnet-treaty.html>]

⁶¹ Gulam H, Devereaux J (2007). ["A brief primer on Good Samaritan Law for health care professionals"](#). *Aust Health Rev* (31): 478–482.

⁶² A **duty to rescue** is a concept in tort law that arises in a number of cases, describing a circumstance in which a party can be held liable for failing to come to the rescue of another party in peril.

⁶³ SOS is not an acronym, but a specific Morse Code, represented as ". . . --- . . ." It was adopted as the standard distress signal in 1912 by the London International Telegraph Convention. G.E. Wedlake, SOS: The Story of Radio-Communication 50 (David & Charles 1973).

⁶⁴ Duncan Hollis. "An e-SOS for Cyberspace." *Harvard International Law Journal*. Volume 52, Number 2, Summer 2011. page 37.

⁶⁵ North Atlantic Treaty Organization, *The North Atlantic Treaty*, April 4, 1949. http://www.nato.int/cps/en/natolive/official_texts_17120.htm.

⁶⁶ ⁶⁶The Telecommunications Act of 1996. Pub. L. No. 104-104, 110 Stat. 56. The 1996 Telecommunications Act included a "good Samaritan" provision to protect Internet Service Providers (ISPs) from liability when they act in good faith to block or screen offensive content hosted on their systems. *Id.* § 230(c).

against thousands of computers and major government, media, and financial web-sites. The attacks were launched from at least five different control hosts in multiple countries, including the United States. The United States government turned to industry to determine the origin and character of the threat and asked the ISP's to shut down the operations and restore services.

In Germany, the Anti-Botnet-Advisory Center helps customers remove botnet threats and other malicious software from their computers. The Center is supported by a group of ISPs that informs affected customers of their infections and then *assists with specific tools* to help the customer eliminate or eradicate the infection.⁶⁷ The Center is working with Norton, Kaspersky, and Avira to provide tailored software that "cleans" customer computers of malicious software. Similarly, the Finish Communications Regulatory Authority (FICORA) directs network operators to disconnect the infected machines of its customers from the Internet until the machine is disinfected.⁶⁸

In late January 2012, the Polish government experienced multiple attacks targeting websites under the gov.pl domain. Most of the attacks were DDoS based, attributed to Anonymous, which declared radical protests after the Polish government revealed plans to sign the ACTA treaty on January 26th. Websites of the Polish Parliament, Ministry of Foreign Affairs and Internal Security Agency were among the victims of these attacks. Organizers enjoy the fact that DDoS attacks are simple and efficient. You press a button and within seconds the website stops responding. Minutes later news portals report about the incident. Collateral customers are then affected, including banks, media, telecommunications companies and Polish Railways.⁶⁹ Governments like Poland turn to their ISPs to assist in the defense of their infrastructure, and work proactively to establish countermeasures and incident response plans to mitigate and minimize the potentially devastating impact of a determined and well-resourced opponent.

As more of industry moves its services to an Internet based infrastructure, one could envision a digital crisis similar to the ash clouds over Iceland that halted air traffic around the world for days in the spring of 2010. While U.S. laws focus on shielding from liability those who choose to help in a situation they did not cause, European laws criminalize failure to help in such a situation.⁷⁰ What if, for example, the e-ticketing of several major airlines and train systems were taken off-line. The duty to assist obligation could be demanded to help restore that service so that passengers could be ticketed and tracked, and packages moved. This is not an impossible hypothetical, as a reservation systems breakdown for United Airlines stranded thousands of passengers and disrupted flights around the United States in January 2006.

Given the integrated and global nature of the Internet and the central role played by the large ISPs, it is incumbent on them to honor *the duty to assist* other ISPs both to warn of imminent danger, such as an emerging attack, and to help when an attack or outage occurs that seriously injures or disables a neighbor ISP. ISPs could deploy a hotline phone system, like the Inter-Network Operations Center Dial-By-ASN (INOC-DBA), that connects "Network Operations Centers (NOCs) and Security Incident Response Teams (IRTs) of Internet infrastructure

⁶⁷ <https://www.botfrei.de/en/ueber.html>

⁶⁸ <http://www.ficora.fi/en/index/saadokset/ohjeet.html>

⁶⁹ http://www.cert.pl/news/4856/langswitch_lang/en

⁷⁰ Benac, Nancy (1997-09-05). "Good Samaritan Laws" Common in Europe but Rare in America". *Wisconsin State Journal*: p. 7.A. ISSN 0749405X. Retrieved 2010-01-07. (Registration Required)

providers, operators of Internet exchanges, critical individuals within the Internet security, policy, emergency-response, and governance community, and equipment vendors' support personnel."⁷¹

