United Nations Educational,
Scientific and Cultural Organization

Politics of the Information Society

The Bordering and Restraining of Global Data Flows

UNESCO Publications for the Politics of the Informaion Society

UNESCO

Politics of the Information Society: The Bordering and Restraining of Global Data Flows

Gus Hosein

February 2004

Published in 2004
by the United Nations Educational, Scientific and Cultural Organization
7, place de Fontenoy, 75352 Paris 07 SP, France

Composed and printed in the workshops of UNESCO

Printed in France
CI-2004/WS/6 cld/d /15794

Table of contents

Introduction 5

I. Regulating Trans-Border Data Flows 7
On Jurisdiction and the Information Society 8
The Internet as its own Jurisdiction 10
The Internet as No Different 11
The Internet as a Unique Problem 12

II. Regulatory Challenges of the Information Society 13
Defining the Internet for Censorship 14
Defining the Internet for Surveillance 16

III. Censorship Interventions and Implications 21
Who Decides and Censors? 22
Why Censor? 23
Censorship beyond Governments I: Intellectual Property 24
Censorship beyond Governments II: Libel and Defamation 25
Politics of Filtering and Blocking 27
Filtering at the Destination ISP 28
Filtering at the End User 29

IV. Hinging on Privacy: Surveillance as Prior Restraint 33
The Right to not Identify as you Speak 34
Towards and Away from the Right to Access Anonymously 38
Chilling Speech through Mass Surveillance 40

V. Recommendations for Future Policy and Summits 45

About the Author 47

Acknowledgements 47

Introduction

In December 2003 the World Summit on the Information Society convened. Great statements were issued, declarations were proclaimed, and opportunities were sought. The timing of the event was fortunate, particularly as events in recent years have radically transformed the 'Information Society' from what it once appeared to in a dream to many, to the realities perceived by the thousands of attendees to the summit.

We once dreamed of a society bountiful in information that would feed knowledge creation, and lead to the empowerment of the individual. Borders would be irrelevant, multiculturalism would thrive, communicating would lead to enrichment, and the truth would be free. While I remain unsure if we have indeed created an 'Information Society', this 'Information Society' naturally inherits many of the challenges, opportunities and risks of the 'Real Society'. No matter what infrastructure we establish, it would be nearly impossible to escape the politics of the people in the world creating it, and the people of the world who would inhabit it.

This report illuminates the politics of this *Information Society* through focussing on the dynamics surrounding free expression and privacy. Many of the contentious policy areas in this Information Society hinge on privacy and free speech. Discourses surrounding the technology and public policy issues including the 'right to communicate', 'freedom to participate', 'incentives to create', access and the 'digital divide' all involve privacy and free expression.

Understanding the policy dynamics surrounding surveillance and censorship supports our understandings of political systems and governance within our current socio-technological environment. If we regard the information and communications infrastructures in our midst as key components of our legal, political economics and social lives and interests, we may identify the sources of control, conflict, and the challenges that we face.

Privacy and free speech are in many ways two sides of the same coin. Collisions are possible, particularly in the areas of media coverage of the personal lives or libel and defamation rules that inhibit some speech. This report focuses rather on the positive link between these rights. The interdependence of these rights and their curtailment is analysed here. The act of censorship may occur through enacting surveillance, and enacting forms of censorship may result in surveillance.

Governments and other institutions are intervening on the right of free expression using a number of regulatory mechanisms, while also chilling free speech and interactivity through increased surveillance. Technology is a key component to these strategies and mechanisms. These mechanisms are mapped out to understand how we are diminishing the open society through our legal, technological, and economic blindness.

I.

Regulating Trans-Border Data Flows

The concept of the 'Information Society' can be traced back to the 1960s, with the advent of computers and the decline of the agricultural and industrial sectors in many economies. The rise of the service sector gave rise to social change. At the same time, information technologies were increasingly being developed, adopted, and used in our daily lives. Our contemporary understanding of the concept refers now to the prevalence of advanced information and communications technologies in our lives.

The 'Information Society' is now inseparable from communications media such as the Internet, advanced mobile telephony, and other media that enable interactive communications. These communications media make use of infrastructures involving wires, cables, strands of glass and plastic, satellites and antennae around the world, enabling trans-border data flows. Using a variety of protocols individuals may now communicate across borders with ease. Service providers allow individuals to use email, news groups, and post information to bulletin boards and host websites, and allow them to *push* and *pull* data packets to and from open resources wherever they may exist.

At some point we allowed the discourse of 'The Information Society' to take over our coping mechanisms for dealing with new technologies. Now policy proposals constantly speak of the coming or advent of the Information Society, and how we must develop, sustain, and market this new Society. In language it is treated as a new place, separate from our older world. In reality, it is merely a rhetorical tool. The old world never ceased to be; it is merely coping with new technologies.

The Internet and other advanced distributed means of communicating challenged the ways in which business is conducted, technologies are developed, and policies are formulated. Individuals could use the Internet as a global marketplace, trade ideas and code applications. New policies, it was argued, would have to reflect the increase of information, and the difficulties of constraining its flow. That is, jurisdiction was being reformulated on a daily basis, and possibly even constructed by the individ-

ual, as the German citizen purchases a book from a U.S. bookshop; or the Australian programmer collaborates with the Canadian on a software application being developed in Norway.

Traditionally, the jurisdiction of government laws and powers are limited to services and servers within its geographic borders. Moreover, traditionally service providers would only have to be held accountable for the laws in place within the jurisdiction that they are physically located. If neither the servers nor the individuals involved existed within the borders of the state, then the governments could not regulate those bookshops, or the code being generated. Or that is how we used to imagine things. Such traditional views of jurisdiction have been replaced by more legally and technologically problematic interpretations.

Some countries consider a source of information to be within its jurisdiction if it can be accessed by nationals, regardless of the physical location of the server. Court decisions in France and Australia, for example, have considered U.S. websites to be under the jurisdiction of their courts, and thus to French and Australian laws. Service providers around the world are in turn placed in problematic legal situations, where they have to comply with laws from a number of jurisdictions, on top of their own national laws.

The bursting of economic bubbles and the emphasis upon global security has given rise to a new form of scepticism regarding the freedom of the Internet and the empowerment involved in the INFORMATION SOCIETY. It is now common to dismiss previous technological-optimist claims regarding the information society. Prior claims regarding 'no one knows who or where you are on the internet', or 'governments are powerless to regulate global networks' are now considered by many as unrealistic. Current articulations include claims that regulating data flows is no different than regulating other activities. The truth is most likely to be somewhere in between.

On Jurisdiction and the Information Society

Trans-national activity creates conflicts between domestic law and the international environment. That is, governments are usually entitled to enact and enforce laws within their jurisdiction; it is, after all, their sovereign right to do so. This 'principle of sovereignty' is often summarized as government's exclusive power within its own borders and virtually nowhere else.[1]

1. Jonathan W Leeds. 1998. United States International Law Enforcement Cooperation: "A Case Study in Thailand. Journal of International Law and Practice" 7 (1):1-14.

There are conditions, however, that arise where this sovereign right is questioned, where conflicts result. One such conflict arises when there is an overflow of activity from abroad. That is, an activity occurs from beyond the jurisdiction that affects the ability of the sovereign jurisdiction to enforce its laws. A second conflict arises when the very ability of a jurisdiction to enact laws is weakened by doubts regarding the ability to enforce rules due to the environment of regulation.

These problems are not unique to the Information Society. Consider a country that decides to pass a law banning the development of a specific drug. The effectiveness of the regulation is questionable if another country does not have this same regulation. Unless the first country can prevent the drug from entering at all entry points, the drug will be available in contravention of the spirit of the law. Similarly for environmental controls: strict controls on air pollution creation in one state may make no difference if a bordering state has no similar controls thus creating an overflow. In each case, the regulation continues to incur costs and burdens without regard to its effectiveness.

With data flows within digital networks and the associated products and services, these conflicts are exacerbated. Action may be conducted from a distance, where the overflow of activity can occur without an individual having to physically enter the jurisdiction. Creating border controls in such a situation becomes even more challenging, on a technological level, affecting the interests of any number of countries, non-governmental organizations, and industries.

Consider one of the earliest policy problems faced by governments: cryptography policy. Governments wished to regulate the use of some software applications, but at the same time were practically powerless to prevent individuals in open democratic states from downloading these applications from other jurisdictions. Other concerns also arose, emphasizing the Information Society and Electronic Commerce. These included concerns regarding the perceived imperatives to develop more communications networks and reduce costs of access, concerns regarding the impediments to conducting business and harming national economies, and concerns regarding the impacts upon civil liberties. In time, the regulations failed, for the most part.

Since then, government have taken lessons from previous policy failures. Trans-border data flows were a clear and present hazard to the establishment of national policy. Data flows did not respect jurisdictions.

The Internet as its own Jurisdiction

One way of looking at this situation is to imagine that the Internet is a jurisdiction of its own, and should be treated as such. Under traditional notions of sovereignty and jurisdiction, governments relied on borders to enable their power, give effect to their rules, create legitimacy to their action, and notice to those who were regulated. According to a famous article by two legal experts on law and the Internet, Johnson and Post,

> The rise of the global computer network is destroying the link between geographical location and: (1) the power of local governments to assert control over online behavior; (2) the effects of online behavior on individuals or things; (3) the legitimacy of the efforts of a local sovereign to enforce rules applicable to global phenomena; and (4) the ability of physical location to give notice of which sets of rules apply.[2]

In effect, the Internet and its 'cyberspace' challenged the sovereignty of governments. The Internet and trans-border dataflows created overflow effects because of the idea of action at a distance. Also, as the argument goes, the Internet's architecture created an environment that resisted government action. At a time when governments were trying to regulate through domestic initiatives such as cryptography policy, Johnson and Post advised that

> Many of the jurisdictional and substantive quandaries raised by border-crossing electronic communications could be resolved by one simple principle: conceiving of Cyberspace as a distinct "place" for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the "real world."

