

Foundations of Technopolicy in a Free and Democratic Society

Norman Bowley¹

"We have grasped the mystery of the atom and rejected the Sermon on the Mount The world has achieved brilliance without wisdom, power without conscience. Ours is a world of nuclear giants and ethical infants." - Omar Bradley

Introduction	2
A Technical Primer	4
Privacy busters: invasive technologies:	5
Here's Looking at You, Kid!	6
I know where you were last summer (every minute of it)	6
Databases	7
Mr. Riker, are you sure that's the real Data?	8
The Day of the RFID's	9
Filtering your java	10
On a clear gif you can see forever	13
Bots, horses, spiders and viruses	13
Fingerprints and watermarks	13
Hacking for fun, profit and jihad	13
Alice and Bob in Juristic Park: Can Cryptosaurus Rex Keep a Secret?	15
The ancient art of secret writing	15
The technical breakthrough: asymmetric encryption	16
Key escrow– when is a secret not a secret?	18
Authentication– proving you are who you say you are	18
Other privacy technologies	19
Remailing	19
Steganography	19
Chaffing and winnowing	20
Tomorrow's encryption	21
The ultimate arbitrage	21

¹ Barrister & Solicitor, Ottawa, Canada

Some other relevant technologies	22
Trusted computing	22
Bionics	22
Human-computer interface	23
HCI and HTTP	24
Open source– can penguins save the day?	26
Larry’s layers: a three-step guide to the internet	26
The Anthropology of Cyberpolicy	26
“Fool me twice, shame on me.”	27
“What shall a man give in exchange for his soul?”	28
Good news in the chicken coop	30
Dewie the Turtle and a Culture of Security	32
The <i>fugu</i> speaks to cyberpolicy	40
Cybermythology	41
Silver bullets	41
Everything’s new	42
Nothing’s new	42
Canaries and carnivores: a sampling of cyberpolicy	43
The American experience: “Taking the First”	44
The British experience: Orwell by increments?	48
The Canadian experience: Should everybody have a George Radwanski?	53
Narco-privacy: the best secrecy money can buy	62
The internet as freedom fighter: can democracy grow from a cyber-café?	63
You can’t say that on the Net!– controlling content	68
Bless you, my file-- the Vatican speaks to the issues	69
Drawing it together– a working approach	70
Principles	70
Principle One: Wisdom	71
Principle two: Technological understanding	73
Pragmatism	74
Conclusion	77

Introduction

Technology has made us powerful and prosperous. It has also given us the ability to incinerate our planet. That we have not yet done so is an incredible stroke of good fortune. But as technology grows increasingly sophisticated it is no longer the mere survival of our species but the survival of our

essential freedoms and ideals which is in question. The speed, amplitude and irreversibility of technological change leave little room for error. Regrettably, policymakers have not proven adept.

This paper reviews the diverse technologies which, in their convergence, can give us god-like power or consign us to a loathsome hell of servitude and fear. Whether we enter a bright and bounteous future or one of dark bondage will depend largely on choices we make in the next five or ten years. Whether we shape ourselves in the image of God or the image of the Borg is ours to choose— but not for much longer.

The discussion, however, is a red-blooded one. Even if the talk of freedom and dignity is a little tiresome, matters of prosperity and stability should not be. The same convergence of technologies which amplifies our power also has enormous downside risk— a kind of multiplier effect which can as easily magnify economic or systemic disaster as it can economic or systemic strength. System and data reliability is more fragile than we care to admit, yet our economy increasingly depends on a high level of confidence in the internet and electronic systems. If we expect to maintain and expand our current prosperity, we need to ensure that our confidence is not mere whistling in the dark.²

This paper intends to discuss, from a legal and policy perspective, the need for a big-picture view of technology's impact and the need for a clear response. In particular, "big-picture view" calls for an analysis of the fashion in which a growing convergence of hundreds of specific technologies draws us all tightly into a world where our expectations of privacy, safety and dignity will be increasingly challenged and where our dependence on an uninterrupted stream of electrons become ever more acute. There is a wealth of literature dealing with specific technologies and specific legislation. In particular, there is a vast body of American literature analyzing privacy and technology from a First and Fourth Amendment perspective. Rather than add to any of that specific literature we hope to provoke some discussion at a broader level³, as befits the international scope and dizzying pace of technology.

There is precious little "big-picture" discussion of cyberpolicy. Lawyers and legal writers have been slow off the mark in grasping the implications of technology's megatrends. We have ceded proactivity to others⁴. Given lawyers' central place in the evolution of a civilized society, and given

² Canadian Bankers' Association report on Cryptography (1998) http://www.cba.ca/eng/CBA_on_the_Issues/Reports/cryptography_report.htm See also Junnarkar, Sandeep ZDNet News May 1, 2002 "Can Your Bank Stop an e-Stickup?"

³ Two thoughtful "big picture" reflections on privacy policy are: A. Michael Froomkin "The Death of Privacy?" STANFORD LAW REVIEW Vol. 52, 1461 and Robert A. Reilly, Conceptual Foundations of Privacy: Looking Backward Before Stepping Forward, 6 RICH. J.L. & TECH. 6 (Fall 1999) <http://www.richmond.edu/jolt/v6i2/article1.html>

⁴ Brockman, John (Ed.) The Next Fifty Years: Science in the First Half of the Twenty-First Century 2002 Vintage Books From the Introduction: "Science is the big news, and it is

that civilized society is riding a dragon who could have us all for dinner, lawyers and legal scholars need to get a grip on the broad trends and implications of the technology and to develop a proactive framework for policy and legal analysis. Far too much current technopolicy has been entirely ill-conceived and like fiscal policy in the early 1930's has exacerbated, not alleviated, the problems.⁵ In our examination of current cyberpolicy we shall discover that policy makers have all too often been barking up the wrong trees.

In order to make good cyberpolicy we must understand cybertechnology (at least at a '101' level) with a broad sense of the growing interactions and the implications of convergences. In particular we need to understand the very technologies which can protect us against irreversible erosion of our fundamental human rights and learn how to foster those technologies while limiting the risk of their becoming instruments of evil. The technologies which can protect the freedom and dignity of the individual can also protect the freedom and dignity of a system or a database.

But making good policy is nothing new. We needn't check our brains at the door simply because we are now talking technology. The understanding of human nature which underlies traditional legal analysis still stands. The seven deadly sins remain pretty well intact notwithstanding ENIAC and its progeny. We can create and we can destroy just as we always have, but now much more powerfully and quickly. It is precisely that speed and power which make it so urgent that we approach cyberpolicy courageously and intelligently. If the world was once going to hell in a handcart, it's now doing so in a bullet train.

Assuming that lawyers and legal thinkers agree that they should have a leading role in technopolicy, and given that we have fallen somewhat behind the curve, how can we create a working approach to policy development? This paper proposes to look at what works, and what doesn't, and to set out a functional approach based on principles and pragmatism.

A Technical Primer

Assuming that no one would suggest we can discuss cyberpolicy without an elementary grasp of the technology, we will begin with a "once over lightly" of some of the key technologies, then consider how the interplay of these technologies impacts our world and our lives. Once we have a nodding

scientists who are asking the big questions. Through their books and articles they have become the new public intellectuals, leaders of a new kind of public culture... The essays presented here are not the marginal discussions of the old-style intellectual culture; the work of this group of scientists centers on developments that affect the lives of everybody on this planet."

⁵Lawrence Lessig: "The law is contributing to the problem." Daniel S. Levine San Francisco Business Times November 30, 2001 "One on one with Lawrence Lessig" <http://sanfrancisco.bizjournals.com/sanfrancisco/stories/2001/12/03/newscolumn10.html>

acquaintance with the technology (nobody should count on this paper to bone up for an engineering exam) we will conduct a brief analysis of the drivers of cyberpolicy, followed by an examination of the treatment of privacy and technology in a variety of settings. After this flying *tour d'horizon* we shall attempt to cobble together a working approach to cyberpolicy in a modern democratic society.

First, let's survey three relevant clusters of technology: those which tend to invade privacy, those which tend to enhance privacy, and a group of miscellaneous technologies which don't fit easily into either category, but are relevant to the discussion.

One comment is in order before we launch into our engineering lessons: From the time this paper was completed in draft in August 2002 until it was revised in October/November 2002, nearly every technology discussed has seen significant advances or adjustments and many of the shadowy trends have taken clearer shape. This velocity of change, more than any other factor, points up the urgency of having a sturdy foundation for cyberpolicy.

Privacy busters: invasive technologies:⁶

The only thing we like better than keeping a secret is knowing one. Any device which allows us to peep into our neighbor's life is bound to be popular, and if knowing your neighbor's secrets gives you a little power over him, so much the better! The Golden Rule doesn't seem to apply when it comes to snooping.

Invasive technology is neither inherently good nor evil. The term 'invasive' is used in a neutral, non-pejorative, sense. Invasive technology is well analogized to fire—essential to civilized life, but a monster when out of control. No one (except the burglar) has any trouble with the concept of a home security system, but few of us would want to live in our very own Truman Show. Learning the secret intentions of an evildoer is, in principle, not a bad thing, nor would anyone doubt the importance of controlling public behavior—traffic signals being a case in point. Camera surveillance can cut shoplifting and a microphone in the crib of a sleeping baby will give Mother considerable peace of mind. Keeping databases is a business essential in today's complex and competitive environment. It is not generally the 'how' of invasive technology but the 'why' and the balance of rights which calls invasive technologies into question.

Here's Looking at You, Kid!

So much has been written about direct surveillance technology that it needs little repetition here. In

⁶ Emir A Mohammed: An Examination of Surveillance Technology and Their Implications for Privacy and Related Issues - The Philosophical Legal Perspective Although 1999 and mostly dealing with surveillance and privacy issues, some interesting commentary and a Canadian perspective. <http://elj.warwick.ac.uk/jilt/99-2/mohammed.html>

addition to the traditional street cameras, we are all well aware of ubiquitous microphones and ‘sniffers’ looking for drugs, explosives or contraband at the airport. We can expect surveillance to move increasingly to the micro level,⁷ become much more intrusive,⁸ read our minds⁹ and start to behave “intelligently”.¹⁰

I know where you were last summer (every minute of it)

A good deal of invasive technology is quite familiar to all of us by virtue of day-to-day encounters or by virtue of watching spy movies. None of us are surprised to see surveillance cameras in the bank or to see a satellite photo detailed enough to pick out make and model of cars parked on a familiar city street. Although we may not work through all of the implications, we know that our cell phones are called ‘cell’ phones because the relevant technology has to break up the geography into a honeycomb of ‘cells’ and that the service provider needs to know where your phone is located at any given time. It may surprise us to know that some service providers have records of our precise whereabouts, going back for several years.¹¹

⁷Scheeres, Julie Wired News August 28, 2002 ‘Tech Keeps Tabs on School Kids’ Describes several technologies, including bracelets, CCTV (with two-way microphone) and DNA ID kits.

⁸Sandhana, Lakshmi Wired News August 26, 2002 ‘There’s No Place to Hide’ “The next word in security is a system so thorough that it will reveal even the contents of a cigarette pack hidden in your coat pocket.” Scanner uses holographic imaging to provide full-body, 360-degree coverage of a person in near real time. Relies on ultra-high frequency radio waves that take about 10 seconds to classify a person as a safe customer or a potential threat. It can identify liquids, plastics, ceramics, explosives, contraband and non-metallic weapons, even through layers of clothing. Could be used to deter shoplifting, as well as to send data to fashion houses to perfectly fit a dress to the scanned individual.

⁹Murray, Frank J. The Washington Times August 17, 2002 ‘NASA plans to read terrorist’s minds at airports’ NASA is working with a commercial firm to develop equipment to receive and analyze brain-wave and heartbeat patterns and feed them into a computer to detect passengers who might pose a threat. The data could then be correlated with the passenger’s databases of travel routines, criminal and credit backgrounds.

¹⁰ Jane Wakefield BBC News Online May 1, 2002, “Surveillance cameras to predict behaviour: Cameras of future could be watching how you behave”
<http://news.bbc.co.uk/1/hi/sci/tech/1953770.stm>

¹¹ Wired News, November 9, 2001 Irish Know Where You Have Been— Ireland’s two cell phone companies keep records for six years, tracking 70% of population within few dozen feet. <http://www.wired.com/news/privacy/0,1848,48251,00.html>

Databases¹²

One group of technologies which has not captured the public imagination, yet which is hugely invasive, involves the collection, storage and retrieval of personal data. Although nobody set out to lay bare your entire life, your birth records, school records, tax records, driving records and a host of other 'public' records are carefully maintained and available for analysis. Add to those all of your credit card purchases, health records, insurance records, library borrowings and tennis club memberships and a fairly complete profile takes shape. To that can be added your toll-road usage, liquor purchases, long-distance phone calls..... a stunningly detailed biography takes shape.¹³

“But who would bother to pull together all those diverse records?” one may ask. The answer is anyone who feels like it, and with not much effort. Relational databases on computers which are increasingly compatible and linked enable all of your life's data to be treated as a single file, available for a price, or to the appropriate authority, or to a semi-skilled hacker.¹⁴

While the greater and longer-term concern must surely be the Orwellian possibilities which collocated databases can open up, the more immediate and spectacular concern is that of identity theft. In short, detailed personal profiles are a goldmine for criminals, whether to make use of your credit card numbers, pose as you while committing a crime, blackmail you with information about some unwise purchase of services..... Credit bureaus, banks, retailers and others who fail to take adequate precaution to safeguard data effectively leave the owner of the data exposed to all manner of risk.¹⁵

Mr. Riker, are you sure that's the real Data?

Putting aside the propriety of keeping microscopically detailed records of our lives, there remain

¹² See Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases A. Michael Froomkin (Although six years old– an eternity in cyberlaw– this is still a definitive and comprehensive work.)

<http://www.law.miami.edu/~froomkin/articles/ocean.htm>

¹³ Simson Garfinkel, Database Nation: The Death of Privacy in the 21st Century O'Reilly & Associates 2000. Book review at <http://elj.warwick.ac.uk/jilt/00-1/kelman.html>

¹⁴For an exhaustive discussion of these technologies and their impact see Database Nation (supra) and A. Michael Froomkin "The Death of Privacy?" STANFORD LAW REVIEW Vol. 52, 1461

¹⁵ Delio, Michelle “Lax Security: ID Theft Made Easy” Wired News December 2, 2002 <http://www.wired.com/news/privacy/0,1848,56623,00.html>

questions of fidelity and reliability (slightly different questions). Any reasonably skilled lawyer knows how easily business records and other evidence can be attacked and how easy it often is to raise significant doubt about the records' reliability.

Electronic records, however, bring with them not only questions of reliability in their original form, but questions of fidelity— that is, whether or not the data presented is free from deliberate tampering. We recall the old Soviet practice of sending photos back to the darkroom to remove this or that non-person from the May Day collection of dignitaries. The crudities of razor blade and airbrush are a faint memory. Today's photo manipulation software allows any twelve year old to amend the class photo to suit his fondest dreams. In the hands of a dedicated retro-historian, newsreels can be made to tell a quite different story. It has been said that history is written by the victors. Perhaps the future will see history re-written by the victors— the technology is not difficult once you control the data.¹⁶

Card tricks

Everyday card readers can also be used as a form of eavesdropping— the rogue store clerk will pass your debit card twice: once through the cash register when you are looking, and once through a hidden reader when you're not. It's all over in a jiffy. A properly located camera picked up your PIN and your secret is now the clerk's secret, too!

Even when the card is used for lawful identification, there may be a greater invasion of your privacy than meets the eye. Bars may use them to swipe driver's license as proof of age, which is fine, but if the data is stored, the bar has acquired a wealth of data about the patron, which data is then available for promotional purposes or even, as a bonus, for sale.¹⁷

The Day of the RFID's

Radio frequency identification tags (RFID's) are the successors to bar codes, and much more¹⁸. Unlike bar codes, they can be read from a distance and can provide far more data. Conceivably, your entire shopping cart at the hardware store could be checked through without lifting a single item out

¹⁶Cook, Gareth Boston Globe May 15 2002 'At MIT, they can put words in our mouths' Technology which permits such realistic modification of moving images that a demo was able to show a woman singing in Japanese, a language she could not speak, at a level to fool viewers. "But scientists warn the technology will also provide a powerful new tool for fraud and propaganda— and will eventually cast doubt on everything from video surveillance to presidential addresses." "This is really groundbreaking work," said Demitri Terzopoulos..... But "we are on a collision course with ethics. If you can make people say things they didn't say, then potentially all hell breaks loose."

¹⁷ Card readers in nightclubs— footnote to be verified

¹⁸ <http://www.aimglobal.org/technologies/rfid/>

of the cart. Not only that, but the store would have far more detailed inventory updates, sales profiling data and, if combined with the data from your credit, debit or loyalty card, a more detailed profile of you as a consumer. And of course, if you tried to get out of the store with an unpaid item, the RFID would have something to say about that, as well. And imagine a world without abandoned shopping carts!