H. Duty to avoid aiding and abetting criminal activity

The recent settlement by Google with the United States Department of Justice underscores a new responsibility for ISPs, that they have a *duty to avoid aiding and abetting criminal activity*. From 2003 to 2009, Google permitted online Canadian pharmacies to place advertisements through Google's largest advertising program - AdWords. This service facilitated the unlawful importation of controlled pharmaceuticals into the United States. In the settlement agreement, Google admitted to its knowledge of, and participation in, unlawful advertising.⁷² It is unlawful⁷³ for pharmacies outside the United States to ship prescription drugs to customers in the United States.⁷⁴ "The Department of Justice will continue to hold accountable companies who in their bid for profits violate federal law and put at risk the health and safety of American consumers," said Deputy Attorney General Cole. "This investigation is about the patently unsafe, unlawful, importation of prescription drugs by Canadian on-line pharmacies, with Google's knowledge and assistance, into the United States, directly to U.S. consumers," said U.S. Attorney Neronha. "It is about holding Google responsible for its conduct by imposing a \$500 million forfeiture, the kind of forfeiture that will not only get Google's attention, but the attention of all those who contribute to America's pill problem."⁷⁵

The Google case study suggests that as soon as the ISP or host becomes aware that a content or activity is unlawful, it could be found guilty of aiding and abetting the offense if it does not take immediate action to prevent the activity.⁷⁶ In 1999, the District Court, The Hague found an access provider was liable for having maintained a link which connected to a site containing counterfeit material:

"Declares it to be the law that by having a link on their computer systems which when activated brings about a reproduction of the works that CST (the plaintiff) has the copyright to on the screen of the user, without the consent of the plaintiffs, the Service Providers are acting unlawfully if and insofar that they have been notified of this, and moreover the correctness of the notification of this fact cannot be reasonably doubted,

⁷¹ INCO-DBA Hotline Phone Q&A, Packet Clearing House, <https://www.pch.net/inoc-dba/docs/qanda.html> (last visited Mar. 6, 2011)

⁷² <http://googlemonitor.com/wp-content/uploads/2011/05/Google%20Agreement.pdf>

⁷³ These activities violate the Federal Food, Drug, and Cosmetic Act; Title 21 United States Code, Section 331(a) and (d) (Introduction into Interstate Commerce of Misbranded or Unapproved Drugs). Where these prescription drugs are controlled substances, such conduct also violates the Controlled Substances Act, Title 21 United States Code, Section 952 (Importation of Controlled Substances).

⁷⁴ <http://googlemonitor.com/wp-content/uploads/2011/05/Google%20Agreement.pdf> and <http://betanews.com/2011/08/28/doj-pharmacy-investigation-undermines-google-credibility/>

⁷⁵ <http://www.justice.gov/opa/pr/2011/August/11-dag-1078.html>

⁷⁶ On aiding and abetting, see the article by Sébastien Canevet, "Fourniture d'accès à l'Internet et responsabilité pénale" (Provision of access to the Internet and criminal liability), available at: <http://www.canevet.com/doctrine/resp-fai.htm>

and the Service Providers have then not proceeded to remove this link from their computer system at the earliest opportunity."⁷⁷

These cases can be extended to other forms of illicit or illegal behavior conducted by customers or subscribers of those service providers. Other areas of the law substantiate this. For example, landlords can be held liable if they take inadequate precautions against criminal activity that harms tenants.⁷⁸ Entrepreneurs may be held liable if criminals use their premises to sell counterfeit or gray market goods.⁷⁹ Still others see it as a risk to their reputation. In March 2011, Microsoft decided that the Rustock botnet, the largest generator of spam in the world, was causing an Internet nuisance because it was damaging Microsoft products as well as its reputation. Accordingly, Microsoft turned to the courts to address the issue. On March 16, 2011, U.S. Marshals accompanied employees of Microsoft's digital crimes unit into Internet hosting facilities in five U.S. cities.⁸⁰ Using a federal court order, they seized the command-and-control servers that were responsible for manipulating an estimated one million computers worldwide.

Microsoft was not alone in its efforts to take down the Rustock infrastructure. The effort required collaboration between "industry, academic researchers, law enforcement agencies and governments worldwide."⁸¹ Microsoft worked with pharmaceutical company Pfizer, the network security provider FireEye, Malware Intelligence Labs and security experts at the University of Washington, each of whom attested in court to the dangers posed by Rustock and the impact on the Internet community. Additionally, Microsoft also worked with the Dutch High Tech Crime Unit within the Netherlands Police Agency to help dismantle part of the command structure for the botnet operating outside of the United States. Moreover, Microsoft worked with China's Computer Emergency Response Team (CN-CERT) to block registrations of domains in China, a pro-active approach aimed at preventing the stand-up of future command and control servers. Finally, Microsoft's digital crimes unit worked with global ISPs and CERTs around the world to remediate the infections.