Their fear was not that national action and national policy were futile, but that they were dangerous within our socio-technological environment. Perhaps applying regulation limited by geographic-borders to an un-bordered environment would be senseless. More importantly, regulation by one jurisdiction will have spill-overs immediately upon another because of the un-bordered nature of cyberspace.

To put it simply, if the U.S. were to regulate a specific form of speech, and since much of the Internet exists within the U.S. then this would have the effect of regulating that speech elsewhere. Another instance is the French court case implicating Yahoo! for enabling the auctioning of Nazi memorabilia.[3] Yahoo! was ordered to prevent French

2. David R. Johnson and David G. Post, "Law and Borders–the Rise of Law in Cyberspace," *Stanford Law Review* (1996).
3. For a good overview of the case, see Yaman Akdeniz, "Case Analysis of League against Racism and Antisemitism (Licra), French Union of Jewish Students, v. Yahoo! Inc. (USA), Yahoo France, Tribunale De Grande Instance De Paris, Interim Court Order, 20 November 2000.," *Electronic Business Law Reports* 1, no. 3 (2001).

nationals from accessing the sections of its website that traded in Nazi artefacts. The challenges of identifying 'French nationals' whilst online are significant, however. Eventually Yahoo! prevented all users in all countries from accessing the auctions-site. In the first case, an American rule would have de facto effects upon the rest of the world; in the second, a French rule would spill-over and affect all other jurisdictions.

The Internet as No Different

Another way of looking at this problem is to treat the 'Information Society', 'cyberspace', and the Internet just as we have treated all other forms of trans-national activity. Cyberspace transactions are not all that different from other trans-national transactions, in that they involve people in 'real space' in different territorial jurisdictions causing 'real-world' actions and effects.

In this sense, cyberspace transactions do not inherently warrant any more deference by national regulators.[4] A policy established by one country will always affect another. There is nothing new with the Internet.

Since the changes in transportation and communications technologies in the first half of the 20th century, multi-jurisdictional activity became common. This coincided with the rise of the regulatory state, and despite the concerns of jurisdictional arbitrage, conflicts of jurisdictions became well understood. Even in legal cases dealing with multiple jurisdictions, courts applied universal customary laws tied to no particular sovereign authority, such as law merchant, the law maritime, or the law of nations.[5]

Now international law permits states to apply its law to extraterritorial behaviour with substantial local effects. According to the leading legal expert on this approach,

> In modern times a transaction can legitimately be regulated by the jurisdiction where the transaction occurs, the jurisdictions where significant effects of the transaction are felt, and the jurisdictions where the parties burdened by the regulation are from.[6]

In truth, countries have been regulating data flows successfully. The European Union finalized a harmonizing directive on data protection in 1995 that included two articles regulating transborder data flows.[7] Countries as diverse as Australia, China, and

4. Jack. L Goldsmith, "Against Cyberanarchy," *University of Chicago Law Review* 65 (1998).
5. Jack. L Goldsmith, "Symposium on the Internet and Legal Theory: Regulation of the Internet: Three Persistent Fallacies," *Chicago-Kent Law Review* 73 (1998).
6. Goldsmith, "Against Cyberanarchy."
7. European Union, "Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data," (1995).

Saudi Arabia have implemented censorship regulations to control what kind of information is sent, received, or both; despite claims of infeasibility and error.

Every new technology in a sense disrupts existing legal regimes. The telegraph dramatically increased the speed and amount of communications, reducing communication time from weeks and months to hours and minutes. Similarly, the telephone reduced the cost and enhanced the frequency and privacy of international communication.[8] The Internet does disrupt our existing practices just as the other infrastructures have, but the Internet does so in some intriguing ways.

The Internet as a Unique Problem

To say that nothing is different now is to be blind to specific changes, problems, and opportunities arising from the development and adoption of the Information Society. Governments often argue that they are merely 'updating' their laws to cater for new technological environment, hoping to minimize debate by referring to major policy change as a natural and uncontroversial event.

Trans-national conflicts have often been resolved through the harmonization of laws. With regards to the Internet, we have seen initiatives emerging from the United Nations, the Council of Europe, the Organizations for Security and Cooperation in Europe, and the Group of 8 industrialized countries to deal with these updates, conflicts, and differences in legal systems. Most recently the World Summit on the Information Society can be seen as a nexus of information sharing on how to effectively regulate economic, social, and criminal conduct across borders.

Trying to treat data flows in the networked environment as we have treated them in the past is problematic. New challenges exist no matter how hard we try to pretend that the new technologies are similar to previous technologies. New technologies may warrant new legal techniques, which may in turn create new conflicts to our international legal norms. Finally, differences between governing systems always exist, and no level of harmonization will adequately protect individual rights.

So we return to the discussion regarding the 'Information Society' and the politics surrounding it. The first approach to jurisdiction and the Internet warned against spill-over effects of national regulations. The second approach warned against treating the Internet as something remarkably different from other trans-national conduct. Where does this leave the role of government in the 'Information Society'? This is where we enter the realm of technology politics.

8. Goldsmith, "Against Cyberanarchy."

II.

Regulatory Challenges of the Information Society

The 'Information Society ' is merely a rhetorical tool; a device for understanding and differentiating between what has come before and what is going on now. 'Cyberspace ' is also a rhetorical tool. What we need to understand is how our 'real world ' structures of laws, regulations, and practices are affected by the information and communication technologies that are constituents of this 'Information Society '. The dream of creating a new society was merely that; the reality is that we exist within our societies with new technologies alongside existing laws, markets, practices, and norms.

The Internet is a forum for interaction and communication, a multiplicity of telecommunications protocols and distributed technologies around the world, ever changing. It is also a social phenomenon, with greater numbers of users in more and more countries. Simultaneously, it is an interactive marketplace that enables electronic commerce, electronic trading and other forms of electronic transactions. It is also the greatest library, the greatest enabler to learning and communication; while being the largest depository of pornography and *indecent and harmful* information ever created. The Internet is a key component of our daily lives.

Is the Information Society separate from what we have known before? Absolutely yes, but no. Are the Internet and its trans-national activity any different from the telegraph and the telephone? Less momentous in many ways, but yes. And finally, are the forms and functions of government any different because of global communications networks? The answer is yes, and dangerously so.

Modern information and communications technologies do present some challenges and opportunities to governments. Already we have shown how the issue of jurisdiction raises problems for governments to regulate; and raises problems when they do regulate. The regulatory challenges go beyond trans-border issues, however. Another challenge is to ascertain how to fit communications infrastructures such as the Internet into the body of regulatory practices. Simply put, do we treat the Internet the same way we treat telephones, television, radio, or print media?

Are users of the Internet potential broadcasters or are they merely individuals communicating point-to-point? The answer to this question has implications for how we regard the institutions that provide internet communications services. Regulating Internet Service Providers (ISPs) as a carrier, like telephone companies, alleviates some of the responsibility of control over content from ISPs, but subjects them to the vast array of telecommunications regulations. Viewing the Internet as a broadcast medium like television and radio makes Internet Service Providers responsible for the content going through their pipes. Sometimes ISPs, depending on their business model, take on the liability through the services provided; mostly, however, the liability is decided by law.

Updating laws to deal with the Internet is in essence the process of deciding whether the Internet is a broadcast medium, a content-neutral medium, or a carrier, among other options. Liability regimes for companies vary based on the regulatory approach adopted by national governments. Notably, according to Algerian law all ISPs must take responsibility for the content of sites hosted; Swiss law only places liability upon the ISP if the true author can not be identified; in Hungary free-web space service providers are not responsible for the content unless the ISP is aware that the sites infringe the law and don't act against it; and the current legal thinking in the United Kingdom is that ISPs are regarded more like 'secondary publishers', like bookstores and archives, rather than a common carrier.

Defining the Internet for Censorship

Governments traditionally regulate content in the broadcasting industry. It is natural to try to apply those rules to the Internet.

The situation in Australia provides an example of the challenges that arise. Consider the statement of a proponent of government regulation, the Deputy Chairman of the Australian Broadcasting Authority:

> Broadcasting and now the Internet make use of public property, the airwaves and bandwidth. Broadcasting remains, and the Internet is clearly emerging as, a means of mass communication of a particularly intrusive nature. (...)
>
> It is essential for policy makers and legislators, as they review existing and prepare new rules for broadcasting and the Internet, to revisit and restate the public interest objectives they believe should apply to those industries and their governance.[9]

9. Australian Broadcasting Authority. 1999. "Broadcasting, co-regulation and the public good," NR 101/1999, 29 October 1999.

This regulator interprets the Internet as a 'means of mass communication', thus falling under the remit of the ABA alongside the regulation of television services. In turn, the ABA acts within its remit to pursue its goal of meeting the public interest for content controls.

The Internet is not the same as television, however. A critic of the government policy to censor national content and to block international content, Professor Roger Clarke responds:

> What is appalling about this statement, the government 's policy, and the legislation that was passed by the Opposition-controlled Senate as well as the Government-controlled House, is that it is framed in blithe ignorance of the nature of the technology and hence of the behaviour that it pretends to regulate. This results in no advantages to the intended beneficiaries, and is to the serious detriment of all involved.[10]

His claim is supported by many others, many of who disagree with censorship. Similar articulations arose from the Australian hacker community,[11] who also advised individuals on the means of circumventing the controls, using encryption, point-to-point connections, proxy connections, and many other technological resources.