The RFID and related devices are already saving motorists and tollbooths millions of dollars and millions of hours by allowing vehicles to be radio-scanned while passing at highway speeds. No more slowing to toss coins into the hopper.

RFID's also have a future in the livestock business, providing herders with not only a great deal of information about their animals, but a far better way to track wayward beasts. The technology will do the same for your Golden Retriever— an RFID implanted subcutaneously will provided the veterinarian with all kinds of data, as well as serving as a loss-proof dog tag.

Anyone who has suffered the cold fear of having a toddler wander off or an Alzheimer's patient disappear from a care facility will instantly appreciate the possibilities of RFID's as tiny, unobtrusive location beacons.

As the range, data storage capability and interactivity capabilities of RFID's increase, their usefulness as tracking and monitoring devices will become greater and greater. The temptation for inappropriate surveillance will also become irresistible to some. Indeed, authorities are floating the idea of scanning vehicular traffic for identification, to better serve the taxpayer of course¹⁹.

Filtering your java

Filtering is an internet-specific invasive technology. An internet filter sifts through data which passes through it, looking for specified features. It could, for instance, be programmed to look for the word "chocolate" and perhaps "chocolat", "chokolade", "cioccolato", etc. so as to expand its reach. When internet traffic is then flowed through the filter, its owners will then be able to identify all the data which contains these words and take the appropriate action, whether blocking attempts to link to chocolate-centric web sites or sending the police out to arrest the chocolate purveyor.

Filtering comes in two main flavors: content restriction and eavesdropping. Content restriction filters attempt to keep the user away from undesirable content. Net Nanny and CyberCop are well-known commercial applications used by parents to keep kids from surfing sites which offer inappropriate content. One can hardly argue with the intent of such an application.

¹⁹SiliconValley.com August 8, 2002 'Calif drivers worry new monitoring system threatens privacy' Project to track electronic toll payment devices affixed to car windshields. Project leaders say they are not interested in individual drivers and have gone to trouble to encrypt serial number of each transponder as it transmits and keep data separate from identities of users. Privacy advocates see a slippery slope.

Internet eavesdropping technology is effectively the same as telephone wiretapping except that it does its work wholesale. Such devices as Carnivore (now known less threateningly as DSC1000) are typically tapped into an ISP where they ‘sniff’ every packet which passes through, looking for the target data, be it a name, an IP address, or Afrikaans profanities. Packet sniffers have to sniff all of the data to get at the target data, that is, they have to read everyone’s mail to get to the target message. In theory, this is not a problem. The sniffer itself has no data storage and has a shorter memory than a law student after a contracts exam. Arguably, sniffer technology is less intrusive than a policeman scanning the crowd for his suspect. In fact, one of sniffer technology’s drawbacks is its doubtful precision.²⁰

The real problem with sniffer technology is that it is (not surprisingly) done behind closed doors. As will be discussed later, there is a total lack of accountability. Exactly how wide the scan, who is scanned, what records are kept, how they are use, is anybody’s guess. Those old enough to remember telephone operators in small communities will recall that they always had the best gossip simply because they knew who was calling whom and got enough snippets of conversation (or better still, just listened in) to have a pretty good handle on the town’s secrets. Whether modern law-enforcement officers have the self-control to ignore everything except the authorized targets will be discussed later, although the reader who is a student of human nature may care to guess the conclusion.

Carnivore has a little cousin called pen register, a much cruder form of eavesdropping, but nevertheless useful enough in some situations. In simplest form a pen register reads your keystrokes and relays them to the eavesdropper. It’s a little like listening into one side of a conversation and is often very handy for surreptitiously obtaining passwords.²¹

Filtering (of either flavor) is pretty straightforward technology, but it has several serious technical downsides., the most serious of which can be a significant degradation of the internet and the other is a notorious unreliability.

²⁰ Schwartz, John New York Times May 29, 2002 “Bin Laden Inquiry Was Hindered by FBI E-Mail Wiretapping” Alleges that Carnivore, in tapping Bin Laden related messages, also picked up “e-mails of noncovered” persons, contaminating the data. “This contradicts everything they’ve said” about Carnivore for nearly two year, said David Sobel, general counsel for the Electronic Privacy Information Centre. “Carnivore is a powerful but clumsy tool that endangers the privacy of innocent American citizens. We have now learned that its imprecision can also jeopardize important investigations, including those involving terrorism.”

Eggen, Dan Washington Post May 29, 2002 “Carnivore Glitches Botched Bin Laden Probe– FBI Memo” More comprehensive summary of foregoing story.

²¹ An interesting discussion at Anthony E. Orr, Marking Carnivore’s Territory: Rethinking Pen Registers on the Internet, 8 Mich. Telecomm. Tech. L. Rev. 219 (2002) <http://www.mttl.org/html/voleight/orrNOTETYPE4-1.pdf> and at http://www.mttl.org/html/voleight/OrrNote4thTYPESET_HTML.htm

Keeping your teenager out of hard-core porn sites is admirable and not likely to degrade much more than your own browsing speed. (Of course, your tech-savvy teenager is probably just going to use the filtering software to get a list of the really hot stuff and go over to use his friend's house to see what the fuss is all about.) Where serious net degradation occurs is when the NetNanny concept is applied to an entire society. Saudi Arabia, for instance, attempts with considerable success to filter everything that comes into the kingdom²². Not only sex, but religion, politics and alcohol are carefully screened. While the British have the technology in place²³, to date Western societies have not gone nearly so far down the road of mandatory mass-filtering.

The reason that large-scale filtering affects the operation of the entire internet is because the essential architecture of the internet is 'end-to-end'. The net, after all, was designed to be an elegantly simple, multiple-redundancy communications system capable of surviving nuclear attack. End-to-end means that the core of the system must be as simple as possible, with all the fancy stuff on the edges. Packets have to pass with as little interruption or meddling as possible. The net must be technologically and content neutral, a simple and unfettered messenger. Any interference with the end-to-end model degrades its efficiency. Filters at the edge may be okay, but every in-stream filter begins to clog the arteries and enough such filters will pull the system down.²⁴

Consider the Australians— an economically, technologically and politically advanced lot who have an entire continent to themselves. The Aussies are in a better position to force all electronic data in and out to pass through a single pipe than just about anyone else. Concerned about internet gambling, the federal government asked the Gartner Group whether forcing all communication through a single pipe to filter out offshore gambling was practical. Gartner's answer was a categorical "No."²⁵. (Of course, the growing capabilities of wireless make the 'single pipe' concept rather poor in any event.)

Even at the edges, filters are not trouble-free technology. This is essentially because they rely on humans to tell them what to filter. After that, they're pretty stupid. For instance, software which is instructed to filter out 'sex' will probably prevent you from visiting the web site for the Duke of *Sussex* Pub, or using a search engine to research sextons, sextants or the sexual habits of fruit flies. Sexual abuse recovery groups, anti-abortionists, and animal rights groups deploring gratuitous

²² Zittrain, Jonathan and Edelman, Benjamin Harvard Law School Berkman Center for Internet & Society (Ongoing paper, 2001) 'Documentation of Internet Filtering in Saudi Arabia' Discusses fairly heavy site-blocking by Saudi officials.

²³ Authority to be verified— either BBC online or the Guardian?

²⁴ Zittrain, Jonathan news.com July 23, 2002 'Can the Internet survive filtering?' Very useful discussion of the dangers inherent in the breakdown of end-to-end neutrality, the engineering principle central to the net that says that the middle must be as simple and uncomplicated as possible, with the fancy features around the edges.

²⁵ <http://www.iaa.net.au/gartner.pdf>

violence frequently find their sites on the “bad-guy list”.²⁶ Although the sampling technology gets more sophisticated every day, the ability to assess accurately the two to three billion web pages in existence in mid-2002²⁷ is just not there, and the probability is that the web will grow faster than the sophistication of the technology. In short, filters are fallible and are likely to remain so.

The great agony in filter design is whether to under-filter or over-filter, that is, whether errors should run in favor of inclusion or exclusion. The answer to the question is usually resolved along commercial lines. Let’s consider, PornSwatter, a highly popular (and entirely fictitious) family filter program. Now the vendor has to decide whether it’s better to have the Duke of Sussex Pub angry at him for over-filtering or Mrs. Smith, eager to protect her ten year old from a glimpse of knickers. Which one better fits the demographic profile of purchaser? You have probably guessed that PornSwatter will consistently over-filter and take its chances with outraged pubs.

Exactly how weak is filtering technology? The federal district court in Philadelphia (apparently reluctantly) ruled that “commercially available filtering programs erroneously block a huge amount of speech that is protected by the First Amendment,” resulting “in a substantial amount of over- and underblocking” also finding that “filtering products’ shortcomings will not be solved through a technical solution in the foreseeable future.” The court therefore found that the CIPA requirements violated the First Amendment rights of library patrons.²⁸

On a clear gif you can see forever

Cookies used to be good, now we can’t be so sure. Web bugs and clear gifs (a picture file one pixel in size so it won’t be seen) sound cute, but they can be rather sinister. Tiny programs, these devices are sent out to your computer whenever you visit a website and with varying degrees of permanence, send back data about you and your computer. Combined with geoidentification technology, the computer on the other end of the line can know an astonishing amount of information about you, your habits, and your computer.²⁹

²⁶Schwartz, John “Internet Filters Block Health Information, Study Finds” New York Times, December 10, 2002

²⁷ As at July 2002, Google asserted it had catalogued 2,073,418,204 web pages.

²⁸ McCullagh, Declan Wired News May 31, 2002 Report on Multnomah (CIPA library case) decision. “At the heart of the decision was one key point: Buggy software.” “We find that, given the crudeness of filtering technology, any technology protection measure mandated by CIPA will necessarily block access to a substantial amount of speech whose suppression serves no legitimate government interest.” The inaccuracy of the filtering (which is unlikely to improve in the foreseeable future) means that a large part of the filtering lead to a direct infringement of the First Amendment. (see also New York Times June 1, 2002 John Schwartz)

²⁹ Olsen, Stefanie CNET News.com February 12, 2002 “Quova upgrade pins down AOL users” Discusses software which is capable of identifying user down to city level (unless they are

Bots, horses, spiders and viruses

At the high risk of significant oversimplification, one may group trojan horses, viruses, robots and spiders as a set of technologies which are designed to enter your computer (generally) via an internet connection and once there, perform an assigned task. In the case of spiders, the task may be simply to gather data and take it back home. The trojan horse will typically get into your system and open the door for a subsequent attack and the virus will typically do nasty things to your computer or your data, often enough replicating itself and have you forward it to all your friends.

Fingerprints and watermarks

Just as public key encryption yields the beneficial corollary of authentication, so steganography yields a variety of uses beyond secret communication, including ‘fingerprinting’, ‘watermarking’ and data security. Fingerprinting is the insertion of unique characteristics and watermarking is the insertion of a hidden code designed to trigger a particular response. The user of the program, music CD, movie DVD or whatever will be unaware of the watermark or fingerprint until the designed event has occurred. The application in the detection and prosecution of copyright infringement is obvious.

Hacking for fun, profit and jihad

Little needs to be said here about hacking, denial-of-service attacks and related activities as these are reasonably well-discussed in the popular press. Prospective or wannabe hackers have little trouble finding instruction and any serious policy maker would do well to visit some of the “how to hack” websites³⁰. Hacking (or more accurately, ‘hacking into’) is generally taken to mean the unauthorized access to a system whereas a denial-of-service attack is frequently accomplished by an automated flood of data requests which is geared to pull down the system by virtue of its impossible demands.

In this paper it is more important to consider the motivations of the hackers or attackers than to understand their methods.

anonymizing in some fashion, in which case it will advise of that) allowing the site to block the viewer appropriately, and to combine this data with other data for higher levels of intelligence. See also Cha, Ariana Eunjung Washington Post January 4, 2002 “Rise of Internet ‘Borders’ Prompts Fears for Web’s Future” Discussion of geolocation technology and its impact. Will allow nations some control over content, perhaps by penalizing offshore sites which do not block their nationals.

³⁰ These move constantly, as one might imagine. Use any search engine to find dozens of them.

Hackers are the ultimate geeks³¹. Most have a mountain-climber complex (they do it “because it is there”.³²) A few elite hackers hack for financial gain, either criminally or as well-paid consultants. A growing number, however, hack for political reasons and there is good reason to believe that many of these are state-sponsored.³³ Increasingly, hacking is being used as a tool in garden-variety corporate espionage.³⁴

Being hacked can be extremely serious.³⁵ As well as the primary injury of loss of critical data to malevolent or unknown persons, organizations will inevitably face the secondary injury of lawsuits by third parties— customers, suppliers, patients, clients.....— who suffer financial loss or embarrassment by virtue of the failure of the organization to adequately protect confidential

³¹ See The Jargon File – Source of Official Hacker Jargon at <http://www.tuxedo.org/~estr/jargon/html/>

³² An insight into the ways of the hacking world can be obtained by juxtaposing these two reports: Middleton, James, vnunet.com October 10, 2001 ‘Hackers launch cybeware on terrorists’ <http://www.vnunet.com’News/1125948> Middleton, James, vnunet.com October 12, 2001 Fluffi Bunni attacks YIHAT hackers (Describes the hacking by Fluffi Bunni of the hackers discussed in the first article.) <http://www.vnunet.com’News/1126084>

³³Rennie, David The Daily Telegraph August 23, 2002 ‘Hackers launch cyberwar on US targets’ Computer experts in the private sector have identified Pakistan, Iran, Russia, Egypt and China as hotbeds of information warfare, espionage and hacking. China’s military has boasted of making cyberwarfare a top priority, recruiting top young graduates... See also Kan, Ahou China Business Weekly April 24, 2001 ‘US and Chinese Hackers Plan to Launch a Cyberwar’ Describes the 2001 cyberwar between US and Chinese hackers after the 2001 spy plane incident, and ‘Hackers launch ‘phase three’ of online intifada’ http://www.moqwama.org/articles.doc_2000/online.htm

³⁴ Examples (or alleged examples) include: White, Michael The Guardian August 10, 2002 ‘No 10 “Hacked into BBC news computer”’ The Conservatives last night challenged Gavyn Davies, the Labour-appointed chairman of the BBC, to get the bottom of suspicions reported by John Simpson that Downing Street staff hacked into the corporation’s computer network in their efforts to influence news coverage. Downing Street rejected any suggestions of impropriety as “utter drivel”. See also an account of the Princeton-Yale hack at <http://fyi.cnn.com/2002/fyi/teachers.ednews/07/29/yale.princeton.ap/>

³⁵O’Harrow, Robert Jr. Washington Post, August 16, 2002 ‘Sleuths Invade Military PC’s With Ease’ Describes the frequent successful attempts of consultants, inexperienced but armed with free, widely available software, who located and entered unprotected military PC’s then roamed at will through sensitive files containing military procedures, personnel records and financial data, including radio encryption techniques, laser targeting systems, security clearance data and NASA financial routing numbers.

information.

Alice and Bob in Jurassic Park: Can Cryptosaurus Rex Keep a Secret?

Privacy technology is neither such a mystery nor anything new. Any time two or more people use a device to exclude others from their discussion, they're using privacy technology. Cockney rhyming slang is a classic example. Parents of pre-schoolers will 's--p--e--l--l' out words to keep the substance of their discussion secret from the kids. In a similar fashion, during the Second World War Allied forces employed Navajo, Cree, Ojibway and other speakers to conduct open radio communication on the fairly safe assumption that such languages were completely unintelligible to the enemy. And of course, the game of baseball would be nothing without body-language.

The ancient art of secret writing

Story has it that Histaeus of Miletus, wanting to incite Aristagorus to rebel against the Persians but not too eager to be found out as treasonous, shaved the head of a trusted slave, tattooed the message on his bald pate, waited for the hair to grow back, then sent the slave on his way. If the story is true it is one of the earliest instances of *steganography* (hiding a message in an innocuous-looking place).

Julius Caesar used a rudimentary form of letter shifting (where each letter in the message is shifted, say, three letters along in the alphabet) to send battle plans through enemy lines— an early form of *cryptography* (coded writing).

Mary Queen of Scots used cryptography to send out a plot to murder Elizabeth. Unfortunately for Mary, her messages were intercepted by Sir Francis Walsingham, head of Elizabeth's secret service, who deciphered them. As a result, Mary was executed for treason in 1587. Sir Francis thus provides us with an example of *decryption*. (As one might imagine, since the wish to know a secret is just as powerful as the wish to keep a secret, the art of encryption has developed with the art of decryption hot on its heels. Few stories are as intriguing as the twin stories of code-making and code-breaking.)