Microsoft demonstrated that a multinational corporation can and should be responsible for discriminating against the illegal activity operating on service provider infrastructures. The global cooperation that it enjoyed during the takedown of the Rustock botnet suggests that others may follow-suit with a duty to avoid aiding and abetting criminal activity.

Because ISPs are a platform for global access they can also become an instrument for illicit or illegal activity. Individually, law enforcement agencies will never be able to defeat the clever

⁷⁷ http://www.coe.int/t/dghl/monitoring/ecri/legal_research/combata racism on internet/Internet_Chapter3_en.asp and See details of the case on <http://www.juriscom.net/elaw/e-law11.htm>

⁷⁸ See, for example, *Sharp v. W.H. Moore, Inc.*, 796 P.2d 506 (Idaho 1990). and Doug Lichtman and Eric Posner "Holding Internet Service Providers Accountable." Chicago John M. Olin Law & Economics Working Paper No. 217. July 2004. page 9.

⁷⁹ See, for example, *Fonovisa v. Cherry Auction*, 76 F.3d 259 (9th Cir. 1996) and Doug Lichtman and Eric Posner "Holding Internet Service Providers Accountable." Chicago John M. Olin Law & Economics Working Paper No. 217. July 2004. page 9.

⁸⁰ Bruce Sterling. Microsoft versus Rustock Botnet. Wired Magazine (online). 28 March 2011.

[http://www.wired.com/beyond_the_behond/2011/03/microsoft-versus-rustock-botnet/]

⁸¹ Bruce Sterling. Microsoft versus Rustock Botnet. Wired Magazine (online). 28 March 2011.

[http://www.wired.com/beyond_the_behond/2011/03/microsoft-versus-rustock-botnet/]

tactics and agile criminal infrastructures. Therefore, ISPs must have a *duty to avoid aiding and abetting criminal activity* and must play an important role in addressing and deterring illegal activity, fraud, and misleading and unfair practices that are conducted over their networks and services. Internet based activities should comply with the law and all parties have responsibility to improve the safety and stability of the Internet of the future, including individuals, providers, ISPs, and judicial authorities.

Conclusion

The Internet is widely viewed as both a critical infrastructure in itself and a key component of other forms of critical infrastructure, underpinning economic and social activity at a global level. This paper exposes the gap between ISPs' written responsibilities and the unwritten, yet expected ones. As illustrated by our examples, precedents are emerging around the world for ISPs to shoulder more responsibility for the stewardship of the Internet. The first three duties contain the basic functions, the expected services that an ISP should undertake as part of their participation in the global internet: (a) duty to provide a reliable and accessible conduit for traffic and services; (b) duty to provide authentic and authoritative routing information; and (c) duty to provide authentic and authoritative naming information. Networks and the platforms on which Internet users rely upon should not be susceptible to operator error or cyber attack. We can no longer be one-click away from an infection or worse yet, no service. As such, many countries are turning to their regulatory authorities to apply pressure on their ISPs to facilitate the adoption of these core functions.

The next four duties usually fall outside of a regulatory regime, yet in many ways fall within our unwritten expectations or social responsibility of ISPs to maintain the security and integrity of the Internet as a global platform for communication and commerce. These duties are echoed in a recent OECD communique entitled, "Principles for Internet Policy Making."⁸² The four duties of (d) duty to report anonymized statistics on security incidents to the public; (e) duty to educate customers about the threats; (f) duty to inform customers of apparent infections in their infrastructures; and (g) duty to warn other ISPs of imminent danger and help in emergencies, complement each other and help the Internet community to work together to stem the tide of the proliferation of malicious activity that poisons our Internet experience and infects our Internet infrastructure. Today, some ISPs limit spam, notify customers of botnet infections, and partner with law enforcement to deny the distribution of child pornography. Some ISPs might participate strictly for business purposes - to reduce fraud, infections, and unnecessary bandwidth use. Others may engage for more altruistic purposes, like brand enhancement or a differentiated "secure" service assuming responsibility for the safety of the Internet and their users, perhaps at their own expense.

Finally, while the Internet knows no specific geography, it facilitates activities between law-abiding nations. ISPs have a *duty to avoid aiding and abetting criminal activity*. Internet based activities should comply with the law and all parties have responsibility to improve the safety and stability of the Internet of the future, including individuals, providers, ISPs, and judicial authorities.

⁸² Organisation for Economic Co-operation and Development. "Communique on Principles for Internet Policy Making." Delivered at an OECD High Level Meeting, The Internet Economy: Generating Innovation and Growth. 28-29 June 2011. Paris, France.