Proponents of censorship often turn to introducing new technological resources of their own. Early in the policy debates, rating systems for content were proposed, similar to those in the movie and television industry. Under this scheme, files and websites were to be attributed with a rating. The American Civil Liberties Union responded with a report countering the film and television industry view of the Internet: that because of the *culture, economy, and structure of the Internet* such a rating system would be impractical, particularly due to international arbitrage and concerns for the burdens upon small business.[12]

Another technological resource introduced by proponents of censorship worldwide is client-side filters that would prevent users from accessing 'indecent files'. This is similar to the policy developed in the U.S. to implement V-Chips in all televisions so as to prevent viewing of indecent material, as rated by the television broadcasters.

10. Roger Clarke, "Subject: Aba Demonstrates Its Ignorance to the World," *Forwarded to the Politech Mailing List, message titled FC: More on Australian official demanding Net-regulation – demonstrating ignorance to the world,* November 3 10:42:30 -0800 1999.
11. Dogcow, "Evading the Broadcasting Services Amendment (Online Services) Act 1999," (2600 Australia, 1999).
12. ACLU, "Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet," (American Civil Liberties Union, 1997).

Filters on the Internet are much more problematic, however. A number of reports released by academics and non-governmental organisations have interrogated the capacities of the filters and showed that because of the *nature of the Internet*, its distribution, and the challenge behind creating sufficient automated verification of decency, these filters would also block some 'non indecent' content. Additionally, some indecent material still was not filtered. Some reports claim that these filters are not at all *objective*, they block web sites that opposed the interests of the developers, such as free speech organisations.[13]

Interesting issues also arose with the first formal policy process on Internet-content regulation in the U.S. In the 1990s, the U.S. Congress passed a law ordering age-verification controls to be present on 'indecent' websites. When the Communications Decency Act was struck down by the courts in *ACLU v. Reno*, the argument was that it was too difficult to ascertain what constitutes 'indecent' information, even while restricting access based on the age of consent was also technologically challenging and costly. The court stated that "any content-based regulation of the Internet, no matter how benign the purpose, could burn the global village to roast the pig", and this was "due to the nature of the Internet" and the U.S. Constitution.[14] The court recognised that the Internet was unlike any communications infrastructure previously constructed, and it had the capacity of forming an empowering force for individuals. Efforts to regulate it must proceed cautiously, they argued. The CDA was not such a process.

Numerous countries have followed from what the U.S. Congress began through establishing their own laws on regulating content. Attempts to regulate the liability faced by Internet Service Providers have emerged; to require authentication measures for speech that is deemed indecent; to require the implementation of filtering at ISPs and gateways; to advocate the use of filtering software by consumers; among other regulatory strategies and mechanisms. The faults and dangers identified in the early stages of the censorship debate in the U.S. continue to apply, however. This has not stopped international governmental organizations from advocating changes to law to prevent indecent or harmful information from being published.

Defining the Internet for Surveillance

Governments traditionally have rules on communications surveillance. Born out of

13. Electronic Privacy Information Center, "Faulty Filters: How Content Filters Block Access to Kid-Friendly Information on the Internet," (1997).
14. "ACLU v. Reno." United States District Court for the Eastern District of Pennsylvania, 1996.

practices to intercept post, telegraph, and wireless telegraphy, the 20th century saw the emergence of laws to permit the interception of communications over the telephone system. There are now frequent attempts to 'update' these communications surveillance laws to include the Internet. Put simply, governments are also trying to regulate the Internet as a telephone system.

The United Kingdom, for example, passed the Regulation of Investigatory Powers Act in 2000, extending its power to intercept communications to the Internet. The government at the time argued that none of the sought powers are new. The law applied to all communications service providers, so that "a level playing field should apply across all types of industry, and it enshrines in statute the existing principle that service providers should maintain a reasonable intercept facility."[15] The Internet service provision industry is to be regulated in the same form as the telephone industry in an effort to harmonize the regulatory landscape between industries.

The U.S. policy to date is to require all telephone companies to have a surveillance capability, though this has not yet extended to Internet service providers. At the time that this report was written, there were efforts to include Internet voice telephony (VoIP – Voice over IP) under U.S. laws requiring intercept capabilities to be embedded into the service.

This would build from earlier initiatives by the U.S. Government. In 1999 the Department of Justice appealed to the Internet Engineering Task Force (IETF) to develop a protocol for the Internet that allowed for wiretapping. The nature of the 'voice' of the IETF was democratic where all members had a vote, and anyone can be a member. After a lengthy debate, the IETF decided against creating such a protocol. Some dissented, as they believed that the IETF could (and should) create a deterministic protocol for wiretapping that could be used around the world; but deterministic in the sense that it required the use of a high-safeguarded warrant regime technologically. Some felt that an opportunity was thus missed. According to Stewart Baker, former general counsel to the NSA,

> The IETF 's (...) refusal to consider this issue was hailed as a civil liberties victory at the time. In fact, it has had the ironic effect of making it more likely that wiretap solutions will be proprietary and designed in quiet consultation with the FBI. Bottom line: the notion that the Net inherently resists government control is in for a bad decade.[16]

15. House of Commons. 2000. "Second Reading of the Regulation of Investigatory Powers Bill," by Jack Straw, Home Secretary. 6 March, 2000.
16. Stewart Baker, "Re: Metaswitch Embeds Police Spy Features in New Net-Phone Switch," (Politech Mailing List, 2003).

Discussions were thus taken out of open fora, and alternative techniques were developed. The U.S. deployed Carnivore, now entitled DCS 1000, a computer system that is attached to the network of ISPs and records traffic.

Treating the Internet like the telephone system also enables the surveillance of 'traffic data'. In the days of plain old telephone systems, after much legal debate, the content of communications were considered sensitive and therefore any breach of confidentiality required constraint. These 'constraints' usually involve warrants, e.g. judicial warrants in the U.S., politician-authorised warrants in the United Kingdom. The same rule did not apply to traffic data, however. This data includes the numbers called, calling numbers, and time. It was considered less invasive to collect and disclose traffic data, and therefore only required minimal constraint. It was particularly helpful that traffic data was stored by telephone companies and thus available to law enforcement authorities. Communications content were not, routinely at least, kept by telephone companies, so this reduced the burden for telephone companies to adhere to the law: traffic data was available, legally less sensitive, and so accessible to governments.

By placing the Internet in the same category as telephone companies, governments are able to gain access to Internet traffic data, as collected at ISPs. The information collected under the legal language of 'traffic data' is radically different on the Internet, however. It includes all the addresses to which you sent emails, all the servers to which you connected, all the people with whom you have chatted, possibly all the websites you have visited, pages you have looked at, and issues you have researched. The Council of Europe has noted:

> The collection of this data may, in some situations, permit the compilation of a profile of a person 's interests, associates and social context. Accordingly Parties should bear such considerations in mind when establishing the appropriate safeguards and legal prerequisites for undertaking such measures.[17]

Regardless, most laws grant to governments easy access to this 'traffic data', regardless of how sensitive this data may be, and how different it is from telephone traffic data.

A more complex approach was taken by the U.S. Government, under successive White House Administrations. The Clinton Administration first announced its intention to update lawful access powers to include cable-based internet connections,

17. Council of Europe, "Explanatory Report to the Convention on Cybercrime, ETS No.185," (Strasbourg: 2001).

proposing "amendments [that] will update the statutes in outmoded language that are hardware specific so that they are technologically neutral".[18] This 'outmoded language' was contained in the Cable Act of 1984. The Cable Act protects cable traffic data, or television viewing preferences, to a degree greater than even the content of communications. While the Clinton Administration failed to achieve a change in law for the treatment of Internet traffic data generated by Cable companies, the Bush Administration was more successful in October 2001 in the USA-PATRIOT Act. The USA-PATRIOT Act amended the Cable Act so that when Cable companies provided internet services, access to traffic data would be provided to law enforcement agencies under the same regime as telephone traffic data, a significantly weaker protection. This was heralded by the Attorney General.

> Agents will be directed to take advantage of new, technologically neutral standards for intelligence gathering. (...) Investigators will be directed to pursue aggressively terrorists on the internet. New authority in the legislation permits the use of devices that capture senders and receivers addresses associated with communications on the internet.[19]

The law permits access to much more information, even more than television viewing habits. The data includes email addresses, telephone numbers, websites viewed, possibly search terms, locations, and files downloaded. Yet the law protects this sensitive data as thought it was trivial.

The Internet is thus defined as a broadcast medium when it is useful to advancing the interests of government for censorship; but is defined as a telephone communications infrastructure when it advances the interests of government to conduct surveillance with minimal restraint. Neither interpretation reflects the reality of the technology or the invasiveness of the controls.

18. John Podesta, "Speech by the White House Chief of Staff on Cybersecurity," (Washington, D.C.: National Press Club, 2000).
19. Senate Committee on the Judiciary, *Testimony of the Attorney General*, September 25, 2001.

III.

Censorship Interventions and Implications

There was a time when the adage that 'the internet interprets censorship as damage and routes around it' could have been true. The situation is vastly different now. It may be dangerous for individual nation-states to establish jurisdictions over global data flows. Regardless, governments are creating laws to censor speech and conduct surveillance of individuals. Similarly, there are hazards involved in defining the Internet the same way we treat other communications infrastructures. Again, governments continue to do so usually to advance their abilities to regulate data flows and to conduct surveillance.[20]

A number of mechanisms are used to achieve censorship. These mechanisms are deployed at the sources of control within the Internet architecture. These sources include the source of the speech, the source Internet Service Provider, the destination ISP, and the destination of the speech or the end-user.[21] The mechanisms used to regulate these sources include

- direct rules controlling what content can be expressed and accessed
- requirements to install filters and other technological means to block data flows
- licensing regimes for expression, transmission, and reception
- liability regimes for source speakers and ISPs
- defamation and libel rules
- copyright and intellectual property regimes

among others. These mechanisms are used together or individually depending on the case.