Early American history reveals that cryptography had become quite sophisticated and was used not only for military purposes but political as well³⁶. Thomas Jefferson invented a code-wheel system still used by the US Navy until very recently. But the advent of electricity, then radio, saw cryptography flourish. By the Second World War early electronic enhancement of encoding saw the invention of the storied Enigma machine with its code-wheels. (It was, in fact, the need to perform 'brute force' attacks on 150,000,000,000,000,000,000 possibilities that provided an important

³⁶ John Fraser: The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution.http://vjolt.student.virginia.edu/graphics/vol2/home_art2.html

impetus to the development of early computer technology!³⁷)

As encryption and decryption came to rely on more and more sophisticated and costly electronic gear, the technologies became increasingly the exclusive domain of richly-funded national government agencies. Particularly at the height of the Cold War, these national security organizations came to believe that it was impossible and unthinkable that anyone else could or should have access to powerful encryption. Thus, when off-the-shelf powerful encryption technology was developed during the late 1970's through early 1990's, the security establishment reacted as if atom bombs could be picked up at the corner store. They set out to convince governments that the fate of the world hung in the balance, and to a large extent succeeded. As we shall see, this tail-wagging-the-dog jealousy needlessly complicated policy development and continues to do so.

The technical breakthrough: asymmetric encryption³⁸

Until very recently all encoding and decoding was symmetrical. This means that the same rules which were used to encode had to be used in reverse to decode. No matter how complicated the coding formula, it was used in reverse to arrive at 'plaintext'. In the Julius Caesar example above, if you add three to encode, you subtract three to decode. Of course, with computers the algorithms became much more complex, but nevertheless the rule remained the same: reverse the coding to decode. This coding/decoding formula is called the 'key'.

Just as decryption was a powerful incentive for the development of computers, in turn, computers with their ability to perform complex calculations (algorithms) at astonishing speed which took symmetrical encryption to its maximum potential. Of course, the same computing power which could be harnessed to decrypt by brute force (that is, by trying this, then that, and yet another, algorithm until the machine finally stumbles onto the winning ticket) could be used to create ever longer, more sophisticated, algorithms. As computing power increased³⁹, the time required to break most codes by brute force fell until it became trivial even on a desktop machine, thus calling for ever more convoluted combinations of hardware and software. All this put encryption beyond the reach of the average computer user, but left it reasonably 'crackable' by the dedicated enemy with sufficient resources. Code was therefore of little use to general computer users but vulnerable to the dedicated decipherer. Cryptography became the exclusive province of national security agencies, a kind of surreal "Spy vs. Spy" world.

The obvious problem with symmetric encryption is that if you want the recipient to read your

³⁷ The story of Enigma has been told a thousand times, including the movie U-571 which is pretty close except that the credit goes to the wrong Navy. A nice summary is at <http://www.iwm.org.uk/online/enigma/eni-intro.htm>

³⁸ For a thorough, delightful and important discussion of cryptography in the modern era, see Levy, Steven: *Crypto: How the Code Rebels Beat the Government— Saving Privacy in the Digital Age*. 2001 Penguin Putman Inc.

³⁹ Moore's Law states that computing power doubles roughly every eighteen months.

message, he has to have the key. Any interloper who could intercept the message could just as easily intercept the key, and once that happens (as is inevitable) the jig is up for any secret message. Obviously, if a way could be found that the intended recipient could use his own, unique and secret key, unknown even to the sender, this risk of key disclosure would dissipate. But such an idea is so counter-intuitive as to seem some kind of voodoo mathematics, a kind of numerical alchemy. How is it possible to undo a calculation other than by reversing it?

As with nearly every great invention, the answer flew in the face of accepted wisdom. Mathematics did not easily give up her secret, but from the late 1970's to the mid 1990's an entirely new departure in cryptography emerged, step by painful step. Algorithms were developed and applied which enabled the sender (Alice, of course) to use one key to encrypt while the recipient (Bob) would use his secret, private key to decrypt.

The solution derives from a kind of mathematical lobster trap known as a one-way function— easy to get in, hard to get out— which has its basis in prime number theory⁴⁰. Anybody can multiply two very large primes, but it takes a very powerful computer a very long time to factor the resulting number back to its components.⁴¹ As a simple example, consider how easy it is to multiply 37 by 59, but factoring 2183 takes considerably longer. This one-way simplicity coupled to a one-way complexity lies at the basis of a powerful cryptographic tool.

The need to get around the problem of sending the key to the recipient without having the snoop surreptitiously making a copy can now be completely ignored, because it doesn't matter any more. The key that is used to encrypt is a public one, available freely to anyone who wants a copy. Since I created the key using a randomly chosen pair of large primes, the chances of your cracking the code in your lifetime are slim, and for all practical purposes I am the only person who knows those underlying primes. If you want to send me an encrypted message, use my public key and send it to me. Unfortunately for the eavesdropper, the key that encrypted won't decrypt. There is no symmetry. I alone, as the recipient of the communication and the creator of the public key, know the two large primes and I use this knowledge to decrypt the cyphertext into plaintext.⁴²

⁴⁰A prime number is one which cannot be factored down into smaller whole numbers. We all know the small primes (1,3,5,7,11,13.....) but the larger ones are much too difficult for lawyers and other mortals to comprehend.

⁴¹It was not until July, 2002 that a reliable algorithm was developed to establish if a large number was prime. This development still does not imperil asymmetric encryption. See Joseph, Manu Wired News August 26, 2002 'Primed for a math breakthrough' Review of the efforts of Prof. Manindra Agrawal of IIT to find an algorithm to show whether or not a given large number is prime., with zero errors.

⁴² A helpful primer on public-key encryption is found in the Atlantic Online at www.theatlantic.com/issues/2002/09/mann_g.htm The "free big book"— downloadable as a 269 page manual is the RSA Laboratories FAQ, available at <http://www.rsasecurity.com/rsalabs/faq/>. An exhaustive treatise is Bruce Schneier "Applied Cryptography, Second Edition" John Wiley & Sons, 1996.

Key escrow– when is a secret not a secret?

Although not truly a technical issue, key escrow⁴³ should be mentioned here for the sake of rounding out the discussion. As can be imagined, large security agencies who had effectively owned strong encryption technology for decades, were not much excited by the thought that anybody could freely use powerful encryption technology. To get a rope around the problem, the agencies said to their respective governments something like the following: “Look, this thing is a Pandora’s Box. We know that strong encryption is being used for all sorts of evil, and it will only grow worse if you don’t control it. Since the horse is out of the barn, what we need is to require everyone to lodge their private keys with somebody trustworthy, like us or someone we can control—a ‘trusted third party’⁴⁴” In effect, you can keep your secrets as long as the authorities think you should. Leave your house keys at the police station, if they need to search your house, there’s no need for a messy B&E, or in another variation, if a public authority thinks he’d like to check out your house, you’re obliged to let him in. Sometimes warrants would be required, sometimes they could be obtained on a “back-fill” basis, and sometimes the stated good faith of the searcher is all that is required. As one might imagine, not everyone met these proposals with enthusiasm and the issue has become something of a litmus test in the safety vs. liberty debate.⁴⁵

Authentication– proving you are who you say you are

The magic of public key encryption produces a delightful, and now essential, corollary: authentication. If you send me a message encrypted with your private key, rather than your public key, and I apply your public key, one-way function guarantees that I will get a result that you, and only you, could have intended. I can be completely certain, therefore, that it was you and not an imposter. Thus, I can trust the message as being authentically and uniquely yours.⁴⁶ It is this

⁴³ H. Abelson, R. Anderson, S. Bellovin, J. Benaloh, M. Blaze, W. Diffie, J. Gilmore, P. Neumann, R. Rivest, J. Schiller, B. Schneier The Risks of Key Recovery, Key Escrow, and Trusted Third-Party Encryption A little dated, but a good discussion of key escrow etc. <http://www.counterpane.com/key-escrow.html>

⁴⁴ Akdeniz et als: Cryptography and Liberty: 'Can the Trusted Third Parties be Trusted ? A Critique of the Recent UK Proposals' http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/default.htm

⁴⁵ Whitfield Diffie: Key Escrow: Its Impact and Alternatives: 1994 testimony to Congress, but good discussion of key escrow, clipper chip and related issues.

⁴⁶ John D. Gregory: The Authentication of Digital Legal Records (undated paper) <http://www.it-can.ca/LegalDev/DigitalLegalRecords.html>

authentication which provides the essential security for today's e-commerce.⁴⁷

One may note, without elaborating at this juncture, the obvious conflict between authentication and key escrow.

Other privacy technologies

Encryption, which relies for its success on computational gymnastics, is not the end of the privacy story. There are at least three other basic methodologies and an infinite number of combinations.

Remailing

The simplest privacy technology is anonymous remailing. In its basic form remailing does not encrypt, but may provide me with anonymity. Thus, if I want to send you a message criticizing my boss, the boss may intercept the message but not be able to finger me for the unkind words. To protect me, I rely on one or more remailers who will forward the message after stripping it of its identifiers. If the remailing chain consisted of ten remailers between me and you, the boss could only pin the criticism on me by going to each remailer (in reverse order), force each to tell him the identifier of the immediately preceding sender which he or she stripped off, thus working back through the chain to me. I only need to count on one who will not give up the secret, and given that the remailers are all over the globe, my chances are pretty good. Toss in some encryption, and I can feel pretty confident that my boss will never get me. Although remailing is essentially a volunteer effort, some commercial houses are beginning to offer their services⁴⁸.

Steganography

Another technology, as old as Histaeus, is proving itself to be as powerful and useful as cryptography. Steganographic technology hides information within another media in such a way that it is not apparent. If you like, it is a form of communicative camouflage.

During World War Two the Germans developed the microdot— a technical drawing reduced and reduced in size until it appeared as a simple dot. The dot was then inserted into an innocuous typewritten letter addressed to a person of no particular note and sent on its way. The letter would be recovered by the true recipient, and the dot would be re-enlarged until the drawing reached its original size.

⁴⁷A very helpful overview of the technology and the law may be had at: W. Everett Lupton, Comment, The Digital Signature: Your Identity by the Numbers, 6 RICH. J.L. & TECH. 10 (Fall 1999) <http://www.richmond.edu/jolt/v6i2/note2.html>

⁴⁸Can Zero-Knowledge Hush Up the Net? Article re Zero-Knowledge products to provide pseudonymity.

Steganography is the communications equivalent of dissolving sugar into coffee— the sugar is there, but you can't see it. It is so useful as a privacy device because it will work with nearly any medium, and one medium can be “dissolved” into another, undetectable unless you know or stumble upon the method used. For instance, a techno-music fan was recently playing his favorite song through a particular type of spectroscope. To his astonishment, a human face appeared on the spectroscopic screen. After considerable fine-tuning, it was discovered that the face belonged to the artist who had deliberately encoded his visage, steganographically, into the music.⁴⁹

Good software, most of it free or low-cost, currently exists to enable me to insert data into graphic, sound, data or any other type of file with only mild degradation of either file. I can put a music file in a picture, a text message in a spreadsheet, or whatever I wish. Only someone who knows what to look for, and how, will derive any benefit. Although the technology is still very young it has enormous promise.

Steganography has important promise in providing a high level of data security. This is achieved by making data disappear. Thus, although I may successfully hack into your system, unless I have the magic lamp, I will never see the data files on your hard drive, in fact, I may not even see the hard drive. It may be hidden in other data, sound, pictures, or apparently just made to disappear by hiding in the structure of the media.

A recent open source wrinkle holds significant promise for advancing freedom of expression in repressive regimes by enabling the user to mount an innocuous website and hide therein powerful content.⁵⁰ Camera/Shy would allow you to build a web site dedicated to Bernie the Bunny, full of delights for the children but steganographically hiding messages extolling Methodism as a pathway to Krishna Consciousness.

Chaffing and winnowing

A well-known and well-used device is the dispensing by a military aircraft of millions of tiny pieces of aluminum ‘chaff’ to fool radar or anti-aircraft missiles. ‘Chaffing and winnowing’, developed by one of the pioneers of public key encryption, follows this concept. By loading a message with extraneous, erroneous and intentionally confusing data, it becomes the babbling of a madman. However, the recipient will know how to ‘winnow’ the chaff to leave the intended message.⁵¹

⁴⁹ Kahney, Leander Wired News May 10, 2002 ‘Hey, Who’s That Face in my Song?’
<http://www.wired.com/news/culture/0,1284,52426,00.html>

⁵⁰ Reuters July 14, 2002 ‘Hacker group targets Net censorship’

⁵¹ Rivest, Ronald: Chaffing and Winnowing: Confidentiality without Encryption—description of a non-encrypted technique for confidential messaging. Example of alternative to “traditional” methods, points out the obvious that it avoids the attempts of law enforcement agencies to obtain keys, etc.

Although chaffing and winnowing has not yet caught on as a significant privacy technology, it is mentioned by way of illustration of the inventiveness which keeps privacy technology ahead of those who wish to reign it in.

It takes little imagination to appreciate that the various technologies will be used in combination. A text message which is chaffed, encrypted and steganographically inserted into a music file is going to present something of a challenge to the most determined snoop!⁵²

Tomorrow's encryption

The reader should note, finally, that while algorithmic-based encryption is and will probably remain sturdy for the foreseeable future, the advent of more powerful machines and aggregated computing will eventually compromise this approach to encryption. Breaking technology based on non-algorithmic technologies, including photonic streams, will almost certainly become commonplace well before algorithmic encryption has to hang up its skates.

The ultimate arbitrage⁵³

Not all jurisdictions have the same views about what communication is good and what communication is bad. As a result, various jurisdictions become havens for particular sectors of the online world. Online gambling, for instance, may even be encouraged in an impoverished nation where the evil is unlikely to affect its people but the cash flow will be attractive to the national treasury (or the leader's bank account, as the case may be.) The same regime, however, may take a very dim view of websites or chat rooms which are critical of the regime.

The ultimate in online arbitrage, therefore, would consist of web servers which operate outside all jurisdictions, perhaps on board a ship or oil platform. A forerunner of this device is operated as an internet hosting company, HavenCo. which operates on an abandoned military platform, dubbed Sealand, a self-proclaimed sovereign state, in the North Sea operates just off the coast of Britain on an abandoned military platform located just outside the former three-mile limit (but now well within the existing twelve-mile limit) Internet servers are linked to outside world through satellite links,

⁵² Shachtman, Noah 'A New Code for Anonymous Web Use' Wired News July 12, 2002 Describes a powerful anonymity tool akin to anonymous remailing, but much more powerful. Combining features of peer-to-peer with virtual private network and open proxy servers, the Six/Four code allows "If it's implemented properly, it could be on the scope of PGP (Pretty Good Privacy)," said Chris Wysopal, of the security firm @Stake, referring to the 1990s e-mail security standard. John Henson, chief scientist of the peer-to-peer software maker Open Cola, added, "It's at least a first crack at a working model of the next phase of the Internet -- secure communications by trusted peers over an untrusted network."

⁵³ Arbitrage is the practice of choosing where to do business based on a preference for the laws of the particular jurisdiction.

with any kind of site or communication permitted except child porn, spamming and hacking. As well as online gambling sites, HavenCo hosts a growing number of political groups banned in their own countries. Says the owner/operator, “Regulations in other countries simply increase demand.”⁵⁴

Some other relevant technologies

To round out the technical overview, we will briefly discuss trusted computing, bionics and HCI.

Trusted computing

The meaning of the expression ‘trusted computing’ is not what one might initially guess. It’s not about you trusting your computer, it’s about somebody else trusting your computer. Thus, if you go online and ask the studio to download a movie, the studio will want to know if it can *trust* your computer to play the movie one time only. Similarly, within a networked environment, and more particularly a VPN (virtual private network), I will want to know that the data I exchange with you can be trusted and that your machine isn’t “leaky”.

As currently conceived, trusted computing combines hardware and software to ensure that data is processed exactly according to the specifications of the data provider. The implications for secured information and economic transactions are very significant. However, it also contains the potential to concentrate market power in the hands of a few large players beyond anything we have yet seen.⁵⁵

Bionics

Bionics is a huge discipline and only a lawyer would try to discuss it in two or three brief paragraphs. At its simplest, the use of bionics in computing is based on the unique characteristics possessed by each human being. Not only our fingerprints, but our facial structures, hand structures, gaits, irises, retinas, voice patterns, and various other emanations set us apart from the billions of other humans on the planet. Computers can be taught to distinguish one human from another, or at least to narrow the range of probable candidates. Once identified, one can be given access, ignored, or arrested—depending on the parameters of the program.