ISPs have unparalleled visibility into global networks, which enables them with the proper tools, to detect cyber intrusions and attacks, as they are forming and transiting towards their targets. There are a limited number of ISPs that provide the world's Internet service (basic communication and enhanced services). If the leading fifteen or twenty companies were to become early adopters and market leaders for the eight duties of stewardship, they could make a significant difference in the overall security and resilience of the Internet. The top twenty-five companies in 2009 by brand value are reflected below in Table 1.

Alternatively, the top twenty Autonomous Systems (ASes) by customer cone size⁸³ could assume broader responsibility for the health and hygiene of the Internet. These twenty ASes described in Table 2, which approximately map to ISPs represent the broadest coverage of direct and indirect customer reach.⁸⁴

Regardless of the methodology chosen (i.e, market penetration or by topographic connectivity) a small number of ISPs could lead the way in ensuring the reliability, integrity, and security of the Internet as a critical infrastructure and thereby put pressure on the rest to follow. ISPs do come in many forms and sizes and go by many names: the phone company, the cable company, the wireless company, etc. They have become the stewards of the Internet: planning and managing resources, providing reliable connectivity, and ensuring delivery for traffic and services. In 2012 we should ask the ISPs to assume the *explicit and implicit* duties outlined in this paper to ensure the reliable delivery of an essential service - the Internet. Upon implementing these eight duties they will likely recognize one more unstated duty that is in the best interest of their business - to use their purchasing power to design and deploy a next generation technology that protects users and accounts for security at the onset. Afterall, meeting tomorrow's demands for network capacity, new applications, and an expanding base of users requires extending and investing in the infrastructure. Anticipating the next-generation security requirements up-front makes perfect business sense.

⁸³ Customer Cone: the set of ASes, IPv4 prefixes, or IPv4 addresses that can be reached from a given AS following only customer links.

⁸⁴ The Cooperative Association for Internet Data Analysis (CAIDA) show that the top 20 Autonomous Systems account for the majority of the IPv4 prefixes and addresses. [<http://as-rank.caida.org/>]

Rank	Brand	Parent Company	Brand Value (\$bn)
1	Vodafone	Vodafone Group	26.59
2	AT&T	AT&T	24.6
3	Verizon	Verizon Comm	24.38
4	Orange	France Telecom	18.35
5	China Mobile	China Mobile	13.87
6	Telecom Italia	Telecom Italia	9.43
7	T-Mobile	Deutsche Telekom	8.96
8	Movistar	Telefonica	7.95
9	NTT DoCoMo	NTTC	7.54
10	BT	BT Group	7.29
11	Sprint	Sprint Nextel Corp.	7.07
12	Telefonica	Telefonica	6.33
13	Alcatel-Lucent	Alcatel-Lucent	5.16
14	America Movil	America Movil	5.08
15	Telstra	Telstra Corp.	4.64
16	O2	Telefonica	4.62
17	China Unicom	China Unicom	3.45
18	Qwest	Qwest Comm Intl	3.06
19	SoftBank	Softbank Corp.	3.02
20	KDDI	KDDI Corp.	3.01
21	Telenor	Telenor	2.97
22	Swisscom	Swisscom	2.96
23	MTS	Mobil TeleSystems	2.79
24	CNC	China Netcom Group	2.55
25	Airtel	Bharti Airtel Ltd	2.48

Table 1: Top 25 Telecom Companies in the World, 2009.⁸⁵

⁸⁵ Sriram Vadlamani. "The Top 25 Telecom Companies in the World, Based on Brand." Asian Correspondent.com. 12 April 2009. <http://asiancorrespondent.com/515/top-25-telecom-companies-in-the-world-based-on-brand-value/>

AS Rank	AS Name	Customer Cone		
		Number of ASes	Percentage of all ASes	Percentage of IPv4 addresses
1	Level 3 Communications	35,753	96%	97%
2	Hurricane Electric	33,621	91%	91%
3	Global Crossing Ltd.	33,427	90%	91%
4	Metromedia Fiber Net	30,524	82%	85%
5	Tinet SpA	29,989	81%	83%
6	Sprint	28,636	77%	82%
7	NTT America Inc.	28,501	77%	81%
8	Cogent/PSI	27,722	75%	73%
9	TeliaNet Global Network	27,573	74%	74%
10	AT&T Services, Inc.	27,375	74%	81%
11	Deutsche Telekom AG	27,114	73%	76%
12	Tata Communications	26,018	70%	73%
13	MCI Communications	25,632	69%	70%
14	ReTN.Net Autonomous	25,567	69%	68%
15	Savvis	25,077	67%	71%
16	Beyond The Network A	24,854	67%	70%
17	UPC Communications	24,538	66%	69%
18	XO Communications	24,364	66%	68%
19	Swisscom	23,944	64%	66%
20	Cable and Wireless	22,897	62%	68%

Table 2: The Top Twenty ASes by Customer Cone