Using these various mechanisms, data flows are controlled in the name decency, security, and morality. Filters may be established at the destination ISP to block a user

20. Others have performed reviews of the laws established around the world to censor information or to regulate free expression. The leading report in this area is the Silenced report from the GreenNet Educational Trust and Privacy International. C.f. GreenNet Educational Trust and Privacy International, "Silenced: An International Report on Censorship and Control of the Internet," (London: 2003).
21. Jonathan Zittrain, "Internet Points of Control," *Boston College Law Review* 43, no. 1 (2003).

from accessing information that is deemed harmful. Individuals may be compelled to use the filters deployed on their computers within cybercafés or at public libraries. Those wishing to express themselves may be made subject to libel laws that usually require identification, and in turn some form of licensing of ISPs. Licensing of ISPs may also place a liability on ISPs for the content that they may host. Finally, ISPs may be demanded to remove hosted content, and to disclose information regarding the individual who posted the questionable content. Many, if not all these powers may be invoked under intellectual property law.

Who Decides and Censors?

There are impediments to gaining access to the Internet that may not always be seen as a direct influence of governmental power. In a number of countries, the cost of access is prohibitively high, allowing access by the national elite only. Market structure contributes to this problem in some regimes, where government near-monopolies in countries like Bahrain, Burma, Belarus, Tunisia and Liberia serve the dual-purpose of limiting market access and ensuring government control. Even market diversity doesn't promise a problem-free regime, however. In Bangladesh, the government cut off lines of sixty service providers, on grounds that they did not get their licenses renewed; but providers argued that the interruption of service was intended to force them to stop providing internet-telephony in order to preserve the state voice-telecommunications monopoly.

In the days of monopolistic telephone service providers and state-run enterprises, regulators were scarce and rules were enforced directly by governments. Now, from country to country, the authority that oversees the regulatory process varies; some are government departments, others are regulators, and in some situations they are independent bodies. Government departments regulate in Switzerland (where the police have sent letters directly to ISPs to block racist content), Italy (National Security Committee and Ministry of Communications), Laos (a committee including a number of ministries that establishes rules for Internet users), and Tunisia (Tunisian Internet Agency, which is part of the Telecommunications Ministry). Regulatory bodies are responsible for deciding appropriate content in Australia (Australian Broadcasting Authority can issue take-down orders to ISPs in Australia), India (Communications Commission of India), South Korea (Information Communication Ethics Committee can remove content without court orders), and Hungary (National Radio and Television Council).

Regulators may still contain government members, and may be heavily influenced by government. Some countries with such a model include the United Kingdom's Internet Watch Foundation created at first to fend-off regulation. Hungary also has a Content Providers' Association, with similar origins to the IWF but has become more problematic with proposals regarding anti-porn filters, the erasure of 'vulgar and aggressive expression' or anything against 'good taste' and has made recommendations regarding potential copyright offences. The continuing challenge, however, is that these authorities are all bound by geography.

Why Censor?

The purposes for which speech is controlled or constrained are broad, and vary. The number of varying and fragmented definitions of 'indecent' speech is alarming. Some of the most exemplary are listed here.

Censorship occurs in many countries to protect national security, but what 'security reasons' means in the Cote D'Ivoire compared to 'public security and national harmony' in Singapore remains to be known and compared. Egyptian law censors content to defend 'public morals', regulating faulty or ill-motivated rumours or agitating news if the objective thereof is to disturb public order, induce fear in people, or causing harm to public interest. The Egyptian laws have been invoked frequently.[22]

Peru has banned information that is 'contrary to moral or good customs'. Morocco's laws have been used to arrest newspaper editors for insulting the king, and for publishing a communiqué from an Islamist group,[23] while other 'taboos' include questioning Morocco's claim to Western Africa. Tunisia dissuades any commentary that implies criticism of government policies. Zimbabwe regulates anything that is 'likely to cause alarm of despondency', carrying a prison sentence of up to seven years. Australia regulates content that is unsuitable for minors.

China censors information that disturbs state order, reveals state secrets, and harms the country's honour; and also filters some pornographic sites. India censors material that is 'lascivious' or that 'appeals to the prurient interest'. Websites are blacked-out if they promote hate, slander, defamation, gambling and racism, violence and terrorism, pornography including child pornography and violent sex. Alongside

22. Glenn Frankel. 2004. "Egypt Muzzles Calls for Democracy." Washington Post, January 6, 2004, A01.
23. Committee to Protect Journalists, " CPJ Delegation Meets with Moroccan Ambassador: Calls for Immediate Release of Jailed Editors," (New York: 2003).

content that depicts incest, paedophilia, bestiality, and necrophilia, Singapore further regulates content that promotes homosexuality and lesbianism. South Korea has a court case pending on whether it is constitutional to continue to regulate content that relates to lesbianism and homosexuality.

Many continental European countries ban content that promotes racism or xenophobia. The Council of Europe is promoting a harmonizing measure to ensure that all member states criminalize such speech, and order its take-down from websites within the CoE. These countries also have advanced structures for libel and defamation.

While the U.S. Government may be more constrained at regulating speech due to the U.S. Constitution and its jurisprudence, other forms of censorship arise. For example, consumers are constrained by Terms of Services of providers that actually limit the constitutional rights of users, permitting some speech and activity, while restricting speech and access that is otherwise legal.[24] Industry and private actors are thus implicated in the censoring of data flows.

Censorship beyond Governments I: Intellectual Property

Most discussions of censorship tend to focus on government action. The concern regarding censorship and controls of data flows should instead focus on the mechanisms exerted at the sources of control. Industry, particularly when it aligns with governments, can be a powerful source of censorship. In the name of copyright and intellectual property protection, alarming laws are passed and practices are accepted.

Some of these legal practices actually represent collisions of interests among industries and sectors. For example, Canada banned the provision of video streaming, because it interfered with previous regimes on broadcasting. Denmark and Hungary have tenuous legal situations for the act of 'deep linking', banning portal-sites from linking to specific articles on other news sites instead sending individuals through the front pages of these news sources. In the U.S. the content industry and the communications industry are in legal conflicts over the release of subscriber details of Peer-to-Peer service users.

In other situations, however, a collusion of interests arises. In contrast to the case in the U.S., Belgium has lead the way in 2000 with the tracking of users who use

24. Sandra Braman and Stephanie Lynch, "Advantage ISP: Terms of Service as Media Law – a Comparative Study," (University of Alabama, 2002).

Peer-to-Peer applications, where ISPs provide names of their users to the music industry under a 'gentleman's agreement'.

Copyright law in the U.S. goes even further. Publishing the means to circumvent copyright protection mechanisms may be subject to prosecution under the 1998 Digital Millennium Copyright Act (DMCA). Under the law this is an offence even if the individuals who published the material are not in the U.S. In 2001, for example, Dmitry Sklyarov, the Russian computer programmer who wrote software by-passing the copyright protection in Adobe eBooks, was arrested at a hacker convention in Las Vegas where he'd given a talk about his work. In the end, he was not personally prosecuted, although Elcomsoft, the Moscow company for which he worked, was. The jury acquitted Elcomsoft, in part because writing the software was not illegal in Russia. In another case, when a 16-year-old Norwegian student named Jon Johansson wrote the software DeCSS to by-pass the system that protects commercial DVDs, he was subjected to charges by the Motion Picture Association of America, again under the DMCA. The MPAA did not stop there, however: it also sued anyone who only linked to the software, including Eric Corley, the editor of 2600: the Hacker Quarterly, who (along with many others around the Web) linked to DeCSS from the magazine's Web site.

Increasingly the world is following the U.S. in the realm of copyright. Europe is establishing a regulatory regime analogous to the U.S.'s DMCA. This will have disastrous effects on speech when combined with European surveillance regimes. Meanwhile, Australia and Canada appear ready to adopt both the intellectual property regime of the U.S. and the surveillance practices of Europe.

Censorship beyond Governments II: Libel and Defamation

Individuals and groups may also have the power to censor the conduct of others in the realm of libel and defamation.

In a study in the United Kingdom, the Law Commission[25] found that some ISPs received over a hundred complaints a year from solicitors and individuals claiming defamatory material hosted or facilitated at these ISPs. The majority of the letters appeared to be from solicitors complaining about web sites created by disgruntled customers. Unfortunately, the Commission admitted that the safest course of action for the recipients of these letters of complaint is to remove the material 'without regard to the

25. Law Commission, "Law Commission Report on Defamation and the Internet: A Preliminary Investigation," (London: Law Commission of England and Wales, 2002).

public interest or truthfulness'. This is because of the questionable legal status of ISPs under British law. The Law Commission worries that campaigning groups are most likely to be susceptible and subject to such letters. This legal regime comes dangerously close to chilling political speech.

So long as ISPs are regarded as 'secondary publishers' or somehow responsible for the content hosted by their services, they are likely to be held liable. The Law Commission sees one possibility is to exempt ISPs from liability completely, as in the U.S. Alternatively, clearer guidance is required as to the status of ISPs as publishers, archivists, or mere conduits and carriers.

Additional attention must also be given to the arising jurisdictional problems in libel and defamation cases. Increasingly ISPs and content providers are at risk from libel and defamation laws around the world. Such a case arose in Australia, where the Australian courts decided that a libel case held against Dow Jones, based in New York, was within its jurisdiction. A Canadian court has recently ruled similarly using the Australian case as an example. The ruling claims that an article written by the Washington Post when an individual was living and working in Kenya could be tried in Canadian courts years later, as the newspaper should have "foreseen that the story would follow the plaintiff wherever he resided".[26] The European Union, working to resolve the conflicts of laws in defamation action, is establishing that anyone posting to the Internet will be subject to defamation laws of every member state of the EU.[27] Another Canadian court recently concluded that defamation conducted whilst anonymous carries "a greater risk that the defamatory remarks are believed", concluding that higher damages should be paid by those who libel others over the Internet.[28]

This situation, if not appropriately addressed, could lead to a situation where we have censorship by virtue of legal intimidation. This could occur through either the intimidation of an ISP or the intimidation of an individual, chilling his right to speech.