⁵⁴ Hermida, Alfred BBC News Online July 9, 2002 ‘Web rebels profit from net controls’ <http://news.bbc.co.uk/1/hi/sci/tech/2115887.stm>

⁵⁵Lemos, Robert “Trust of Treachery? Security technologies could backfire against consumers” CNET News.com November 7, 2002 <http://news.com.com/2009-1001-964628.html>
See also Becker, David “Xbox Live not for everyone” CNET News.com November 11, 2002 <http://news.com.com/2102-1040-966419.html>

Because various bionics can be used to identify us, they are ideal as pass keys, whether into our computers, homes, secure sites, databases, or whatever. However, they also provide the basis for extremely precise surveillance, the results of which can be stored away forever.⁵⁶

Bionic technology improves with each passing day, but at this point in time it is far from foolproof. For instance, face recognition technology which has been touted as the answer to terrorism in American cities has demonstrated statistically very significant unreliability.⁵⁷

Human-computer interface

The last important piece of the technical puzzle is HCI– human-computer interface. From switches through punch-cards, keyboards, mice and touch-screens, human input to computers has become democratized but not necessarily simple. Less common, but quite reliable input can be made by voice, temperature, chemical analysis, optical scanning and dozens ingenious ways to translate the physical world into storable bytes which can be manipulated. Some progress has been made with direct neural input, allowing direct manipulation of the machine by simply ‘thinking’ the commands.⁵⁸

Communication is a two-way affair and machines need to talk back if they are to be of use to us. Computers communicate not only by video screen and printer, but in fact for years they have communicated with the real world in a hundred different ways. On board automotive computers control precise jets of fuel into the engine, custom-made pellets for a thousand broilers are dispensed at the optimum moment in a fully-automated version of chicken heaven (or chicken hell, depending on your perspective). Today, with component miniaturization, neuro-electronic communication and

⁵⁶ Baard, Erik Wired News August 8, 2002 ‘Smile, You’re on In-Store Camera’ Technology to ‘level the playing field’ for brick and mortar firms by tracking, analyzing, cross-referencing and data-basing the behavior of customers on the floor.

⁵⁷ Scheeres, Julia Wired News, May 16, 2002 Airport Face Scanner Failed In a test of face recognition tech at Palm Beach International Airport, a test group of 15 employees was compared to a database of 250 airport workers over a month, in optimal conditions. It failed 53% of the time. Similarly, Tampa police has been testing face recognition over a six month period and failed to make a match with a database of known criminals.

⁵⁸ Etienne Benson Stanford Report, November 28, 2001 “Engineer studies advances in recovery of paralyzed patients”
<http://www.stanford.edu/dept/news/report/news/november28/shenoy-1128.html>

increasingly sophisticated understanding of our minds and bodies, the day of seamless, unobtrusive interface between machines and humans is upon us.

One particularly exciting branch of HCI involves the restoration of vision to the blind.⁵⁹ The restoration, and even enhancement, of the senses and of mobility through HCI is swiftly passing from fiction to reality.

Yet another field of research which will open a universe of possibilities (both good and evil) is distance tactile duplication.⁶⁰ Whether granting the shut-in the opportunity to walk through a rose garden or go on a virtual shopping trip, we can enrich the lives of those who have lost mobility. Today we train pilots in cockpit simulators, tomorrow medical students will conduct delicate microsurgery with their hands feeling every tissue and contour as they guide their virtual scalpels.

There are, though, other applications, less benign. Let us consider one example of an active danger and one of a passive danger.

HCI and HTTP

HCI opens the door to active monitoring or control of the human mind and body.⁶¹

Imagine, for instance, a high-risk diabetic. Her blood-sugar is constantly monitored and a tiny insulin pump responds with micro-insertion directly into the bloodstream, replicating the natural activity of the pancreas. But because the patient is high-risk and something of a troubling case, her blood-sugar, temperature, heart rate and a dozen other vital statistics are transmitted to a computer at the local

⁵⁹ Kotler, Steven “Vision Quest” Wired Magazine, September 2002
www.wired.com/wired/archive/10.09/vision_pr.html

⁶⁰ See “First transatlantic handshake shows off Internet2– The net gets touch feely”, October 30, 2002 “You can not only feel the resulting force, but you can also get a sense of the quality of the object you are feeling– whether it’s soft or hard, wood-like or fleshy,” said Mel Slater, Professor of Computer Science at University College of London....
<http://www.silicon.com/bin/bladerunner?REQUNIQ=1036465244&30REQEVENT=&REQAUTH=21046>

⁶¹ See, for instance Newton, Christopher Australian IT July 2, 2002 ‘Getting to the truth about lies’ “From thermal-imaging cameras designed to read guilty eyes to brain-wave scanners that essentially watch a lie in motion, the technology of truth is leaping forward.”

hospital. Programmed to look for and announce danger signals, the computer also assembles and analyzes the data to provide her specialists with clues for better managing the disease. But best of all, her doctors can remotely command the micro-pump to provide more or less insulin, as required.⁶²

Now imagine a violent sex offender. As a condition of his latest release from custody, he has agreed to the implantation of a device not unlike that of the diabetic. The staff at the psychiatric hospital take a great deal of satisfaction that the former offender is now leading the life of a happy, productive citizen, and the police are happy not only to know exactly where he is from moment to moment but to be able to monitor heart rate and neural signals which could indicate he is going to get into trouble. And best of all, if he seems to be getting into trouble, they can remotely nudge up the dosage of medication, or if things really seem to be getting out of hand, sedate him.⁶³

Finally, imagine a political trouble-maker in a technologically advanced but repressive regime.....⁶⁴

HCI may well have its greater impact on democratic societies from far less Orwellian directions, however. Given humankind's terrible predilection to fall into addictions and given our apparently insatiable appetite for online pornography and video games, one really does not want to think much about the inevitable social dislocations which simply have to flow from the integration of tactile sensation into the online experience.

Open source– can penguins save the day?

In crudest terms, open source is software which is written and published on the basis that users can access and modify the underlying code but must in turn allow others the same access and rights to their work. Effectively, operating systems and applications are written by an international collective. While any serious discussion of open source would turn this paper into a book, the phenomenon is of growing importance and deserves some mention, if only on a “heads up” basis.

⁶²CBC News, November 5, 2002 <http://www.cbc.ca/stories/2002/11/05/pacemaker021105>

⁶³The technology is within reach. See: Scheeres, Julia “Brits Mull Chipping Sex Offenders” Wired News, November 19, 2002
<http://www.wired.com/news/business/0,1367,56464.html>

⁶⁴ See thought-provoking article “The Future of Mind Control”, The Economist, May 23, 2002

Does open source impact cyberpolicy? Clearly and significantly. Open source flits across borders and responds to no authority except that of the collective. Regulating open source should be left to King Canute. This is not to say, however, that cyberpolicy is helpless in the face of open source—simply that it must be wise and understand that while it cannot command the ebb and flow of the tides, it can regulate human behavior on the waterfront.

A very recent development, and one to be watched, is the “enhanced source” licensing agreement which takes open source licensing a step further— it actually requires any user of the code to respect privacy, free expression, due process and other rights.⁶⁵

Larry’s layers: a three-step guide to the internet

The final technical concept for policy makers is that of the “layers” most aptly described by Lawrence Lessig⁶⁶: the *physical* layer (that is, all the wires and the gadgets), the *logical* layer (that is, the protocols and routines that make everything happen as it should) and the *content* layer (what we go to the net to get). Typically, policy makers are concerned about the content layer and attempt to regulate the result. The difficulty is that if they don’t understand the physical and the logical layers, the attempt to regulate the content layer can have significant effects on the underlying strata of the internet, as we have seen.

The Anthropology of Cyberpolicy

Law is about people, not things. Good and effective law takes into account the forces and motivations which cause us to do what we do as individuals and as societies. Of all the drivers and motivators, probably the most significant revolve around control— the desire to control others or evade being controlled. Whether the effort to control is selfish or for a perceived “greater good” and whether the effort to escape is a valiant expression of free speech or the furtive dodging of the wicked, the industry of individuals, governments, special interests, merchants or criminal organizations serves as the key focal point for understanding what drives technical advances and in turn the demands made on our legal systems. In the following paragraphs we will examine a few examples of these very human drivers of cyberpolicy. As always, we will try to avoid either a pejorative or laudatory tone— the point is simply to illuminate and avoid some of the naivete which infuses much cyberpolicy discussion.

⁶⁵See “Human rights enshrined in open source software” Silicon.com December 2, 2002

⁶⁶“The Future of Ideas: The Fate of the Commons in a Connected World” Random House

“Fool me twice, shame on me.”⁶⁷

Not everyone speaking to the cyberpolicy discussion has a big-picture view— in fact, probably most do not. There are, however, several communities whose voices are disproportionately loud and whose self-interest is such that their positions need to be taken with a significant bit of salt. Not surprisingly, the most prominent such community is the law enforcement and security establishment—genuinely nice people as individuals, but collectively not above crying wolf.

Following Canada’s 1971 October Crisis, several RCMP officers distinguished themselves by burning down some barns where the FLQ had purportedly been holding clandestine meetings.⁶⁸ After stout denials, the truth came out and several officers were charged. Canadians responded as Canadians tend to do,⁶⁹ first by appointing a Royal Commission then turning the matter over to the comics. The poor Mounties, of course, were just trying to serve their country, but clearly forgot a few basic points about living in a democracy. Even the world’s most likeable police force can make a fool of itself.

Without for a moment taking away from the essential nature and pure intentions of police and security operations, any reasoned discussion of cyberpolicy can’t avoid recognizing that these agencies all too often get a little carried away and need to be held accountable. Policemen have hobby horses, too. They are, after all, as human as you and me.

The American security forces, for instance, stoutly denied the existence of any such device as Carnivore until finally it was forced out of the closet in April 2000. Americans have finally come to terms that the great J. Edgar Hoover was, to put it mildly, eccentric and kept extensive dossiers on anyone who could do him harm or good.

Very recently, in a May 17, 2002 opinion of the United States Foreign Intelligence Surveillance

⁶⁷Actually, "Fool me once, shame on you. Fool me twice, shame on me." Attributed to various Godfathers, probably apocryphal.

⁶⁸RANKIN, Murray, "Burning Barns and Keable: Can a Provincial Crime Inquiry Probe the RCMP? Supreme Court Law Review, (1980): 381-400.

⁶⁹One of the few real differences between Canadians and Americans is in the response to scandal. Americans tend to outrage, Canadians see an opportunity for low humour. It’s tough to be outraged when its -40°.

Court⁷⁰ revealed at pp. 16ff that in September 2000 the US government had come clean to confess error in some 75 FISA applications, the errors relating to misstatements and omissions of material facts, including one by the then Director of the FBI. After some investigation, in March 2001 the government confessed to a further series of quite deliberate deception of the court by FBI officers.

Now, it is not the purpose of this discussion to poke fun at, or embarrass, law enforcement or security officials, but to bring a little reality to bear when we hear statements such as that by New Zealand Law Commissioner Donald Dugdale, when discussing the proposed Terrorism Act which will require New Zealand computer users to hand over passwords and encryption keys when asked, said the thinking behind the obligation was that it was a civic duty. "The good citizen will help the police."⁷¹ Simply put, those with the responsibility to make cyber policy need to have an adult view of police and security officers as well-meaning people with agendas and axes to grind, just like the rest of us, and that amongst them are one or two liars and crooks who will take advantage of privileged information, just like the rest of the population.⁷² Policy makers cannot have stars in their eyes.

As well as those law enforcement/security community, there are other choruses of self-interest seeking a cyberpolicy tailored to their particular

“What shall a man give in exchange for his soul?”⁷³

On an individual level, technology can offer a significant degree of personal safety and assurance, but with the same technology strip away almost all privacy and dignity. Let’s use medical care as an example.

The case of the diabetic patient discussed above could soon be commonplace. Personalized databases of our medical histories, including every hospital record, nurses’ journals, doctors’ notes, prescriptions, psychiatric assessments, counseling notes, drug and alcohol treatments, sexually transmitted diseases, workplace injuries, notes of spousal assaults– the full profile, will be available

⁷⁰<http://www.fas.org/irp/agency/doj/fisa/fisc051702.html>

⁷¹Barton, Chris The New Zealand Herald March 21, 2002 "Passwords access for police proposed".

⁷² Hilzenrath, David S. Washington Post, May 23, 2002 “2 FBI Agents Charged in Internet Fraud Scheme”

⁷³ Jesus, Matthew 16:25

online.

Obviously, if one is hospitalized with sudden, serious and puzzling symptoms while vacationing in Yellowknife, one would be very grateful that the attending physicians can have instant recourse to the full picture. Even better, your personal specialist from Halifax comes online during the surgery and talks the local surgeon, somewhat less experienced in your condition, successfully through the procedure. At one point, both doctors are a little baffled by the strange condition of the gall bladder and another specialist from Sydney comes online for a few minutes. In fact, for two or three of the vital steps, she takes control of the instruments.⁷⁴

But let's turn the coin over. You are a promising young female police officer, having graduated *magna cum laude* from police academy. Your career has been stellar and promotion steady. However, Internal Affairs has decided to take a peek at your medical records. They note that when you were eighteen you had an abortion, at twenty you were counseled for depression and at twenty-three attended on your doctor complaining of being assaulted by your then fiancé. They also note that your father died at fifty-three with alcoholic complications and that your mother has twice been on long-term disability for emotional breakdowns. Suddenly your reputation as the life of the party and your willingness to work to exhaustion are no longer seen as great police material but as clear signs of eventual trouble. Your career stumbles, you are no longer the golden-haired girl. You're simply out of luck.

The same medical records can be used for or against you. What makes the difference between the two scenarios?

A considerable and important discussion surrounds the protection of privacy by giving the individual property rights in his or her privacy. Given the significant body of literature in place and that the thrust of the present discussion is in a different (but not competing) direction, we take only enough time to point the interested reader in that direction.⁷⁵

Good news in the chicken coop

⁷⁴ Virtual Medical Worlds Monthly "Surgeons perform successful near real time telesurgery from New York on patient in France"
<http://www.hoise.com/vmw/01/articles/vmw/LV-VM-10-01-20.html>

⁷⁵ See MELL, PATRICIA: SEEKING SHADE IN A LAND OF PERPETUAL SUNLIGHT: PRIVACY AS PROPERTY IN THE ELECTRONIC WILDERNESS
http://www.law.berkeley.edu/journals/btlj/articles/11_1/Mell/html/text.html

Early in the paper we spoke of civilized society riding a dragon who could have us all for dinner. Let's develop that concern a little more fully.

There is quite enough literature, professional and popular, detailing a frightening future for mankind where all of us are inventoried, monitored and controlled like so many broilers. I don't intend to add to that— here we intend to find solution, not sensation. Nevertheless, there exist today scores of technologies which, if not controlled, can and will erode our privacy, freedom of expression and our democratic traditions. Most such erosions are like the one-way functions of which we read earlier— easy to get in, hard to get out. The chicken coop may be closer than we think.

The good news for the broiler factory chickens is that they never have to worry about the fox. In the same fashion, given enough surveillance, data snooping, databasing and implanted RFID's we may not have to worry about muggers, terrorists or identity thieves (although I like the chickens' chances a little better.) There shouldn't be any serious debate that we can pile on security-enhancing technology without losing privacy, freedom of expression and democratic expression. What should be the debate is whether or not we choose to do so, and if we choose to make some of the trade-offs, on what criteria.

Three codes and a cross-wind

In Lessig's very useful analysis he explains cyberpolicy as the interplay of two codes which he calls 'East Coast Code' and 'West Coast Code', that is, between legislation and architecture.⁷⁶ The analysis is an important one, particularly for traditional policy thinkers who fail to understand why techno-legislation so often stumbles.

For the purposes of this discussion, however, let me inject a third code, a kind of political-linguistic code which infuses nearly all of the discussion over cyberpolicy. In particular, there are few topics which trigger as much charged language as that having to do with privacy and the privacy technology.

“Many of the debates swirling around "law and cyberspace" are familiar ones. Questions about whether, and how, to regulate conduct on the global network tend to revolve around

⁷⁶ *Code and Other Laws of Cyberspace* etc, But see excellent counterpoint article David Post, 2000: What Larry Doesn't Get— A response to Lessig's "Code". PDF at <http://www.independent.org/tii/WorkingPapers/Code.pdf> and further analysis at BEYOND LESSIG'S CODE FOR INTERNET PRIVACY: CYBERSPACE FILTERS, PRIVACY-CONTROL, AND FAIR INFORMATION PRACTICES A thumbnail sketch of Lessig's ideas may be had in his brief paper at Lessig (2000) The Code in Law, and the Law in Code <http://cyber.law.harvard.edu/works/lessig/pcforum.pdf>

familiar themes, and those of us who participate in these debates arrange ourselves along familiar axes, settling into our accustomed roles as though sinking into our favorite easy chair: libertarians and liberals, interventionists and free-marketeers, economic conservatives and social conservatives, and the like.”⁷⁷

With this background of shrill voices⁷⁸, the policy maker faces the additional difficulty of writing legislative code which will not be nullified by computer code but will enhance, enable or direct computer code so as to further the five non-negotiables.

Magicians amuse and astound us, but they couldn’t do much if we got closer and paid more attention. They fool us because they can make us see things as they want us to, in large part by distracting us from the way things really are.

Policy makers can’t be distracted so easily. They need to see things as they really are. Cyberpolicy makers also need to see things as they could become.

Given the fragility of each of these non-negotiables and the terrible consequences of getting it wrong, cyber-policymakers can afford few mistakes. This is exactly why policy makers simply must not allow themselves to be distracted by any single-focus interest group, no matter how shrill the clamor. The non-negotiables need to stand as a bright-line test of every claim by whichever Chicken Little is insisting the sky is falling.

Dewie the Turtle and a Culture of Security⁷⁹

How important is it to have a safe internet? Barton Gellman, writing in the June 27, 2002 Washington Post, June 27, 2002 speaks of the possibility of enemy hackers taking control of major

⁷⁷David G. Post Drake Law Review, 2001Constitutional Law Symposium "THE FREE USE OF OUR FACULTIES": THOMAS JEFFERSON, CYBERSPACE, AND THE LANGUAGE OF SOCIAL LIFE

⁷⁸ Washington Post post September 11 article re “regretting writing PGP”, and response to same http://www.philzimmermann.com/news-Response_WashPost.shtml
<http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A1234-2001-Sep20>

⁷⁹Dewie is the happy little turtle who, the FTC hopes, will teach kids to be safe online and get us all into a “culture of security”.

undertakings such as the Roosevelt Dam, with a million people living downstream. “Most of these devices are now being connected to the Internet. But because the digital controls were not designed with public access in mind, they typically lack even rudimentary security, with fewer safeguards than accompany the purchase of flowers online. Much of the technical information required to penetrate these systems is widely discussed in the public forums of the affected industries. The security flaws are well-known to potential attackers.”⁸⁰

While perhaps dramatic, Gellman’s article nevertheless expresses clearly the astounding vulnerability of automated systems which are linked to the internet. How many would that be? In most Western nations, that would be just about everything – power grids, traffic lights, chemical plants, banks, sluice gates... In March 2001, a disgruntled former employee in Australia was convicted of using a computer and radio gear to hack into a computerised sewage system. Upset about being passed over for a job, the employee remotely instructed the sewage system to release millions of litres of waste into public waterways..⁸¹ What damage could be done by a truly malevolent hacker? One would rather not think about it.

In her CNET News report of July 16, 2002⁸² Margaret Kane reviewed the audit of the US Federal Deposit Insurance Corporation which revealed significant security weaknesses, with hundreds of users having access privileges that allowed them to modify financial software and read, modify, or copy financial data. Network software contained configuration weaknesses that could allow users to bypass access controls and gain unauthorized access to FDIC networks or cause network system failures. There was overall a weak control over who had access and the lack of a business continuity plan.

System insecurity is not limited to government. Reuters reported on August 26, 2002 that a well-known but unidentified hacker-turned-consultant personally demonstrated for them how to hack the banks. In quick succession he used the internet banking facilities of three of Sweden’s major banks to break into the heart of their accounts. He stopped short of (but could have easily) accessing customer accounts and transferring funds. Then he covered his tracks and left.⁸³

In early January, 2002 the Computer Science and Telecommunications Board of the National Research Council reported that American cyber security was in fact weakening, becoming

⁸⁰ “U.S. finds clues to potential cyber-attack”
http://www.siliconvalley.com/mld/siliconvalley/business/special_packages/security/3554402.htm

⁸¹ BBC News, June 27, 2002 <http://news.bbc.co.uk/1/hi/sci/tech/2070706.stm>

⁸² CNET News.com July 16, 2002

⁸³ Reuters, August 26, 2002 <http://news.com.com/2100-1001-955442.html>

increasingly vulnerable to cyber attacks, partly because companies were not implementing security measures already available, stating that “Even without any new security technologies, much better security would be possible today if technology producers, operators of critical systems, and users took appropriate steps.”⁸⁴ How serious is the problem? A 2002 Business Software Alliance survey found that 47% of corporate network administrators believe that US businesses would be attacked within next year, with 45% believing their own company was unprepared (vs. 19% who believed they were ready.)⁸⁵ The US General Accounting Office reported in late 2002 that fifteen of twenty-four US government departments received failing grades with respect to their system security, with the Department of Transport receiving a grade of 28 out of 100, perhaps in part because the post of Chief Information Officer had been vacant for over a year and a half.⁸⁶ Even the Department of Justice came in for serious criticism.⁸⁷

Significant system breaches can occur casually by virtue of loss of theft of laptops. The Associated Press reported on August 5, 2002 that the US Department of Justice had lost over 400 laptops, over half of which contained sensitive law enforcement or national security information. Two days later, Yahoo! News headlined ‘Two Laptops Missing from Central Command HQ’ At least one was believed to contain classified material. In this latter case, Chairman of Joint Chief of Staffs General Richard Myers said, “In the end, security comes down to individual responsibility. It comes down to your trust and confidence in the people that work there. And you do all the appropriate checks and all that sort of thing to ensure that the people have the right background and motivations.”

Well, no, General Myers, it’s a little more than just counting on trustworthy individuals. This is the twenty-first century. What is needed is an end-to-end approach which derives from an informed, big-picture analysis. Jim Whitmore in his paper⁸⁸ submitted to the 21st National Information Systems Security Conference, 1998 concludes, “So, is there a prescription for security in e-business? My conclusion is that, at this time, the prescription includes individualized analysis and solution design,

⁸⁴Reuters, January 8, 2002

⁸⁵Lernos, Robert CNET News.com July 24, 2002 ‘Tech pros: Cyberbomb’s ready to go off’

⁸⁶ Reuters, November 19, 2002 “U.S. cybersecurity review– again”
<http://news.com.com/2102-1001-966444.html>

⁸⁷ Krebs, Brian “Justice Department Faulted on Oversight of INS Computer Systems”
Washington Post, November 25, 2002
<http://www.washingtonpost.com/wp-dyn/articles/A38140-2002Nov25.html>

⁸⁸<http://csrc.nist.gov/nissc/1998/proceedings/paperD13.pdf>

with a view toward end-to-end trusted processes. Secure technologies can create insecure solutions.”

Doubtless, an essential element in true overall internet and system security is the establishment of security practices at the micro level in each organization⁸⁹. However, if it ended there, such micro efforts would count for little– it may be satisfying to be sure that your IT is secure, but if your ISP, communications carrier or the power utility is out of commission, your accomplishment will be rather hollow.

Julia H. Allen and Dr. Carol A. Sledge in their paper ‘Information Survivability: Required Shifts in Perspective’ discuss the need for a change in system security to a more global approach, including a shift from purely IT driven solutions to enterprise-wide, risk management solutions.⁹⁰

In the very recently published OECD Guidelines for the Security of Information Systems and Networks– Toward a Culture of Security,⁹¹ the Organization for Economic Co-operation and Development draws our attention to its 1992 Guidelines (published under the interesting acronym GASSP)⁹² and notes

The use of information systems and networks and the entire information technology environment have changed dramatically since 1992 when the OECD first put forward the Guidelines for the Security of Information Systems. These continuing changes offer significant advantages but also require a much greater emphasis on security by governments, businesses, other organisations and individual users who develop, own, provide, manage service and use information systems and networks (“participants”).

Ever more powerful personal computers, converging technologies and the widespread use of the Internet have replaced what were modest, stand-alone systems in predominantly closed networks. Today, participants are increasingly interconnected and the connections cross

⁸⁹ See, for instance, Internet Security Alliance, Common Sense Guide for Senior Managers 1st Edition– July 2002 Top ten recommended information security practices. Sets out ten excellent practices at the organization level. www.isalliance.org

⁹⁰ Allen, Julia H. and Sledge, Dr. Carol A. 2002 The CERT Coordination Center of the Software Engineering Institute, Carnegie Mellon University “Information Survivability: Required Shifts in Perspective”

⁹¹<http://www.oecd.org/pdf/M00033000/M00033182.pdf>

⁹²<http://web.mit.edu/security/www/GASSP/gasspb1.html>

national borders. In addition, the Internet supports critical infrastructures such as energy, transportation and finance and plays a major part in how companies do business, how governments provide services to citizens and enterprises and how individual citizens communicate and exchange information. The nature and type of technologies that constitute the communications and information infrastructure also have changed significantly. The number and nature of infrastructure access devices have multiplied to include fixed, wireless and mobile devices and a growing percentage of access is through “always on” connections. Consequently, the nature, volume and sensitivity of information that is exchanged has expanded substantially.

As a result of increasing interconnectivity, information systems and networks are now exposed to a growing number and a wider variety of threats and vulnerabilities. This raises new issues for security. For these reasons, these Guidelines apply to all participants in the new information society and suggest the need for a greater awareness and understanding of security issues and the need to develop a “culture of security”.

The following table compares the 1992 Guidelines to those of 2002:

1992 Guidelines	2002 Guidelines	Changes
<p>1. Accountability Principle</p> <p>The responsibilities and accountability of owners, providers and users of information systems and other parties concerned with the security of information systems should be explicit.</p>	<p>1) Awareness: Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.</p> <p>Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.</p>	<p>Up from #2, more focussed</p>

<p>2. Awareness Principle</p> <p>In order to foster confidence in information systems, owners, providers and users of information systems and other parties should readily be able, consistent with maintaining security, to gain appropriate knowledge of and be informed about the existence and general extent of measures, practices and procedures for the security of information systems.</p>	<p>2) Responsibility: All participants are responsible for the security of information systems and networks.</p> <p>Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.</p>	<p>Was #1 in 1992.</p>
<p>3. Ethics Principle</p> <p>Information systems and the security of information systems should be provided and used in such a manner that the rights and legitimate interests of others are respected.</p>	<p>3) Response: Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.</p> <p>Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.</p>	<p>Up from #4 (in part) and #7 (in part)</p>

<p>4. Multidisciplinary Principle</p> <p>Measures, practices and procedures for the security of information systems should take account of and address all relevant considerations and viewpoints, including technical, administrative, organizational, operational, commercial, educational and legal.</p>	<p>4) Ethics: Participants should respect the legitimate interests of others. Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.</p>	<p>#3 in 1992</p>
<p>5. Proportionality Principle</p> <p>Security levels, costs, measures, practices and procedures should be appropriate and proportionate to the value of and degree of reliance on the information systems and to the severity, probability and extent of potential harm, as the requirements for security vary depending upon the particular information systems.</p>	<p>5) Democracy: The security of information systems and networks should be compatible with essential values of a democratic society. Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.</p>	<p>Similar to 1992 #9 “Equity”</p>

<p>6. Integration Principle</p> <p>Measures, practices and procedures for the security of information systems should be coordinated and integrated with each other and with other measures, practices and procedures of the organization so as to create a coherent system of security.</p>	<p>6) Risk assessment: Participants should conduct risk assessments. Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.</p>	<p>#’s 6,7&8 are essentially new and reflect the more comprehensive approach of 2002</p>
<p>7. Timeliness Principle</p> <p>Public and private parties, at both national and international levels, should act in a timely coordinated manner to prevent and to respond to breaches of security of information systems.</p>	<p>7) Security design and implementation: Participants should incorporate security as an essential element of information systems and networks. Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation’s systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.</p>	

<p>8. Reassessment Principle</p> <p>The security of information systems should be reassessed periodically, as information systems and the requirements for their security vary over time.</p>	<p>8) Security management: Participants should adopt a comprehensive approach to security management. Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.</p>	
<p>9. Equity Principle</p> <p>The security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.</p>	<p>9) Reassessment: Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures. New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.</p>	

What can we draw from the progression from the still excellent 1992 guidelines to the different-in-tone 2002 guidelines? In my analysis, the key is a shift from local, organization-centred and technology-driven approach to an approach which requires all of this but calls for a shift in thinking which is both end-to-end in the organization and co-operative among organizations and countries. It is, perhaps, the recognition that security is the responsibility of the Global Village and is, in my view, a giant step in the right direction.

Data security and integrity

Data security issues are closely related, but not identical to, systems security issues. The concerns may be summed up nicely as:

One of the primary reasons that intruders can be successful is that most of the information

they acquire from a system is in a form that they can read and comprehend. When you consider the millions of electronic messages that traverse the Internet each day, it is easy to see how a well-placed network sniffer might capture a wealth of information that users would not like to have disclosed to unintended readers. Intruders may reveal the information to others, modify it to misrepresent an individual or organization, or use it to launch an attack. One solution to this problem is, through the use of cryptography, to prevent intruders from being able to use the information that they capture .⁹³

The *fugu* speaks to cyberpolicy

The *fugu*, or puffer fish, is much prized by the Japanese. Apparently if it's prepared right you get a wonderful rush. But the preparation of *fugu* is very finicky. If you don't get it quite right, your diners die.⁹⁴

Cyberpolicy makers absolutely have to operate with the care of a *fugu* chef. The consequences of getting it wrong are immense and potentially irreversible. As Lessig quite correctly warns us⁹⁵, the internet may well usher in the most repressive society the world has ever seen. Whether this frightening prediction comes to pass or whether the net ushers in a golden era will depend entirely on the choices of policy makers over the next decade or so. There is little margin for error. Perhaps more than any other area of policy making, cyberpolicy demands that the door be closed while the horse is still in the barn.

Given both the complexity and the gravity of the issues, policy makers must avoid all distraction and focus on a small number of non-negotiables at the centre. Regulators and programmers can take care of all of the fine points, but true policy makers must be steely-eyed in staying a true course.

Cybermythology

⁹³ Security of the Internet. Published in The Froehlich/Kent Encyclopedia of Telecommunications vol. 15. Marcel Dekker, New York, 1997, pp. 231-255.

⁹⁴ Chefs who prepare *fugu*, or pufferfish, in Japan must be licensed by the Environmental Sanitation Division of the Bureau of Health. Only one in four candidates passes the written test and the final exam consists of eating your own cooking. Improperly prepared *fugu* kills over 60% of those who consume it.

⁹⁵ Lawrence Lessig "The Future of Ideas: The Fate of the Commons in a Connected World" Random House

Policy making in banking, intellectual property, admiralty and all the other traditional areas of legal policy ride on in the grand majesty of profound jurisprudence. Not so with cyberpolicy. With technology seeming to race far ahead of social policy and with stories of this or that fabulous new device tumbling over yesterday's marvels, who can keep up with what is real and what is myth? Which voice is that of the prophet and which is that of the siren? Which light is the beacon and which is the lure?

Policy makers are as susceptible to cybermyths as anyone else. If we hope to have wise cyberpolicy, we need to recognize and discount the more prevalent mythology. Let us examine some of the more common ones.

Silver bullets

Alchemists never die, most just become software engineers. Their patrons never die, they just become consumers. Raised on Popular Science, we are confident that universal health, wealth and salvation are all in advanced stages of development in a lab in California. When we read about cold fusion in a glass of water, part of us is skeptical and part of us wants to believe. Anti-gravity? Ridiculous, of course, but just maybe, gee, wouldn't it be neat if.....???

The alchemists who don't become engineers become lawmakers. Ever since (and likely well before) King Canute stood on the sea shore and ordered the tide to go out, lawmakers have waved their wands at all manner of perceived evils. More often than not, the magic statutes only compound the problem.

While both technicians and lawmakers may cling to childish notions of magic potions and silver bullets, we really need to grow up if we expect to have a mature cyberpolicy. Without belaboring the point, we suggest that Hans Christian Andersen's "The Emperor's New Clothes"⁹⁷ retains most of its wisdom.

Everything's new

In the same vein as the "silver bullet" mythology is the notion that technology has turned human

⁹⁶ BBC News July 29, 2002 <http://news.bbc.co.uk/2/hi/science/nature/2157975.stm>

⁹⁷ <http://hca.gilead.org.il/emperor.html>

nature on its ear and that history is on a brand-new course. In the 1990's most of us trusted a dollar or two to stock analysts who assured us that the dot.com boom was unlike anything in human experience and would rocket ever onwards and upwards, creating wealth from thin air. Of course we were naive, and the bears came and ate our wealth all up. The more elderly amongst us (including the writer) remember the Dawning of the Age of Aquarius. We're still waiting. How many times can Lucy pull back the football before Charlie Brown catches on?

Nothing's new

The converse of "Everything's new" is "Nothing's new" and it's not a bit more reliable as a lodestone for the policy maker.⁹⁸ Unfortunately, a good deal of cyberpolicy discussion is mired in the Palaeolithic mid-1970's.

Moore's law suggests that computing power is 65,000 times what it was in 1976. At least as important is the sea change in technological culture— in 1976 there may not have been ten people in the world with the capacity and inclination to write encryption software, outside of the big concerns and the "agencies". A couple of years ago Jon Johansen⁹⁹, a seventeen year-old Norwegian farm boy, cracked DeCSS software and nobody really thought it was too big a deal (from a technical perspective, that is). Today there are probably thousands who could write PGP from scratch. As we will see in the next part of the discussion, legislators all too frequently get caught writing law which has been technologically bypassed before it is proclaimed. Nothing could be better calculated to bring the administration of justice into disrepute.