Defamation laws have been used by governments, too. Some countries make defamation a criminal act. The Singaporean government has filed defamation suits against opponents. Similarly, the Georgian defamation law is used to shield the gov-

26. See coverage of the case by Michael Geist, "Web Decision extends long arm of Ontario law," The Toronto Star, February 16, 2004.
27. Article 19, Press Release: "ARTICLE 19 concerned that proposed Rome II Regulations pose threat to Internet publishers' freedom of expression," January 14, 2004.
28. Patrick Brethour, "Net Libel Open to Higher Damages: Judge says anonymous Web postings can magnify impact of defamatory comments," Globe and Mail, February 11, 2004.

ernment from media scrutiny, using both civil and criminal sanctions, with the government suggesting the introduction of lengthier sentences for defamation of public officials. According to Article 19, the Global Campaign for Free Expression,[29]

- defamation should be decriminalised;
- public bodies, including bodies forming part of the legislative, executive or judicial branches of government, should be barred from suing in defamation;
- statements of opinion, as opposed to factual accusations, should not be actionable in defamation;
- Internet Service Providers and others performing similar functions should be shielded from liability;
- there should be a defence of reasonable publication;
- damages awarded should always be proportionate to the harm suffered, and a fixed ceiling be established for non-material harm.

Censorship need not be written on the books of law; the mere fact that the books containing the laws may be perceived by the layman as an indication of fault and error may lead to censorship.

Politics of Filtering and Blocking

The Web is probably the simplest of all applications to censor, in that a Web site is usually created by an identifiable individual and hosted on a commercial service. The would-be censor therefore has many options: contact the hosting ISP to ask that the site be taken down; arrest or sue the originating individual; or add the Web site's address to the database of sites citizens and/or consumers may not visit. All these methods have been used. The one risk in the case of the first two of these options is that removing a controversial Web site can sometimes be taken up as a cause célèbre by the rest of the Net, with citizens of countries outside the purview of the censor establishing sites mirroring the original content as a protest.

Blocking technology is often used, but to be effective it must be implemented robustly. The risk is that users will figure out a way around it, such as by using anonymising (proxy) Web sites or accessing the content via other effective proxies such as the "cache" option on the search engine Google. Both function by acting as an intermediary, receiving the Web site and displaying it for you. This is the virtual equivalent

29. Article 19, "Harsh Georgian Defamation Laws Must Be Amended," (London: The Global Campaign for Free Expression, 2004).

of sending an unknown assistant to a bookstore to buy you a copy of a book you were banned from reading.

The technologies and techniques of blocking and monitoring are developed through politics, for specific tasks, and also limited by technical means. The source of the blocking can be either at the ISP or at the end-user.

Filtering at the Destination ISP

Blocking selected Web sites may be carried out at the national level, but this may be conducted ideally in countries with limited numbers of ISPs. In such cases, access to the Internet does not follow from a decentralised model but rather goes through a government-run firm that is responsible for monitoring and blocking access.

China is renowned for its 'Golden Shield' that restricts Chinese citizens from accessing information from servers outside of China. The method of filtering, according to analyses from the Harvard University Berkman Center for Internet & Society, involves packet-level filtering integrated into routers at the border. Keyword filtering also occurs, so that a file downloaded from a server that is not otherwise filtered can also be rendered inaccessible. In their study, the researchers found that Google searches in China for 'justice china' , 'dissident china' resulted in less than half the results being blocked. Meanwhile, the servers for BBC, CNN, Time, PBS, and other major news sites were blocked. Blocking is not always consistent, however, as the researchers found that Reuters was blocked for a period of time, but then unblocked; similarly for the Washington Post.[30]

The researchers from the Berkman Center conducted a similar study on blocking done in Saudi Arabia.[31] In Saudi Arabia all web traffic is forwarded through the government's Internet Services Unit, which filters data to preserve "Islamic values". This includes blocking sexually explicit content and pages that relate to drugs, bombs, alcohol, gambling, and pages insulting Islam. The researchers found that some sites regarding religions were blocked, as well as some sites about humour, music, movies, and content relating to homosexuality. Health pages, educational sites such as the Women in American History section of the Encyclopaedia Britannica Online, the Anne Frank House, and sites regarding Middle Eastern politics were also blocked.

30. Jonathan Zittrain and Benjamin Edelman, "Internet Filtering in China," *IEEE Internet Computing*, March-April (2003).
31. Jonathan Zittrain and Benjamin Edelman, "Documentation of Internet Filtering in Saudi Arabia," (Berkman Center for Internet and Society, 2002).

A final exemplar of ISP-filtering arises in the state of Pennsylvania. Pennsylvania has a law requiring that ISPs filter, at the level of the internet-protocol, designated websites that distribute child pornography. The Berkman Center researchers[32] find that this is highly problematic because 87.3% of active .com, .net, and .org websites actually share IP addresses. This means that any designated IP-address that is blocked because of one website that is disabled by the Pennsylvania rule would result in any number of additional, unrelated websites being blocked as well. An additional problem is that since U.S.-based ISPs service Pennsylvanian users and are unable to differentiate them from non-Pennsylvanians, the effect of the ban goes well beyond Pennsylvania. In September 2002, WorldCom announced that it would block access to the designated IP addresses for all of its North American subscribers in order to comply with the Pennsylvanian law. [33]

Filtering at the End User

At the end-user level, filtering software is available commercially. These software applications are marketed in a number of countries both to parents worried their children will access undesirable material online and companies and other organisations concerned that their employees will abuse their work-supplied Internet connections by accessing pornography.

The use of these filters is often mandated by law. U.S. law ties funding to the use of blocking software in libraries and schools. Australian law, Chinese and Argentinean policies require various forms of filters to be deployed. In some countries, such as Denmark, South Korea, and Afghanistan, schools, libraries, and cybercafés are required to use filtering software to protect the children who use their systems. All these forms of censorship affect disadvantaged people disproportionately, as they are compelled to use these facilities for all their Internet access.

Blocking software typically relies on an internal database of undesirable sites, sometimes supplemented by specific words and/or phrases whose appearance on a site will cause it to be blocked. The commercial organisations that make this software are generally very secretive about the exact contents of these databases. Government regulators have acted similarly. When asked under freedom of information laws to disclose

32. Benjamin Edelman, "Web Sites Sharing IP Addresses: Prevalence and Significance," (Berkman Center for Internet and Society, 2003).
33. Lisa Bowman and Declan McCullagh. 2002. "WorldCom blocks access to child porn." CNet News.com, September 23, 2002.

which sites were blacklisted, the Australian Broadcasting Association declined to do so. In both cases, it is suggested that the blocked content often include sites above and beyond the classifications they say they block.

One problem is that any attempt to censor the Internet by blocking material by looking for specific keywords is likely to block unrelated material, even unintentionally. AOL, for example, had to tell some British users to misspell the name of their home town when their actual home town, Scunthorpe, fell afoul of its software's built-in censor because of a string of four letters in the town's name. Similarly, attempts by filters to block sexual discussions using such keywords as "breast" will also block support groups for patients with breast cancer. In 2003 Members of Parliament in the United Kingdom found it impossible to conduct electronic discussions of the Sexual Offences Bill after Parliament introduced a new system to block pornographic junk email.

Commercial blocking software has been shown to have other, less mechanical, problems. Publishers of the software have been shown to block articles and analyses that are critical of their software. Other filters have been found to represent the interests of their proponents, blocking sites that promote safe sex, abortion, and even human rights organizations; even though these sites do not fall afoul of the legislative regimes within which they are developed.

Researchers have spent a great deal of time trying to deconstruct the block lists to draw attention to the problems with filtering. They have pointed to numerous cases of overblocking, where sites that do not contain indecent content remain blocked. They have also found a significant amount of underblocking, where software fails to filter content that it is intended to filter.[34]

As an example, consider the Google search engine. Google SafeSearch is a filter that excludes some search results that are deemed sexually explicit or undesirable. The results lists of searches are scanned by an automated process to filter pornography and explicit sexual content to shield children particularly. A study conducted at the Berkman Center for Internet & Society found a number of misclassified results, however.[35]

34. Benjamin Edelman, *Sites Blocked by Internet Filtering Programs: Edelman Expert Report for Multnomah County Public Library Et Al., Vs. United States of America, Et Al.* (2003 [cited February 24 2004]); available from http://cyber.law.harvard.edu/people/edelman/mul-v-us/.
35. Benjamin Edelman, *Empirical Analysis of Google Safesearch* (Berkman Center for Internet & Society, April 14 2003 [cited February 12 2004]); available from http://cyber.law.harvard.edu/people/edelman/google-safesearch/.

> Omitted pages include US government sites (congress.gov, thomas.loc.gov, shuttle.nasa.gov), sites operated by other governments (Hong Kong Department of Justice, Canadian Northwest Territories Minister of Justice, Israeli Prime Minister's Office, Malaysian National Vocational Training Council), political sites (Vermont Republican Party, Stonewall Democrats of Austin, Texas), news reports (including New York Times articles about blogs, deflation, and US military strategy, as well as other articles published by the BBC, c|net news.com, the Washington Post, and Wired), educational institutions (a chemistry class at Middlebury College, Vietnam War materials at Berkeley, University of Baltimore Law School, Northeastern University), and religious sites (Biblical Studies Foundation, Modern Literal Bible, Kosher for Passover). Of omitted sites without obvious sexual content, a few seem to be blocked based on ambiguous words in their titles (like Hardcore Visual Basic Programming), but most lack any indication as to the rationale for exclusion.

Even sites that were targeted to and helpful for children were omitted, including the contents of the Grolier Encyclopaedia. Sites containing information on sexuality were blocked, as well as sites on drug controls. All this blocking occurs even as some explicit content continued to be listed.