North Americans and Europeans also need to consider another aspect of change: cyberspace will not long remain our sole province and we can no longer expect to control it all by our legislation. China and India are becoming technological powerhouses, South Africa disputes ICANN hegemony and a parade of nations from Norway¹⁰⁰ to Peru¹⁰¹ says "no thanks" to Windows. Cyber policy makers increasingly have to think globally, and in particular the US cannot expect to have much more luck

⁹⁸ "There are two kinds of fool. One says, 'This is old, and therefore good.' And one says, 'This is new, and therefore better.' " - John Brunner

⁹⁹See <http://wneclaw.wnec.edu/faculty/kalodner/courses/softwarelaw/JohansenArrest.html>

¹⁰⁰Associated Press July 16, 2002 "Norway Says No Way to Microsoft"
<http://www.wired.com/news/business/0,1367,53898,00.html>

¹⁰¹Julia Scheeres Wired News April 22, 2002 "Peru Discovers Machu Penguin"
<http://www.wired.com/news/business/0,1367,51902,00.html>

than King Canute in setting global cyber policy.¹⁰²

Canaries and carnivores: a sampling of cyberpolicy

It was (and perhaps somewhere still is) the practice of coal miners to take canaries underground. If the little yellow birds died, the miners knew they had only minutes before the deadly coal gas would kill them too. The treatment of cryptography and privacy may be regarded as the techno-canary in the cyberpolicy coal mine. Ironically, anyone who understands IT knows that crypto is now accepted as a key to security:

“But "weak encryption" is no longer a reasonable excuse for insecure systems. It's clear by now that real security comes not just from strong crypto, but from recognizing and embracing human strengths, frailties and common behaviors in building, managing and using complex systems. People are always the weakest link.”¹⁰³

Unfortunately, policy makers in our democratic societies haven't caught on. They remain mesmerized by the siren song of the security and law enforcement communities who still don't much like the idea that the citizen should keep secrets from them. In non-democratic societies, of course, one can understand the imperative to scrutinize the lives of the citizen.

The American experience: “Taking the First”¹⁰⁴

Although there is an ocean of learned and popular American literature dealing with cyberpolicy, there appear (at least to an outsider) to be three major discussion points. The first has to do with the attempts to control cryptography through export control and key escrow. The second arises out of post-September 11 initiatives in the US Constitutional setting. The third is the ‘big picture’ cyberpolicy discussion led by Lessig, Froomkin, Post and a handful of others. As essential as it is, this third discussion seems regrettably at the academic edge of policy making.

It is frightening to think of the night which would fall upon the globe if the torch of American democracy burned out. This is not to suggest that the American democratic experience is better than that of Canada, India, Germany or elsewhere. It isn't. But whether the rest of us like it or not, the

¹⁰² Cockburn, Christina A., WHERE THE UNITED STATES GOES THE WORLD WILL FOLLOW--WON'T IT? 1999 21 Houston Journal of International Law 491

¹⁰³Ray Ozzie news.com August 14, 2002“[The myth of cybersecurity](http://news.com.com/2010-1071-949678.html)”
<http://news.com.com/2010-1071-949678.html>

¹⁰⁴

United States is so powerfully influential that if American democracy sneezes, the rest of the world catches pneumonia. Americans understand that their military is a shield of freedom throughout the world. They are not as acutely aware that the state of the human condition in their Union infects all of us.

The first thing which strikes the outsider reading American cyberpolicy literature is that almost all of it is a constitutional argument. “Strikes” is really too weak a word— one is simply overwhelmed by the all-pervasiveness of the Constitution in all this discussion.

Now, the Constitution is a wonderful thing in cyberlaw discussion. It is also an impediment. Wonderful when the discussion invokes the powerful broad principles and the courageous judicial expansions, an impediment when the discussion descends to a box-checking exercise. Obviously, like all of us, the American lawyer needs to check off the boxes when arguing at first instance, but it is the broad-principle arguments which are accepted and followed in common-law courts the world over.

The US Constitution has been detailed, interpreted, explained, polished and burnished like fine art, and it diffuses into every pore of American existence. So integral is the Constitution to American legal thinking that, from the outsider’s perspective, it appears that an American cannot perform legal analysis which does not pivot around the Constitution. Visitors (Canadians, at least) are awed by the worshipful reverence paid to it and we are left with the impression that Americans can’t imagine how you can run a successful democracy without a written constitution.

All of this to say that the almost the American discussion of cyberpolicy revolves entirely and reflexively around the Constitution, in particular the First Amendment (“*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.*”) and to a lesser extent the Fourth Amendment (“*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.*”) Again, as it should be.

What is essential for American cyberpolicy, however, is that the discussion lift itself from the reactive to the proactive. If I might be so gauche as to horn into someone else’s family discussion, it would be to implore American writers to focus on the broad principles, lofty ideals and the daring, breathtaking notions that the dignity and rights of the citizen came before the dignity and rights of the government.

Interestingly, privacy as a right was not much discussed during America’s first century or so, probably because nobody gave it a lot of thought in the agrarian society of the day. It was pretty well taken for granted (and, I supposed, enforced by the right to bear arms. But as cities grew and the information age (mass distribution newspapers, telegraph and telephone) began to change the face

of society, impingement upon privacy grew as an area of legal concern. Warren and Brandeis were among the first to articulate the right to privacy.¹⁰⁵

If the Constitution provides the framework for the American analysis, the grist for the mill has been provided by the tug-o-war between the security establishment and the cryptographers. As described above, in the modern age and until the late 1970's the huge US security establishment had a corner on the cryptography market. The technology was so complex and sophisticated that it took an army of men running buildings full of mainframes to devise, write, or decipher Cold War code. There was really no law or policy on cryptograph-- there didn't need to be one.

The popularization of encryption/decryption had no appeal to the security establishment. To a large extent there was a genuine concern for national security as well as the fear that widely available encryption would hand crooks an unfair advantage. To some extent, at least, there were more petty reasons such as the loss of professional mystique and the often-expressed sentiment that if you have nothing to hide, you don't need encryption. The notion that an emerging e-commerce would require a robust encryption technology was accepted very late and very grudgingly.

As it became apparent that the cryptography genie was getting out of the bottle, the security establishment and their legislative interpreters attempted at first to keep it in by controlling the technology.¹⁰⁶ The US National Bureau of Standards proposed DES¹⁰⁷, a powerful symmetric encryption algorithm, strong enough to resist brute-force cryptanalysis by anyone unless they had access to acres of mainframes (and we all know who had those.) The effect was that encryption was available to the public, but an encryption which was readily decipherable by the security establishment. If there had to be popular cryptography, better it be this kind.

So as to keep a balanced discussion, we have to understand that the security people were not trying to acquire greater power or invade new areas of private life. Up to this point in time it was understood that the best cryptography could provide was limited privacy. If the cyphertext could be intercepted, given enough time and resources it could almost certainly be decrypted. Even at the spy vs. spy level, nobody could expect perfect secrecy. What the agencies were giving up, in a sense, was the virtual monopoly on the everyday use of cryptography. What they were keeping was their long-standing practice of cracking people's codes, as of right as they understood it. Provided that the interception of the message was otherwise lawful, the decryption was clearly not unlawful.

The response to all of this was typically American. The little guy took on the government and won.

¹⁰⁵ Warren and Brandeis, "The Right to Privacy" Harvard Law Review Vol. IV December 15, 1890 No. 5

¹⁰⁶ Foreshadowing Lessig's "code" analysis.

¹⁰⁷ Data Encryption Standard

It was Bunker's Hill all over again. Consequently, when the Diffie-Hellman, RSA and PGP algorithms were introduced, the security agencies understood clearly that the world had turned upside down.¹⁰⁸ Without regulatory intervention, strong encryption now belonged to every American, or worse still, to everyone on the planet. Undecryptable cyphertext of terrorists, money-launderers and drug traffickers could travel under the very noses of security agencies. In the vernacular, they "freaked out".

On the other hand, the developers of strong encryption had a rather different view of the world. First, they did not believe that the monsters under the bed were as scary as the security made them out to be. Second, they knew that the security services, or at least some of them, had no credibility when it came to privacy abuse and could not be trusted with unlimited access to everyone's personal information. Third, and most important, they appreciated that technology and society were in the midst of a sea change. As computer scientists they, more than the security people, understood the big-picture and could see that keeping secrets would not be a privilege, nor even a right, but an essential.

Battle lines were thus laid out— on the one side the security forces and their sponsors, desperately fighting to maintain a historic right to decrypt secret messages (and why would anyone bother to encrypt who had nothing to hide?) and on the other the programmers, cypherpunks and civil libertarians who, suspicious of the motivations and power-tripping of the security agencies, fought to save freedom from the spooks.

Not surprisingly, the security people got to the legislative and executive branches long before the cryptographers did, and generally had exclusive influence. During the first Bush and the entire Clinton administrations, the legislative agenda was very clear: keep strong cryptography out of the hands of anyone but the US security agencies (and perhaps its trusted allies) and if it did get out, then prevent its export and ensure that the agencies could, when they required, obtain the encryption key. The two key features of US encryption policy during the late 1980's and the 1990's were therefore export control and various forms of key management.

Export control is a regulatory attempt to prevent weapons or weapons-equivalent devices from falling into the hands of the enemy. A wide range of strategic material is seen as being of significant military value to an enemy. The international community recognizes the risk inherent in allowing unfriendly entities to obtain strategic material and has taken concerted effort to limit these risks.¹⁰⁹ As one might imagine, if security forces don't want powerful encryption in the hands of their own citizens they surely don't want it in the hands of the enemy. The spy agencies went flat-out to convince the government that the fate of the free world rested on the containment of strong

¹⁰⁸ "The World Turned Upside Down", played as the British surrendered at Yorktown, October 17, 1781 (or so legend has it: see <http://www.americanrevolution.org/upside.html>)

¹⁰⁹ The Wassenaar Agreement page <http://www.wassenaar.org/> with links to each country.

encryption. The government bought in to the argument and ate up the entire cyberpolicy discussion for the next ten years. In retrospect, their decision was not only absurd (to use Bill Clinton's expression, how do you nail Jello to the wall?) but it distracted the government and legal community from the larger and more important discussions that were needed. The important discussions really have not yet begun in earnest.

Where is US cyberpolicy in 2002? Frankly, in limbo. With only a few notable exceptions, there appears to be no robust public discussion at the big-picture level. At the same time, some of the Bush administration's post September 11 initiatives have now lost much of their shine and need examination on their merits. (Lest I be misunderstood, I am in entire agreement with the Bush administration's expressed intent to root out terrorism in every corner of the planet. More important, though, let's not let the terrorists enjoy watching us lose our freedoms.)

The key piece of legislation (but not the only one) which bears important scrutiny is the PATRIOT Act.¹¹⁰ To get a sense of the "nitty-gritty" of security forces' view of the application of the Act, see the Field Guide.¹¹¹

The common law, however, keeps grinding along. Free speech continues to find protection, and there is always cause for hope. The US Supreme Court continues to produce powerful, lucid decisions which brush aside all kinds of short-sighted populist excuses to abridge freedom of speech and thought.¹¹²

¹¹⁰Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 <http://www.epic.org/privacy/terrorism/hr3162.html> See also EFF Analysis Of The Provisions Of The USA PATRIOT Act http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html . (The PATRIOT Act must win the prize for the current practice of naming legislation with emotionally-charged titles which frequently have little to do with the thrust of the legislation and which are often quite misleading.)

¹¹¹ US Department of Justice, Computer Crime and Intellectual Property Section (CCIPS) Field Guide on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001 <http://cybercrime.gov/PatriotAct.htm>

¹¹² Most recently, see *Watchtower v Stratton* decide June 17, 2002 While the author does not at all share the religious tenets of the Watchtower Bible and Tract Society (the Jehovah's Witnesses), the Society deserves a huge vote of gratitude for its steadfast willingness to stand firm in the face of attempts to shut down its evangelizing. The Jehovah's Witnesses have been the driving force behind freedom of speech, religion and association all over the world. In Canada, they virtually wrote the book on free speech, beginning with *Roncarelli v. Duplessis*,

Discussion of the Homeland Security Act of 2002. Concerns that both law enforcement and big business rode the terror threat to acquire a host of new powers and privilege, including broad surveillance without subpoena or oversight, and the opportunity for companies to report just about anything, claim it to be related to homeland security and that such data is Critical Infrastructure Information, and the data cannot be disclosed.¹¹³

Further discussion of proposed Total Information Awareness System, a Pentagon research project headed by John Poindexter of Irangate fame.¹¹⁴ Proposal would allow the federal government to “troll” all available databases of medical, personal, credit, and other information.

The British experience: Orwell by increments?

The British have always been leaders in encryption/decryption. In fact, there is some evidence that asymmetric encryption was discovered by the British (and the security establishment at that) at least a decade before its discovery in America.¹¹⁵ As well, Britain’s history of courage and sacrifice in the defense of freedom and democracy can never be questioned. It seems therefore counter-intuitive that Britain has some of the most aggressive anti-privacy laws and practices of any Western democracy. How could this be, and what lessons can be learned?

While Britain’s response to America’s tragedy of September 11, 2001 was that of a close friend, there was also something of a ‘welcome to the club’ tone. The United Kingdom had already seen terrorism in the homeland for decades. Shocking atrocities had become almost daily events in Northern Ireland and the threat and reality of IRA bombs in London became part of daily life. It is not surprising, therefore, that British public opinion tilted in favor of security at the cost of some loss of personal freedom. It is noteworthy to see how much.

Another fortuitous event added to the acceptance of reduced personal privacy. In the early 1990's surveillance cameras were a new and uncertain experiment. On February 12, 1993 11 year old Jon Venables and Robert Thompson led toddler Jamie Bulger by the hand to a secluded place and murdered him, apparently just for fun. Britons were shocked, saddened and outraged. When it was learned that the perpetrators had been brought to justice because their grainy image had been

[1959] S.C.R. 121.

¹¹³ Weinstein, Lauren “Taking Liberties With Our Freedom” Wired News December 2, 2002 <http://www.wired.com/news/politics/0,1283,56600,00.html>

¹¹⁴ Puzanghera, Jim “Massive database dragnet explored” November 21, 2002 San Jose Mercury News, Page 1A, (searchable at <http://www.siliconvalley.com>)

¹¹⁵ Crypto, op cit at 313

captured on CCTV, the technology transformed immediately from intruder to friend and guardian. From then, CCTV has spread to every street corner such that the each Briton is captured by surveillance camera, on the average, five times daily.¹¹⁶ Freedom-loving, democratic Britons appear to have accepted Big Brother's watchful gaze with something between gratitude and unconcern.¹¹⁷ It may also be noteworthy that Britain's is the first government in the world (not just in the free world) to float the notion of implanting tracking devices in its own citizens.¹¹⁸

With limited exceptions, the British response to the regulation of encryption, as well, seems more cowed than one might have thought. The Regulation of Investigatory Powers Act¹¹⁹ (RIPA) has effectively eliminated the requirement of a search warrant based on affidavit evidence and has transferred oversight and approval of searches in hands of the Office of Surveillance Commissioners. (The Office is said to be understaffed and underfunded.) Not only the police and security forces, but local councils, the Post Office and a handful of other bureaucracies can now ask for a certificate from the Office of Surveillance Commissioners and electronically snoop.¹²⁰

Although most of the scheme had already fallen quietly into place, at the last moment the opposition

¹¹⁶ HELEN GIBSON TIME International April 8, 1996 Volume 147, No. 15 "VOYEUR ON THE CORNER-- Big brother Britain spies on its citizens with unblinking cameras" <http://www.time.com/time/international/1996/960408/technology.html>.

¹¹⁷ JEFFREY ROSEN New York Times October 7, 2001 "BEING WATCHED A Cautionary Tale for a New Age of Surveillance" <http://www.nytimes.com/2001/10/07/magazine/07SURVEILLANCE.html>

¹¹⁸ Scheeres, Julia "Brits Mull Chipping Sex Offenders" Wired News, November 19, 2002 <http://www.wired.com/news/business/0,1367,56464.html>

¹¹⁹ See the Act at Regulation of Investigatory Powers Act 2000, UK Statutes 2000 Chapter 23, see esp. offences at ss 53-54, penalties up to five years imprisonment and fines. <http://www.hmso.gov.uk/acts/acts2000/20000023.htm>
Homepage of the Regulation of Investigatory Powers (RIPA) Act 2000 <http://www.homeoffice.gov.uk/ripa/ripact.htm> For a much more critical view of RIPA, see the Regulation of Investigatory Powers Information Centre <http://www.fipr.org/rip/> British site dedicated to attacking the Regulation of Investigatory Powers Information Act This is a huge resource for commentary (mostly British, but some international) on wiretapping, e-surveillance, etc.

¹²⁰ Jeffrey Yeates CALEA AND THE RIPA: THE U.S. AND THE U.K. RESPONSES TO WIRETAPPING IN AN INCREASINGLY WIRELESS WORLD 2001 12 Alb. L.J. Sci. & Tech. 125

Conservatives in the House of Lords, the popular press, and civil libertarians caught a sense of the enormity of it all and began to raise a great hue and cry. At the very last moment, proclamation of the third regulation was suspended “for consultation”.¹²¹

Given the apparent casual acceptance by most of the British public of Big Brother’s watchful eye and the near acquiescence to a general right of every public official from MI5 to dog-catcher to demand one’s encryption key and read one’s e-mail, the outsider may be excused for some skepticism when the current Labour government proposed that the next national general election take place by internet.¹²²

How can it be that the Mother of Parliaments in whose fair isle ‘Britons never, never shall be slaves’ could allow such significant intrusion of privacy, or conversely, allow such crippling of a technology which provides high levels of privacy? There are, perhaps, four explanations:

1. Britons have nothing quite like the First and Fourth Amendment, or any kind of written constitution, to provide the clear and sharp test of first instance;
2. Britain’s higher courts have not yet had the opportunity to shine a bright light on the efforts of the legislature to restrain personal freedom in the same way that the American courts have.
3. Although the British have a strong tradition of democracy, there may not exist in the British Isles quite the same strain of individualism which has so colored the political culture of the New World. A more Old World respect of authority and order is part of the political and legal culture; and

¹²¹ Reuters June 18, 2002 England Halts ‘Big Brother’ Regs. Home Secretary David Blunkett confirms withdrawal of final regulations of RIPA. Some in House of Lords pledge to block the regs. Lord Strathclyde, Conservative leader in the House

The Guardian June 18, 2002 “Blunkett: we blundered over data access plan” (Essentially, Blunkett says “Look, you’ve got it all wrong, we mean no ill by this. You’re just confused, so we’re going to back off and explain it all so you get it straight. We were in a bit too much of a hurry.”

¹²² Hencke, David Guardian July 17, 2002 ‘E-votes will push out ballot box 'by 2006' Tony Blair has set 2006 for the first possible general election where the traditional ballot box will be consigned to the museum and millions of people will be voting online or by post.

4. Luck. The New World should not be too smug— it is only recently that we have had to face the reality of terrorist threats on our continents. Would we have been more decisive in choosing personal freedom over safety?

This should not be taken as suggesting that every Briton has quietly accepted these intrusions into or limitations of the privacy. There have been three vigorous centers of resistance: the academic, the technical and the political.

British academics have long been at the forefront of technopolicy and it is not surprising that they have had much to say about the technology-driven erosion of privacy, both at home and abroad.¹²³

Similarly, British technology is leading-edge, both in the formal and informal sectors. A vigorous cypherpunk community, with deep roots in the academic community, has made its response known. Faced with RIPA's draconian measures, and in particular the significant penal provisions calculated to eliminate internet privacy, a group of cypherpunks announced an "anti-snooping operating system" called M-o-o-t. This tool is calculated to avoid RIPA's power to force disclosure of encryption keys, by which storing the keys and data overseas, on any server that allows encrypted FTP access, to the extent of even sharing files between different servers. Using both a steganographic file system developed at Cambridge to make the data "disappear" and a Napster-like file swapping program, the tool made it impossible for the computer user to give up his key because it resided, hidden, in someone else's FTP server in another country.¹²⁴

Probably the best news in all of this is that the British Privacy Commissioner seems to have stepped into the fray with a pronouncement that the whole scheme may be unlawful. We will all, of course, be watching with bated breath.¹²⁵

¹²³ See, for instance Yaman Akdeniz: UK Government Policy on Encryption <http://webjcli.ncl.ac.uk/1997/issue1/akdeniz1.html>

¹²⁴ Knight, Will NewScientist.com May 29, 2002. See also Leyden, John The Register, May 29, 2002 "Cypherpunks aim to torpedo RIP key seizure plan" Plan to defeat Part 3 of RIPA with M-o-o-t. See also The information hiding homepage digital watermarking & steganography <http://www.cl.cam.ac.uk/~fapp2/steganography/> As well, see The Steganographic File System (1998) <http://citeseer.nj.nec.com/60142.html> Discussion page for Steganographic File System developed at Cambridge by Anderson, Needham and Shamir. "Unless you know the filename and password, you can't even tell the file exists."

¹²⁵ Miller, Stuart Guardian Unlimited July 31, 2002 'Snooping laws may be illegal' Opinion is that the sweeping powers granted by the anti-terror legislation in combination with the

What lessons can be taken here?

1. The citizenry of an advanced Western democracy will permit a considerable encroachment of their civil liberties where they believe their safety is at significant risk.
2. Such encroachment of civil liberties can continue to expand significantly so long as it occurs gradually.
3. At best, legislators were pushing ill-considered law well ahead of the public acceptance curve on the basis that “Something has to be done!” At worst, draconian and invasive measures, with no sunset provisions, were put into place to deal with emergency situations and then left in place.
4. Legislators are quite ready to set aside such historic protections as court-supervised search warrants in the interests of expedience.
5. Like King Canute, the legislators thought they could command the tides. Like Canute, they were disappointed— in this instance, technology provided a complete and lawful end-run and made the legislation useful only to catch the small, the slow and the stupid.
6. The office of a Privacy Commissioner, given sufficient autonomy and power, can be of great importance in keeping well-meaning but ill-considered legislative policy from infringing our liberties.
7. Big government appears not to be even-handed as between intrusive technology and privacy technology, but appears to have at least some bias in favor of the former.

The Canadian experience: Should everybody have a George Radwanski?

As a Canadian I should like to be able to say that we have got it right. Unfortunately, I can't. Canadian cyberpolicy isn't bad, but it isn't brilliant, either. With two significant exceptions, Canadian cyberpolicy is a Tweedledum to the American Tweedledee. To appreciate the differences it is important to understand the similarities.

RIPA grants far-too sweeping power. Very interesting analysis.
http://www.guardian.co.uk/uk_news/story/0,3604,766702,00.html

The US and Canada are the worlds largest trading partnership and represent each other's single largest cross-border customers. Through NAFTA they have achieved very substantial economic integration. North American telecommunications are a seamless web. Many Canadian and American security officers deal on a first-name basis and sometimes see the border as an administrative nuisance. There is less culture shock involved in a move from suburban Calgary to suburban Denver than there is in moving from rural Vermont to downtown Los Angeles. Even our politics are culturally similar– a Michigan Democrat and an Ontario Liberal could trade places in each other's caucuses, pausing only to learn some vocabulary. With such similar populations, North America presents an ideal laboratory for studying different experiences in cyber policy.

The American population is roughly ten times that of Canada. Although Canada's economy is among the ten largest in the world, it is far smaller than that of the US. It is hardly surprising, therefore, that the vast majority of policy initiative starts south of the border and is copied with little modification. It is also hardly surprising that our courts do roughly one-tenth of the business that their American counterparts do, producing one-tenth of the jurisprudence. Simply put, we don't have the same opportunity to make cyberpolicy. Canadian courts habitually refer to American decisions for guidance (not in the sense of binding precedent, but in the sense of avoiding unnecessary re-invention of the wheel.)

Although at first glance one might believe Canada's cyberpolicy to be a bland, Northern version of American policy, there are differences, two of which are quite important and highly useful in suggesting fresh approaches south of the border. One has to do with our more aggressive approach to privacy and one has to do with our very different constitutional histories.

Canada's approach to privacy legislation has twin roots in pragmatism and idealism. We have long had federal and provincial Privacy Acts¹²⁶ and Privacy Commissioners¹²⁷. However, at least at the federal level, however, the Privacy Act had to do with the citizen's rights *vis à vis* the federal government, not the private sector. This latter was a tougher nut to crack and the legislative spirit was more willing than the legislative flesh. Fortunately, pragmatism came to the rescue in the guise of international trade.

The United States is unique in its ability to tell the rest of the world to mind its own economic business. Canada simply doesn't have that kind of economic clout. When the European Union mandated that Europeans could not do business with anyone outside the Union unless the other party had equal or better personal privacy information protection, Canada knew it was time to stop talking

¹²⁶ Privacy Act, R.S.C. 1985, c. P-21

¹²⁷ *ibid* at s. 53

and get on with the legislation. The Personal Information Protection and Electronic Document Act¹²⁸ received Royal Assent April 13th , 2000.¹²⁹ Canadian provinces are now following suit with local legislation which is, if anything, stronger.¹³⁰ PIPEDA is a serious and central piece of regulatory legislation which will continue to put a distinct stamp on the way Canadians do business (and the way non-Canadians do business in Canada, as well.¹³¹)

The privacy provisions of both the Privacy Act and PIPEDA are enforced by Canada's Privacy Commissioner (currently George Radwanski).¹³² The current Commissioner is setting a very proactive tone, a sense of which can be gathered from a sampling from the "Findings under the Personal Information Protection and Electronic Documents Act" website¹³³:

- Bank refuses customer access to internal credit score
- Customer objects to Social Insurance Number on address label of telephone bill
- Bank accused of providing police with surveillance photos of the wrong person
- Bank accused of non-consensual recording and disclosure of telephone conversation
- Bank sends customers' pay stubs to wrong party

Such issues are the pith and substance of daily privacy concerns. The Office of the Privacy Commissioner, by receiving and investigating complaints from Canadians, serves to help develop a body of quasi-jurisprudence, a general code of conduct, in privacy matters. As any of these decisions are challenged, of course, a body of jurisprudence will develop.

¹²⁸ S.C. 2000 c.5

¹²⁹ PIPEDA is general pronounced 'pie-pee-da', sometimes 'the Piped Act' and by stereotypical Canadians, 'piped, eh?' If you want people to think that you've been involved in privacy law for years, however, call it Bill 6

¹³⁰In fact, in 1994 Quebec was out of the gate before the federal government with la Loi sur la protection des renseignements personnels dans le secteur privé.

¹³¹ PRIVACY, EH! The Impact of Canada's Personal Information Protection and Electronic Documents May not be topic relevant, but worth a print and a read.

¹³² See the Commissioner's very helpful "Guide for Businesses and Organizations to Canada's Personal Information Protection and Electronic Documents Act" at http://www.privcom.gc.ca/information/guide_e.asp

¹³³http://www.privcom.gc.ca/index_e.asp

However, the Commissioner's most significant contribution to privacy to date has arisen (or given its ongoing nature, is arising) as a result of a complaint he received from British Columbia's Privacy Commissioner with respect to round-the-clock camera surveillance by the RCMP in Kelowna¹³⁴. In his letter of finding¹³⁵, the Commissioner made the following observations:

It is equally clear, in my view, that police forces cannot invoke crime prevention or deterrence to justify monitoring and recording on film the activities of large numbers of the general public.

I also note that I believe my reasoning to be consistent with that of the Supreme Court of Canada in its decision in the 1990 case of *R. v. Wong*, wherein the Court stated: ".....to permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society.....we must always be alert to the fact that modern methods of electronic surveillance have the potential, if uncontrolled, to annihilate privacy."

I have often stated my belief that privacy will be the defining issue of this new decade. Quite apart from the new pressures the current situation is likely to create, this is because a host of emerging technological challenges to privacy will force us to make choices that will determine what kind of Canadian society we will have not only for ourselves, but for our children and grandchildren. And if privacy at large will be the defining issue, few privacy issues will do more to shape that definition than the choices we make about video surveillance.

In police states, there may be little or no crime, but there is also little or no freedom. Here in Canada, we temper law enforcement activities to accord with the kind of society we choose to be. We do not permit egregious violations of human rights, however effective they might be in deterring or solving crimes.

We make these choices because, while wanting a safe society, we recognize that there is more to safety and a high quality of life than merely the absence of crime. This same perspective needs, in my view, to be brought to the issue of surveillance cameras in our streets and public places. How great a price, in terms of our fundamental right to privacy, are

¹³⁴However, the Commissioner may have just been thrown a much bigger challenge: as this paper was being wrapped up, the Government of Canada announced a discussion paper containing a vision of a new regime of electronic surveillance by law enforcement forces. Given its apparent long grasp, one may confidently expect the Commissioner to have some opinions. See Declan McCullagh, August 27, 2002 "Will Canada's ISP's become spies?" <http://news.com.com/2100-1023-955595.html>

¹³⁵ http://www.privcom.gc.ca/cf-dc/02_05_b_011004_e.asp

we really prepared to pay?

My second concern is that if a proliferation of video surveillance cameras in public places is allowed to take place, it is a virtual certainty that function creep will lead inexorably to the linkage of those cameras with biometric technology that permits identifying individuals by matching their facial characteristics with photos that are on record.

Far from being some futuristic fantasy, this is already being attempted in some U.S. cities, to considerable public consternation. Once sufficient cameras were in place, there is every reason to believe that this approach would initially be advanced by some Canadian police force as well, as an effective way to protect the public from known criminals—as was done in the U.S. at the stadium during the last Super Bowl Game. From there, it would only be a short distance to using readily available photo sources for the general population, such as driver's licence application records, to be able to identify anyone in a monitored public place at any time, or to monitor the whereabouts and activities of any given individual as he or she moved from place to place.

I need hardly elaborate on the effect this would have on privacy rights, or the kind of transformation it would work on Canadian society. Such surveillance/identification would be as deeply wrong as it is unnecessary. Just because something is technologically possible, that does not mean it is socially justifiable or acceptable. But the only effective way to prevent it is to prevent the proliferation of surveillance cameras in the first place.

None of this is to say that there may not be some specific circumstances where it is appropriate for police forces to use surveillance cameras in public places to maintain safety and order.

But all these circumstances differ fundamentally from accepting widespread video surveillance of the general population. From the perspective of privacy rights, video surveillance by the state can only be justified when it is demonstrable that keeping the peace could not be accomplished by any other less privacy-invasive means. Solid evidence is required in each case to justify the use of generalized video surveillance rather than other traditional means of law enforcement. Convenience, efficiency or cost savings should never qualify as such evidence. Video surveillance of Canadians by the state should be the very rare exception, not the norm.

I have gone to considerable lengths in addressing the broader issues raised by this complaint, because of my profound belief that the choices we Canadians make about video surveillance by agents of the state will go a long way towards determining what kind of society we shape for ourselves.

Privacy is a fundamental human right, recognized as such by the United Nations. The level and quality of privacy in our country risks being struck a crippling, irreparable blow if we allow ourselves to become subjected to constant, unrelenting surveillance and observation through the lens of proliferating video cameras controlled by the police or any other agents

of the state.

As RCMP Commissioner Zaccardelli did not agree with Commissioner Radwanski's findings, he instructed his officers to continue their surveillance. Commissioner Zaccardelli enjoyed the support of Canada's Solicitor General MacAulay. As a result, Radwanski instructed counsel to commence a Charter challenge in the Supreme Court of British Columbia. Ultimately, that decision will almost certainly be appealed to the Supreme Court of Canada. One hopes that bench will avail itself of the opportunity to speak at length to the issues of the invasion of our privacies through technological means. How will that decision read? It would be immensely presumptuous to put words in the mouths of the Supreme Court of Canada, but it is very instructive that Radwanski, before proceeding with the Charter challenge, obtained the opinion of Gerard La Forest, retired Justice of the Supreme Court and particularly respected for his grasp of public policy issues. In his letter of opinion¹³⁶ to Mr. Radwanski, former Justice La Forest said (among many other things):

Although you have asked for a legal opinion, I should stress that the issue of general video surveillance is not solely or even primarily a legal question, at least not in the sense that it is to be resolved exclusively by the courts. As you are well aware, it raises broad socio-political issues, the resolution of which will help to define the proper relationship between the individual and the state in coming decades. As I will attempt to describe later, the courts will have a role to play in defining this relationship. But ultimately the continuance of a free society depends on an alert citizenry, the constant scrutiny of legislative organs (now supported by offices like your own), and the sensitive exercise of the executive's power to control overreaching by the police.

The nub of the problem lies in the nature of policing and the attitude of police. Police tend to define their job as the prevention of crime for the protection of the public. Naturally, they strive to obtain the tools they believe may be useful in fulfilling these objectives. But as in the case of general video surveillance, they often do so with little or no empirical evidence that these tools will reduce crime, or even materially assist in doing so. They also often underestimate the dangers these tools may pose to other basic societal values. That is why executive control must be carefully exercised, and why we should look with suspicion at demands for additional intrusions on individual liberty.

In seeking broader powers, the police are assisted by a common misperception in the wider public that the purpose of the criminal law is somehow to eradicate crime. But as the Law Reform Commission noted in its report *Our Criminal Law*,¹ the existence of crime is dependent on many other social conditions. In a free society, the real purpose of the criminal law is to underline the fundamental values of society for the vast majority of citizens who are law abiding.

¹³⁶ http://www.privcom.gc.ca/media/nr-c/opinion_020410_e.asp

The police are often abetted in obtaining unnecessary, ineffective, and dangerous powers by the reflexive belief among many citizens that restrictions on liberty do not affect them, or more dangerously, that such restrictions are insubstantial and worth the sacrifice. This danger has been eloquently expressed by Walter Gellhorn as follows:

In every society, in every age, and certainly in our own there are multitudes who, in Archibald MacLeish's phrase, "fear freedom or are frightened of the loneliness it implies." For the most part, however, inroads on freedom are not initiated by those who prefer that others assume responsibility for directing their lives; these flabby folk become the hordes that sustain dictatorships, but they themselves are too inert to bring it to pass. We need not worry, in my estimation, that freedom will be brought low upon their initiative. Nor do I think that evilly motivated men will successfully trick us into surrendering one after another bastion in a heedless quest for an unattainably perfect security. The real danger lies among those of us who genuinely desire to protect freedom, and who think that this can best be done by limiting it. They propose to give a little here to protect a lot there. The motive is admirable, but the judgment is unsound. The very amplitude of our American brand of freedom sometimes seduces us into believing that a good deal of it can be spent without anyone's really noticing the difference--that we can afford, as Carl Becker put it, "to take liberties with our liberty." But the trouble is that small restrictions accumulate into large restrictions and, in the process, may become as habitual as, before, freedom was. Restrictions justified as necessary safeguards of freedom may in fact safeguard freedom out of existence altogether.