Other studies surveying a number of leading filter applications have found odd results. One such study, conducted by the National Coalition Against Censorship reports that leading filter software vendors overblock on a regular basis.[36] Some of the most contentious blocked sites, blocked by one or more leading applications, include

- The home pages of the Traditional Values Coalition and a member of U.S. Congress.
- MIT's League for Programming Freedom, part of the City of Hiroshima Web site, Georgia O'Keeffe and Vincent Van Gogh sites, and the monogamy-advocating Society for the Promotion of Unconditional Relationships.
- Virtually all gay and lesbian sites and, after detecting the phrase "least 21," blocked a news item on the Amnesty International Web site (the offending sentence read, "Reports of shootings in Irian Jaya bring to at least 21 the number of people in Indonesia and East Timor killed or wounded").
- An essay on "Indecency on the Internet: Lessons from the Art World," the United Nations report "HIV/AIDS: The Global Epidemic," and the home pages of four photography galleries.
- (then) House Majority Leader Richard "Dick" Armey's official Web site upon detecting the word "dick."

36. Marjorie Heins and Christina Cho, "Internet Filters: A Public Policy Report," (Free Expression Policy Project, National Coalition Against Censorship, 2001).

- The home pages of the Wisconsin Civil Liberties Union and the National Coalition Against Censorship.
- The Declaration of Independence, Shakespeare's complete plays, Moby Dick, and Marijuana: Facts for Teens, a brochure published by the National Institute on Drug Abuse (a division of the National Institutes of Health).
- Human-rights sites as the Commissioner of the Council of the Baltic Sea States and Algeria Watch, as well as the University of Kansas's Archie R. Dykes Medical Library (upon detecting the word "dykes").
- Jewish Teens page and the Canine Molecular Genetics Project at Michigan State University.
- The National Journal of Sexual Orientation Law, Carnegie Mellon University's Banned Books page, "Let's Have an Affair" catering company, and, through its "foul word" function, searches for Bastard Out of Carolina and "The Owl and the Pussy Cat."

Filters block access to 'loophole' sites as well. Sites in this category provide services of anonymity, privacy, language translation, humorous text transformations, even web page feature testing, and more. According to one expert:

> For censorware to perform its intended task (the control of information) there must never be any escape from that control. Thus it must ban any site which has the effect of allowing a person to receive information outside of the tracking of the censorware program. So sites which provide privacy, anonymity, and even language translation, must be banned.[37]

Therefore, filters necessarily prevent users from using services that would enhance their privacy. The reason is simple: privacy enables free expression and access to information. Surveillance and the restriction of privacy enable and enhance censorship.

37. Seth Finkelstein, "Bess's Secret Loophole (Censorware Vs. Privacy & Anonymity)," (Anticensorware Investigations, 2002).

IV.

Hinging on Privacy: Surveillance as Prior Restraint

Free expression and privacy are tightly bound to one another. Similarly, censorship and surveillance are interdependent. This section presents how initiatives to enhance surveillance are affecting censorship, generating a chilling effect upon speech. Similarly, censorship initiatives are increasingly relying on surveillance mechanisms.

The famous decision from the U.S. District Court when it struck down the Communications Decency Act argued that the key problem with the law is that it presumed that identity and age verification was possible whilst on-line.

> There is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms. An e-mail address provides no authoritative information about the addressee, who may use an e-mail "alias" or an anonymous remailer. There is also no universal or reliable listing of e- mail addresses and corresponding names or telephone numbers, and any such listing would be or rapidly become incomplete. For these reasons, there is no reliable way in many instances for a sender to know if the e-mail recipient is an adult or a minor. The difficulty of e-mail age verification is compounded for mail exploders such as listservs, which automatically send information to all e-mail addresses on a sender's list. Government expert […] agreed that no current technology could give a speaker assurance that only adults were listed in a particular mail exploder's mailing list.[38]

Any law that attempts to restrict certain types of information from certain classes of people falls under the same problem. Otherwise spill-over effects will naturally arise. Adults will be unable to access content that is in their right to access. Being unable to identify a Pennsylvania internet user has the effect of preventing all North American users of an ISP from accessing websites. French court decisions will affect all users of Yahoo! auction sites.

38. *Chief Judge Sloviter. 1996. American Civil Liberties Union et al. v. Janet Reno, Attorney General of the United States: United States District Court for the Eastern District of Pennsylvania.*

There are no simple solutions to identifying individuals whilst online. Nor are such solutions likely to be ideal, even if they existed. The right for individuals to communicate anonymously is one that is valued by society, enshrined in law, as much as it may be derided.

The Right to not Identify as you Speak

There is a rich tradition of protecting anonymous speech in deliberative democracies. Thomas Paine in 1776 published Common Sense and signed it 'Written by an Englishman'. One of the most celebrated writings in the history of the United States, the Federalist Papers was written pseudonymously in 1787-8. It was claimed to be authored by 'Publius' for the purpose of persuading New Yorkers to ratify the proposed constitution.

The right to participate anonymously is protected in the United States, alongside the First Amendment protecting free speech. The First Amendment to the Constitution of the United States declares that

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof, or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

Any attempt by government to restrict speech can be declared unlawful as unconstitutional. Restrictions on speech may be unlawful on grounds of being vague and thus having a chilling effect on speech; being overbroad in that laws that prohibit protected speech and unprotected speech; establishing prior restraint on speech; regulating the contents of speech, unless there is a narrowly tailored compelling government interest and there is no less restrictive alternative; and rules compelling speech are disallowed. The prohibition on compelling speech has been used to overturn laws requiring individuals to reveal their identity.[39]

One of the earliest legal cases involving anonymous speech in the U.S. actually predated the Constitution. The Zenger trial of 1735 involved John Peter Zenger, a printer, who refused to reveal the anonymous authors of published attacks on the Crown governor of New York. In turn, the governor and his council prosecuted Zenger for seditious libel. Many contend that it was in reaction to these events that the First Amendment to the Constitution of the United States was drafted.

39. Electronic Privacy Information Center, "Free Speech" (EPIC, April 8, 2002 [cited February 2004]); available from http://www.epic.org/free_speech/.

The right to participate in political life anonymously was upheld by the Supreme Court of the United States in the 20th century. In 1938 the Supreme Court, *in Lovell v. Griffin*, voided an ordinance that comprehensively forbade any distribution of literature at any time or place in Griffin, Georgia, without a license. The decision there pointed out that pamphlets and leaflets 'have been historic weapons in the defence of liberty', and that enforcement of the Griffin ordinance 'would restore the system of license and censorship in its baldest form'. Many ordinances of this form existed around the U.S. at the time. While the purposes of these ordinances included the prevention of fraud, disorder, or littering, the Court refused to uphold the ordinances on those grounds, pointing out that there were 'other ways to accomplish these legitimate aims without abridging freedom of speech and press.'

In 1958 the Supreme Court upheld the right of members of the NAACP to refuse to disclose their membership lists to an antagonistic Alabama state government.[40]

In this same period, in *Talley v. California*, the Supreme Court upheld the right to speak anonymously. This case involved a Los Angeles city ordinance restricting the distribution of handbills. The ordinance required the naming of the person who wrote, printed, and distributed the handbill. The petitioner, Talley, was arrested and tried for violating this ordinance with handbills referring to the National Consumers Mobilization, urging readers to help the organisation carry on a boycott against certain merchants and businessmen, whose names were given, on the ground that they carried products of 'manufacturers who will not offer equal employment opportunities to "Negroes, Mexicans, and Orientals".

In the decision for *Talley v. California*,[41] the Justices stated that

> Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws anonymously. The obnoxious press licensing law of England, which was also enforced on the Colonies was due in part to the knowledge that exposure of the names of printers, writers and distributors would lessen the circulation of literature critical of the government. The old seditious libel cases in England show the lengths to which government had to go to find out who was responsible for books that were obnoxious to the rulers. John Lilburne was whipped, pilloried and fined for refusing to answer questions designed to get

40. *NAACP v. Alabama* ex rel. Patterson, 357 US 449 (1958) and upheld in *NAACP v Alabama,* 377 US 228 (1964).
41. *Talley V. California: the Supreme Court of the United States,* 362 U.S. 60, decided March 7, 1960.

> evidence to convict him or someone else for the secret distribution of books in England. Two Puritan Ministers, John Penry and John Udal, were sentenced to death on charges that they were responsible for writing, printing or publishing books. Before the Revolutionary War colonial patriots frequently had to conceal their authorship or distribution of literature that easily could have brought down on them prosecutions by English-controlled courts. Along about that time the Letters of Junius were written and the identity of their author is unknown to this day. Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes.

The Supreme Court opinion explained that the Letters of Junius consisted of a letter written on May 28, 1770, where the author asked the following question about the tea taxed imposed on the US: "What is it then, but an odious, unprofitable exertion of a speculative right, and fixing a badge of slavery upon the Americans, without service to their masters?" The opinion notes that this is "a question which he could hardly have asked but for his anonymity."

Another key case on anonymous speech was *McIntyre v. Ohio Elections Committee.* This case called into question the Ohio Code that prohibited the distribution of anonymous campaign literature. The Code required that all literature contain the name and address of the person or campaign official issuing the literature.

Margaret McIntyre (deceased at the time of the decision) in 1988 distributed leaflets to the attendees of a public meeting at a school in Ohio. While some of the handbills identified her as the author, others referred to 'Concerned Parents and Tax Payers'. A school official filed a complaint with the Ohio Elections Commission, and the Commission fined Mrs. McIntyre $100.

The Supreme Court decision in this case states that there is no suggestion that the text of her message was false, misleading, or libellous. The Court decision[42] states that:

> The interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry. Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment.

Concurring, Justice Thomas offered a different spin, however. Rather than asking whether anonymous speech has historical validity and value, "we should determine

42. *McIntyre V. Ohio Elections Commission: the Supreme Court of the United States,* No. 93-986, Decided April 19, 1995.

whether the phrase – freedom of speech, or of the press, – as originally understood, protected anonymous political leafleting. I believe that it did."

In dissent, Justice Scalia, joined by the Chief Justice argued that anonymous pamphleteering is a pernicious, fraudulent practice.

> It facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity. There are of course exceptions, and where anonymity is needed to avoid – threats, harassment, or reprisals – the First Amendment will require an exemption from the Ohio Law. But to strike down the Ohio law in its general application and similar laws of 48 other states of the Federal Government on the ground that all anonymous communication is in our society traditionally sacrosanct, seems to me a distortion of the past that will lead to a coarsening of the future.

The arguments raised for and against are repeated in case after case involving anonymity and its value to a free and open society.

The most recent related court decision emerged from *Watchtower Bible v. Stratton* in June 2002. Here the court concluded:[43]

> Anonymity is a shield from the tyranny of the majority [...] It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation – and their ideas from suppression – at the hand of an intolerant society.

The court found that it was unconstitutional to require an individual to gain a permit containing one's name in order to engage in door-to-door advocacy of a political cause.

Relating to the Internet, governments have frequently tried to require the identification of individuals prior to granting them the right to speak. In 1996 the Georgia State legislature passed a law that forbade anonymous and pseudonymous online speech. The American Civil Liberties Union (ACLU) warned that the law was unconstitutional because it imposed content-based restrictions upon expression over computer networks.[44] The courts agreed that the law was overly broad, vague, and restricted content, thus violating the Constitution.

43. *Watchtower Bible & Tract Society of New York, Inc. et al. v. Village of Stratton et al.: the Supreme Court of the United States, No. 00-1737,* Decided June 17, 2002.
44. ACLU, "Fahrenheit 451.2: Is Cyberspace Burning? How Rating and Blocking Proposals May Torch Free Speech on the Internet."

> The state of Georgia lawyers] allege that the statute's purpose is fraud prevention, which the Court agrees is a compelling state interest. However, the statute is not narrowly tailored to achieve that end and instead sweeps innocent, protected speech within its scope. Specifically, by its plain language the criminal prohibition applies regardless of whether a speaker has any intent to deceive or whether deception actually occurs. Therefore, it could apply to a wide range of transmissions which "falsely identify" the sender, but are not "fraudulent" within the specific meaning of the criminal code.[45]

This was an influential decision as at that time a number of states and countries were considering establishing similar legal requirements.

Towards and Away from the Right to Access Anonymously

Mounting pressure to deal with indecent material on-line led to the Communications Decency Act, passed by the U.S. Congress in 1996. The parties arguing against the CDA argued that the rationale behind the McIntyre decision applies with even greater force to the Internet. According to David Sobel, a leading expert on the matter:

> Whether the millions of individuals visiting sites on the Internet are seeking information on teenage pregnancy, AIDS and other sexually transmitted diseases, classic works of literature or avant-garde poetry, they enjoy a Constitutional right to do so privately and anonymously. The CDA seeks to destroy that right.[46]

The Court's decision used similar ideas.

> Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR). Many members of SPR's mailing list have asked to remain anonymous due to the stigma of prisoner rape.

The Act was struck down on the grounds of identity, anonymity, and free speech.

The anonymity of users only goes so far as the Internet Service Providers, however. It is no surprise that the Moi regime in Kenya regularly demanded subscriber lists from service providers; that users of Burmese cybercafés must register and provide ID numbers and addresses; South Korea proposed rules to require that National ID num-

45. *American Civil Liberties Union of Georgia V. Miller*, 977 F. Supp. 1228 (1997).
46. Electronic Privacy Information Center, "Internet "Indecency" Legislation: An Unconstitutional Assault of Free Speech and Privacy Rights," (Washington DC: 1996).

bers are provided before being permitted to post on bulletin boards of public organisations; in Italy users are arbitrarily demanded to produce passports at cybercafés; and the mounting concern regarding a law requiring camera surveillance systems in cybercafés in a town in California.[47] Police in India are calling on the state of Maharashtra to require that, as a condition of getting a license, cybercafés must install filters; and they will be forced to ask potential surfers to fill out lengthy forms listing addresses, telephone numbers and other details, including showing photo identity cards.[48] Determining and divulging the identity of users of service providers is increasingly controversial.

The most famous case of compelled identity disclosure for the Internet is the anon.penet.fi case. This anonymous remailer service, anon.penet.fi, was operated by Johan Helsingius from Finland. After three years of operation, with over 500,000 users, the remailer processed more than 7000 messages a day when it was shut down.[49] Helsingius was faced with a search warrant served by Finnish police who were investigating an allegation by the Church of Scientology that anon.penet.fi had been used to make public private information taken from a church computer by placing it on the USENET group alt.religion.scientology.

On August 22, 1996 the District Court of Helsinki ordered Mr. Helsingius to turn over the e-mail address of the sender to the police.[50] As reasons for its judgement, the District Court of Helsinki stated for example that a witness can not refrain from revealing information in a trial and that the messages in question were sent to a public news group and public messages are not protected by law. Helsingius opposed the demand on grounds that the secrecy of postal mail, telephone and other confidential messages is protected by the Finnish Constitution and can not be broken in a preliminary investigation regarding a minor offence such as the alleged copyright offence. Due to the decision of the District Court, and after being raided five times by the police due to other complaints of copyright violations and of messages that insulted officials of foreign nations, Helsingius shut down the remailer server.[51]

47. Anita Ramasastry, "Can a City Require Surveillance Cameras in Cybercafes without Violating the First Amendment? A California Court Rules on the Issue," *Findlaw's Writ Legal Commentary,* February 19, 2004.
48. Zubair Ahmed, "Bombay Plans Cyber Cafe Controls," *BBC News Online,* January 27, 2004.
49. Daniel Akst, "Postcard from Cyberspace: The Helsinki Incident and the Right to Anonymity," *Los Angeles Times,* February 22, 1995.
50. Johan Helsingius, "Press Release: Johan Helsingius Gets Injunction in Scientology Case – Privacy Protection of Anonymous Messages Still Unclear," (Penet.fi, 1996).
51. Johan Helsingius, "Press Release: Johan Helsingius Closes His Internet Remailer," (Penet.fi, 1996).

The fear of criminality in society at the time was certainly a factor in his decision. The London Observer quoted an U.S. Federal Bureau of Investigation advisor as saying that up to 90 percent of all child pornography he'd seen on the Internet passed through Helsingius' remailer.[52] After investigation by the Finnish police, the Observer's claim was found to be groundless – a year prior to the Observer article the Police confirmed that the remailer operations were restricted so that it could not transmit pictures. The remailer was also accused of being frequently used by Russian criminals.[53] Amid these accusations the server was shut down, even as it was used by a British organisation used to prevent suicides among despondent people who did not want to give their names.[54]

Chilling Speech through Mass Surveillance

The disclosure of user identities is increasing. A number of cases have emerged worldwide where courts have ordered the disclosure of the identities of internet-posters, e-mailers, and mere users. Copyright rules that require the release of subscriber information of suspected file sharers only makes matters worse for the protection of personal privacy. To date, it is estimated that over 2400 subpoenas have been filed by the Music and Recording industry in the U.S.[55]

One of the most pressing cases is currently in the United States District Court for the Eastern District of Pennsylvania, between BMG Music and 203 anonymous and unrelated individuals. The recording industry claims that the defendants have made copyrighted music available on their computers for download by others on the Internet. The defendants are thus accused of engaging in wrongful anonymous speech on the internet. The challenge, however, is that because anonymous speech is constitutionally protected, a subpoena for the subscriber information is subject to qualified privilege. Arguably, ascertaining the identity of these individuals would have a chilling effect on anonymous speech: Internet speakers would know that they could be identified by persons who merely allege wrongdoing, without necessarily having any intention of carrying through with actual litigation.[56]

52. CNET Staff, ""Remailer" Service Shut Down," *CNET News.com,* August 31, 1996, 2:00pm PT 1996.
53. Paul A. Strassman and William Marlow, "Risk Free Access into the Global Information Infrastructure Via Anonymous Re-Mailers" (paper presented at the Symposium on Global Information Infrastructure: Information, Policy & International Infrastructure, Cambridge, MA, January 28-30 1996).
54. CNET Staff, ""Remailer" Service Shut Down."
55. Electronic Frontier Foundation, *Subpoena Database Query Tool* (EFF, December 1 2003 [cited February 2004]).
56. Public Citizen et al., "Memorandum in Response to Motion for Expedited Discovery in BMG Music, Et A., V. Does 1-203," (United States District Court for the Eastern District of Pennsylvania, 2004).

The disclosure of personal information is likely to become a more pressing problem, however. Public policies are being developed to compel service providers to disclose to law enforcement authorities the identity of individuals who are using communications services. This disclosure does not end with subscriber information; it also includes traffic data.

Access to this traffic data is problematic from the perspective of privacy protection. According to the European Commission's expert party on Privacy and Data Protection,[57] traffic data and modern communication infrastructures are increasingly sensitive.

> A feature of telecommunications networks and of the Internet in particular is their potential to generate a huge quantity of transactional data (the data generated in order to ensure the correct connections). The possibilities for interactive use of the networks (a defining characteristic of many Internet services) increases the amount of transactional data yet further. When consulting an online newspaper, the user 'interacts' by choosing the pages he wishes to read. These choices create a 'click stream' of transactional data. By contrast more traditional news and information services are consumed much more passively (television for example), with interactivity being limited to the off-line world of newspaper shops and libraries. Although transactional data may in some jurisdictions receive a degree of protection under rules protecting the confidentiality of correspondence, the massive growth in the amount of such data is nevertheless a cause of legitimate concern.

This growth of data is actually worsening due to other policy developments.

In the 1990s, two international bodies were developing agreements for international co-operation in investigating and preventing 'high-tech' or 'cybercrime'. The Group of Eight industrialized countries (G8) has been meeting regularly to discuss harmonizing methods, creating new investigative powers, and means of co-operation, formally since 1995. Similarly, the Council of Europe (CoE), the 43 member state international treaty-making body has laboured to create the Convention on Cybercrime since 1997, which it completed and opened for signature in November 2001. The output of both fora has implications for the disclosure of personal information by ISPs.

The CoE Convention on Cybercrime requires ratifying countries to compel service providers to disclose subscriber information, and preserve and disclose traffic data upon request for any crime. An additional problem is that these powers are

57. Article 29 Working Party, "Recommendation 3/97: Anonymity on the Internet," (Brussels: European Commission, 1997).

expected to be used to share investigative data between countries: when one country asks for data from another country, the second country is expected to comply by demanding the data from the ISP operating in its country. There is pressure on countries to adopt the Convention. This convention would arguably enable the copyright industry in the U.S. to reach internationally, gaining access to subscriber information and other evidence from other countries, even on occasions when it has failed to achieve this in the U.S.

Access to traffic data is an even more controversial when ISPs are compelled by law to archive various forms of traffic data for extended periods, in conflict with the very spirit of privacy laws. The G8 has continually advocated the retention of traffic data. This idea can be traced back to the U.S. in the 1990s. According to the then-Director of the Federal Bureau of Investigation,

> We would encourage the Internet provider industry to maintain subscriber and call information for a fixed period of time; they now discard it very briefly, unlike the telephone companies. Those are records which are very critical in identifying and even tracing some of the [child pornography] cases and leads. That would be a very helpful thing and we certainly hope that it could be done, even on a voluntary basis. Caller ID, retaining caller ID by the Internet service providers would be another hopefully voluntary measure that we would help us, and we are in discussions with the providers to see if we can receive that kind of assistance.[58]

The U.S. later pushed this policy at the EU and the G8. In October 2001 President George W. Bush wrote a letter to the President of the European Commission recommending changes in European policy, to "[c]onsider data protection issues in the context of law enforcement and counterterrorism imperatives," and as a result to "[r]evise draft privacy directives that call for mandatory destruction to permit the retention of critical data for a reasonable period."[59] This was building from recommendations from the U.S. Department of Justice to the European Commission that "[d]ata protection procedures in the sharing of law enforcement information must be formulated in ways that do not undercut international cooperation,"[60] and that

58. Louis Freeh, "Hearing of the Commerce, Justice, State and the Judiciary Committee – Subject: FY '99 Appropriations for Proposal to Prevent Child Exploitation on the Internet," (Washington DC: Federal Bureau of Investigation, 1998).
59. President Bush, "Letter to President of the European Commission: Proposals for US-EU Counter-Terrorism Cooperation," (Brussels: 2001).
60. United States Government, "Comments of the United States Government on the European Commission Communication on Combating Computer Crime," (Brussels: 2001).

> Any data protection regime should strike an appropriate balance between the protection of personal privacy, the legitimate needs of service providers to secure their networks and prevent fraud, and the promotion of public safety.[61]

Very similar language later appeared in the G8 documents from the May 2002 summit regarding data retention.

> Ensure data protection legislation, as implemented, takes into account public safety and other social values, in particular by allowing retention and preservation of data important for network security requirements or law enforcement investigations or prosecutions, and particularly with respect to the Internet and other emerging technologies.[62]

Using the argument that the retention of traffic data was critical for the war on terror, a number of countries adopted retention policies. In December 2001 data retention was introduced and passed under the United Kingdom's anti-terrorism law, followed by France and many others in the EU, with other countries following quickly including South Africa, and Argentina. All these countries now require ISPs (and telephone companies) to keep the traffic data generated by their customers for lengthy periods of time in case the data may be of value for an investigation of any crime. Algeria at one time proposed to record the names and addresses of ISP customers and their visits to websites, but later suspended the practice. The U.S. has not adopted a similar practice as yet.

These new policies permit the mass surveillance of individuals, and enable the sharing of this personal information across borders. Mobile phone internet data may now be transferred between French authorities and U.S. authorities investigating criminal activity. The list of IP addresses that interacted with a server in the United Kingdom are retained systematically by the service provider, and handed over to local authorities with minimal restraint, and may be shared with foreign authorities with even less due process.

The general public appear relatively unaware of these regimes for mass surveillance. When the first cases of copyright infringement occur, however, and an individual's internet usage over a period of years is disclosed in a court to show how an individual shared a song with users around the world, and the investigative data is shared with claimants in the U.S., only then will we get a full grip of this dire situation.

61. United States Government, "Prepared Statement of the United States of America, Presented at European Union Forum on Cybercrime," (Brussels: 2001).
62. G8 Justice and Interior Ministers, "G8 Statement on Data Protection Regimes," (Mont-Tremblant: G8 Summit, 2002).

Perhaps only then we will start to question whether the Internet and the Information Society truly lives up to the potential of being free. It is likely that this may lead to a chilling of free expression: we will be less likely to access material knowing that our ISP is required to maintain a record of that communication for a government-mandated period, and that this information may be shared with local authorities and even other countries. We may be less likely to publish information as it may lead to foreign authorities demanding our subscriber information and additional information held by our local ISP, and then used to bring us to court in foreign jurisdictions. We may be less likely to participate in the Information Society because of the policies developed to 'save it' through 'updating' older laws and developing new ones to combat today's wars and to suit yesterday's vested interests.

V.

Recommendations for Future Policy and Summits

There is an abundance of diversity in the world. A number of societies view speech and privacy differently, regulating each with different intents, purposes, and outcomes. There is a dearth of clear thinking of the implications of these policies. The world is not heading necessarily to a convergence on the destruction of free expression; but nor is the Internet necessarily the great liberator and source of resistance to censorship as presumed previously. The form and nature of censorship on the Internet has taken some surprising turns over the years. When combined with new surveillance policies, however, this surprise quickly turns to alarm.

The 'Information Society' as a rhetorical tool has failed. The term was used when we spoke of the hope of creating a new world with advanced communications technologies enhancing our reach, our knowledge, and our abilities to participate. This dream was never meant to be real; as older institutions and practices could never be separated out.

These institutions include governments and industry. These practices include censorship of 'indecent' and 'harmful' material, copyrighted material, accusations of libel and defamation. Using these mechanisms, and new techniques, they managed to transform the communications infrastructures that were once the source of much of our excitement.

Initially we were warned that it was impossible to regulate an infrastructure like the Internet, which was necessarily trans-national in jurisdiction. Governments did not heed this advice, and established laws censoring speech in their jurisdictions. Then warnings emerged that regulations from one jurisdiction could harm other jurisdictions with spill-over effects, harming not only the Internet but also the democratic rights of citizens. This advice was also ignored. After all, it was contended that the Internet was not unique, and that trans-national activity always occurred, and was always regulated.

Further initiatives resulted. Governments tried to regulate the Internet as a broadcast medium in order to apply prior controls over television to this new

medium, requiring faulty filters that overblock political speech and while continuing to underblock targeted speech. When it suited them, they also regulated the Internet as a telephone system in order to apply earlier rules on requiring surveillance mechanisms. They also 'updated' copyright regimes, libel and defamation rules to incorporate the new communications infrastructures.

The result is that an infrastructure that was to be the foundations for a new global society is, rather, a hastily regulated and over-controlled environment. The regulations and the controls vary, depending on the town, the state, the province, the country, the governmental system, and the industries involved. Control is exerted throughout the infrastructure at the points were power can be exerted to control the flow of data. Filters are implemented and liabilities are assigned.

Where effective controls can not be properly enforced, there remains the power of surveillance. Individuals may currently share files and express themselves, but when their habits are disclosed, divulging their transactions spanning months or years, as required by anti-terrorism policies, their reluctance to transact may grow. When they are compelled to present ID cards or are filmed while using public terminals and cybercafés, they are likely to change their conduct. What was once heralded as an infrastructure that would promote diversity is now part of a society with effective means of normalising behaviour.

World Summits on the Information Society should endeavour to rectify these problems. Rather they end up being mouthpieces for heads of state to declare their initiatives at establishing and supporting their national 'Information Societies', while they attend other more serious international meetings to establish international surveillance regimes. Serious work is required to re-establish freedom within this new world we are constructing. Serious work and energy is already going into combating terrorism and protecting copyright. We are failing to take our own rights seriously.

Much remains to be done. Policies need to be questioned; laws repealed, destroyed, and built up again. Another summit, hosted by one of the world's most repressive governments is not the ideal forum to push such an agenda forward, admittedly. Serious work can begin now, however, and perhaps we need to start in the places where the situation is dire. We can rebuild the 'Information Society' dream so that it stands for something optimistic and good, to replace the representation of cynicism it has become. We can un-border the data flows and legal responsibilities, unburden our rights, unbound ourselves from the prior restraints, and go back to dreaming out loud.

About the Author

Gus Hosein is a fellow with Privacy International, an advisor to the American Civil Liberties Union, and a fellow at the London School of Economics and Political Science. He holds a B.Math from the University of Waterloo in Applied Mathematics, and a doctorate from the LSE in Information Systems. His current research focus includes international policy dynamics, the development of anti-terrorism policies, and general developments in privacy and data protection. More information may be found at http://is.lse.ac.uk/staff/hosein

Acknowledgements

I would like to thank my colleagues at Privacy International, particularly David Banisar, Simon Davies, Wendy Grossman and my colleagues at the GreenNet Educational Trust, including Karen Banks and Heather Ford. I would also like to thank the Open Society Institute for their support for the research phase; as well as the Social Science Research Council for supporting the development of the intellectual foundations of this report. Finally I would like to thank UNESCO for valuing contributions in this field, even my own.