In Kelowna and elsewhere, some citizens have said that they have nothing to hide and are comforted in the belief that video surveillance will permit the police to check the actions of malefactors. But this wholly mistakes the nature of a free society. It is not only criminals who are harmed by intrusions on liberty. In the absence of compelling justification, we should all be free to move about without fear of being systematically observed by agents of the state. As the Supreme Court put it in *Dagg v. Canada (Minister of Finance)*, "privacy is grounded on physical and moral autonomy - the freedom to engage in one's own thoughts, actions and decisions." Privacy, in other words, is at the heart of liberty in a modern state.

.....

As you have compellingly argued, video surveillance without cause poses a grave threat to privacy. This threat is compounded by continuous recording. As I emphasized for the Supreme Court in *R. v. Duarte*, "if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance." The fact that video-only recording does not capture oral communications is not determinative. In *R. v. Wong*, which involved surreptitious video-only surveillance, I again spoke for the Court in holding that "the threat to privacy inherent in subjecting ourselves to the ordinary observations of others pales by comparison with the threat to privacy posed by allowing the state to make permanent electronic records of our words or

activities."

.....

Though the courts have yet to pronounce on the constitutionality of general video surveillance, the principles that have been developed under section 8 can be applied by analogy to the present situation. In *Duarte*, the Court considered whether the surreptitious electronic recording of a conversation between a suspect and a police informant violated section 8. Writing for the majority, I stated that

. . . if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States v. White*, *supra*, put it, at p. 756: "Electronic surveillance is the greatest leveler of human privacy ever known." If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.

.....

The same reasoning was applied in *Wong*. There, I determined for a majority of the court that the unauthorized, surreptitious video recording of activities in a private hotel room violated section 8. I explained my reasoning as follows:

[I]f a free and open society cannot brook the prospect that the agents of the state should, in the absence of judicial authorization, enjoy the right to record the words of whomever they choose, it is equally inconceivable that the state should have unrestricted discretion to target whomever it wishes for surreptitious video surveillance. George Orwell in his classic dystopian novel *1984* paints a grim picture of a society whose citizens had every reason to expect that their every movement was subject to electronic video surveillance. The contrast with the expectations of privacy in a free society such as our own could not be more striking. The notion that the agencies of the state should be at liberty to train hidden cameras on members of society wherever and whenever they wish is fundamentally irreconcilable with what we perceive to be acceptable behaviour on the part of government. As in the case of audio surveillance, to permit unrestricted video surveillance by agents of the state would seriously diminish the degree of privacy we can reasonably expect to enjoy in a free society. . . . Moreover, as *Duarte* indicates, we must always be alert to the fact that modern methods

of electronic surveillance have the potential, if uncontrolled, to annihilate privacy.

It is true that Duarte and Wong dealt with interceptions in contexts where the expectation of privacy was high. The expectation of privacy on a public street, in contrast, is very much attenuated. We cannot reasonably expect the police to refrain from observing or overhearing persons they consider to be suspicious. To require the police to have cause or obtain authorization for such surveillance would unjustifiably limit their ability to investigate and prevent crime. Indeed, it may be permissible for the police to use a video camera to observe and record a particular suspect's movements in public spaces. For this type of targeted surveillance, the relatively minor intrusion into privacy may possibly be balanced by the state's interest in effective law enforcement.

But comprehensive and continuous video surveillance is a very different matter. It permits the police to systematically observe, often at high resolution and across a broad spatial expanse, everyone present within the camera's or cameras' range. This type of video surveillance is equivalent to having individual police officers closely follow, 24 hours a day, every person within a certain geographical space. That would be a police state, not a free society. We may not have a reasonable expectation that the police will never observe our activities in public spaces, either incidentally or as part of a targeted investigation. But surely it is reasonable to expect that they will not always do so. Melvin Gutterman articulates the underlying rationale for this conclusion as follows:

In a variety of public contexts, we may expect to be casually observed, but may justifiably be outraged by intensive scrutiny. In these public acts we do not expect to be personally identified and subject to extensive surveillance, but seek to merge into the "situational landscape." The ability to move about freely without constant supervision by the government is an important source of individual liberty that must be addressed. A fear of systematic observation, even in public places, destroys this sense of freedom. Justice Douglas recognized the importance of this privacy value in a democratic society, commenting that free movement is as dangerous to a tyrant as free expression of ideas or the right of assembly and is, therefore, controlled in most countries.

.....

There is reason to believe, moreover, that general video surveillance can be readily abused. There is evidence that it is often used to monitor unconventional (but not criminal) behaviour and to control members of marginalized groups. As I noted in Landry, broad, discretionary search powers are more likely to be used against disadvantaged groups than the "economically favoured or powerful."

.....

In summary, it is my view that the type of video surveillance employed in Kelowna, with or without continuous recording, violates section 8 of the Charter. This is not to say that all forms of warrantless video surveillance are necessarily unconstitutional. As mentioned, the surveillance of specific individuals in public places may be permissible. And there may be situations where

limited forms of general surveillance is justified, for example the time-limited surveillance of a high security event. I refrain from commenting further on this possibility in the absence of a concrete factual scenario. It should suffice to say that it is my opinion that the type of general video surveillance conducted in Kelowna violates section 8 of the Charter.

More recently, Radwanski has usefully contributed to the debate by commenting¹³⁷ on the “Lawful Access” proposals floated by Canada’s Minister of Justice, Attorney General, Solicitor General and Minister of Industry.¹³⁸

The importance of the lesson? To the Canadian observer, this is (in the vernacular) a “no brainer”! Given the importance of the issues, given the remarkable similarities of our social, economic, political and legal cultures and given the obvious usefulness of the Privacy Commission as a lightning rod, it is impossible to understand why the US doesn’t copy the institution. The only possible reasons which come to mind are that the US couldn’t imagine that someone else could have got there first (obviously, this can’t be the answer) or that there are powerful economic and political forces in the US who wouldn’t want to see such a powerful centre of political discussion of liberty issues (and again, who could imagine this to be the case.) A very useful argument of the importance of a privacy commissioner, and whether or not the US could adopt the same approach has been (politely) made by Ontario’s Privacy Commissioner, .¹³⁹

The Canadian experience is similarly useful to demonstrate that the discussion of privacy and freedom of speech discussion outside a ritualistic analysis of US First and Fourth Amendments can yield essentially the same results.¹⁴⁰

¹³⁷http://www.privcom.gc.ca/media/le_021125_e.asp

¹³⁸Infra, footnote 175

¹³⁹ William S. Challis & Dr. Ann Cavoukian THE CASE FOR A U.S. PRIVACY COMMISSIONER: A CANADIAN COMMISSIONER'S PERSPECTIVE 2000 19 J. Marshall J. Computer & Info. L. 1

¹⁴⁰ See for instance the discussion in *Trinity Western University v. British Columbia College of Teachers* [2001] 1 S.C.R. 772
http://www.lexum.umontreal.ca/csc-scc/en/pub/2001/vol1/html/2001scr1_0772.html

There is perhaps one other lesson Canadians can offer. We too have had periods when we felt justified, as a society, to suspend civil liberties, most recently during the October Crisis. Without exception, we have found ourselves embarrassed and ashamed of our over-reaction.¹⁴¹ One would like to think we have learned our lesson.....

Narco-privacy: the best secrecy money can buy

For enough narco-dollars you get the best. Consider this:

“The drug lords have deployed advanced communications encryption technologies that, law enforcement officials concede, are all but unbreakable. They use the Web to camouflage the movement of dirty money. They track the radar sweeps of drug surveillance planes to map out gaps in coverage. They even use a fleet of submarines, mini subs, and semisubmersibles to ferry drugs...

Henao's cartel is a champion of decentralization, outsourcing, and pooled risk, along with technological innovations to enhance the secrecy of it all. For instance, to scrub his profits, he and fellow money launderers use a private, password-protected website that daily updates an inventory of U.S. currency available from cartel distributors across North America, says a veteran Treasury Department investigator. Kind of like a business-to-business exchange, the site allows black-market money brokers to bid on the dirty dollars, which cartel financial chiefs want to convert to Colombian pesos to use for their operations at home. "A trafficker can bid on different rates -- 'I'll sell \$1 million in cash in Miami,'" says the agent. "And he'll take the equivalent of \$800,000 in pesos for it in Colombia." The investigator estimates the online bazaar's annual turnover at as much as \$3 billion.

The talent and tools are among the best that money can buy, and it shows. For instance, Henao's communications have become so advanced that they have never been intercepted, Colombian intelligence sources say.

The range of Urrego's network extended across the Caribbean and the upper half of South America. He and his operatives used it to send text messages to laptops in dozens of planes and boats to inform their pilots when it was safe to go, and to receive confirmations of when loads

¹⁴¹ Canada's record under the War Measures Act has not been pretty. See the description of internment of Ukrainians, Jews, Japanese and others at http://www.educ.sfu.ca/cels/past_art28.html See also Trudeau's War Measures Act Speech <http://www.nelson.com/nelson/school/discovery/cantext/speech2/1970trwm.htm>

were dropped and retrieved. According to one intelligence official who analyzed Urrego's network, it was transmitting 1,000 messages a day -- and not one of them was intercepted, even by U.S. spy planes."¹⁴²

Although sensational, the story is not isolated. The Russian Mafia runs a very sophisticated credit card fraud scheme based on hacking internet transactions. In Canada, the front-runner to replace the recently imprisoned Hell's Angels leader is a computer expert. Crime understands and uses the power of technology. It is not very likely that criminals will trouble themselves with any kind of restriction on the use or export of cryptography. What policy makers really need to ask themselves, in light of the sophistication of criminals, is whether there is any policy justification for denying good citizens the most powerful encryption available.¹⁴³

The internet as freedom fighter: can democracy grow from a cyber-café?

Tyrants fear an informed citizenry. The role of technology in the downfall of the Iron Curtain has not been lost on repressive leaders. The internet thus presents despots with an exquisite dilemma: how to obtain the economic benefits of technology without exposing their people to dangerous ideas? A few regimes such as North Korea and Myanmar simply don't permit the internet—Myanmar has recently even gone so far as to clamp down on corporate wide area networks¹⁴⁴. Others, in particular Saudi Arabia as discussed above, engage in extensive filtering. Vietnam¹⁴⁵, Kazakhstan¹⁴⁶

¹⁴² Kaihla, Paul Business 2.0 July 2002 "The Technology Secrets of Cocaine Inc." <http://www.business2.com/articles/mag/print/0,1643,41206,00.html>

¹⁴³ Stellin, Susan New York Times March 28, 2002 "Terror's Confusing Online Trail" ends with quoting Lance Cottrell, president of Anonymizer.com "That's kind of the irony in this. For the honest good citizen, privacy is extremely endangered and tracking is ubiquitous. But I don't see a sign that we've ever been able to build a system that criminals with serious intent haven't been able to circumvent."

¹⁴⁴ SiliconValley.com July 12, 2002 'Myanmar makes unlicensed WAN links illegal' In a country where internet is severely limited and censored, the Ministry of Post, Telegraphs and Communications will require companies with WANs to be licensed. License holders will be subjected to periodic checks and will be required to allow encrypted data to be decrypted. Penalties range from seven to fifteen years in prison.

¹⁴⁵ SiliconValley.com June 8, 2002 "Vietnam steps up fight against anti-government materials on Internet" describes "tighter blocking of sites", "replacing outmoded filters", "severely dealing with people who misuse the internet".... See also smh.co.au August 6, 2001 'Vietnam orders new crackdown on Internet dissent' Government has asked authorities to mete

and others¹⁴⁷ use traditional threats, bullying and imprisonment to discourage inappropriate net access,

The Chinese approach to cyberpolicy is noteworthy and quite sophisticated. Whether it delivers for China's leadership remains to be seen.¹⁴⁸ At least some opinion is that China's cyberwall is nearly complete and nearly impenetrable.¹⁴⁹

China is rushing headlong into the digital age— the internet is being embraced with a fervor unmatched almost anywhere. In terms of raw numbers of users, the Chinese have already achieved second place¹⁵⁰ after the United States and is gaining fast¹⁵¹. There is clearly no turning back.

out severe punishment to those caught spreading dissent online. Access to objectionable sites such as those of the emigre opposition, pornography, state secrets and reactionary documents is blocked and e-mail is regularly monitored.

¹⁴⁶ Institute for War and Peace Reporting August 6, 2002 'Kazakhstan: New Threat to Internet" Second instance of author of internet article criticizing the president or his family being sued or arrested.

¹⁴⁷Reuters August 5, 2002 'Iran reformers use Net to fight press ban' describe how news websites are popping up faster than the anti-reform government is able to shut down newspapers.

¹⁴⁸ See recent and thorough RAND study: Michael S. Chase, James C. Mulvenon, "You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies" <http://www.rand.org/publications/MR/MR1543/>

¹⁴⁹Grebb, Michael Wired News, November 5, 2002 "China's Cyberwall Nearly Concrete" <http://www.wired.com/news/politics/0,1283,56195,00.html>

¹⁵⁰ Wingfield-Hayes, Rupert BBC News Online June 5, 2002 'China loses grip on internet' China is now world's second-largest user of internet (56 million last year, growing 6% per month). Communist government making huge efforts to contain (eg. hi-tech police force keeping watch on net 24 hours a day— the 'great fire-wall of China') to keep out all kinds of bad influence from Playboy to BBC. Although hard core democracy and other sites are routinely shut down and operators imprisoned, even government officials use the net to get out information more effectively than waiting for the dull news agencies. People all over China now engage in dialogue and debate. "The Chinese state's once total control on information has been broken and hard as it may try it has little hope of regaining that control." But also see Nairne, Doug, South

The Chinese leadership clearly understands these dynamics and in fact encourages the general thrust. Without doubt, though, the leaders understand that the internet will also bring change China in ways they may not want. How can China reap the benefits of the e-commerce and the internet, yet keep at bay the fearsome viruses of democracy, religious belief and other 'corrupt' values? Even without the net, democratic ideals, Christianity, Falun Gong, Eastern Lightning, Tibetan nationalism and a host of other unsettling movements have flourished, but generally the authorities have kept a lid on them. Clearly the lid comes off unless the authorities can figure out how to maintain a high level of censorship.

China's leadership understands that they have another problem, however. China is eager to regain its traditional role as a first-world state as befits its population, technological and economic power. It has become absolutely dependent on its international trade. The world community expects China's leaders to behave in a fashion that the West finds acceptable. If political power comes from the barrel of a gun¹⁵², at least on CNN China must be seen as a modern society. Censorship cannot be seen to be as heavy-handed as in past decades. At least for world public consumption, censorship must appear reasonable and proportionate.

The final piece of the puzzle is the cybercafe. Not every child in China has her own power pentium multimedia full tower computer with sound surround and high speed internet connect with full gaming capabilities. In fact, not every home has even a basic machine. To be precise, most homes do not have their own computers or internet connection (although certainly many do). In such a setting, the cybercafe becomes the access of choice for most Chinese. In traditional cyberpolicy analysis, the cybercafes are considered a chokepoint. The other major chokepoint, as it is in the West, is the ISP.

China Morning Post, August 14, 2002 'China tightens Web control' Discussion of transition from the "Great Firewall of China" in which attempts to filter content coming into China through the five internet gateways was proving ineffective, to the Golden Shield approach of clamping down on individual users and internet cafés . The Golden Shield will link national, regional and local security agencies and networked video cameras, linked to real-time databases spread across the country that will store a digital record of every citizen. The project will go well beyond blocking and monitoring internet content and incorporate speech and facial recognition, CCTV, smart cards, credit records and other surveillance technologies. Western technology companies are vying for the opportunity to supply the technology.

¹⁵¹BBC News Online 23 July, 2002 "China internet use grows"
<http://news.bbc.co.uk/2/hi/business/2145865.stm>

¹⁵² Mao Tse-tung "Problems of War and Strategy" *Selected Works*, Vol. II, p. 224.

Chinese cyberpolicy would seem therefore to have three prongs. The crudest is filtering and snooping¹⁵³, nearly as crude, but perhaps more effective is to control the cafes, and the most elegant, but of unknown effectiveness, is the Pledge. China's communist rulers understand business and know all about licensing power as a policy device. Knowing that service providers and internet cafes are for-profit businesses, they have a simple proposition: "Play by our rules and you can be in business, but if you don't we'll shut you down."

First, in March 2002 over one hundred service providers and other significant players in the Chinese cyber economy were invited to sign a public pledge to "promote self-discipline in the country's Internet industry". Its thirty-one articles are calculated to "advance the healthy and orderly development of the Internet industry in China." The key principles are "patriotism, observance of the law, fairness and trustworthiness" and the pledge encourages "lawful, fair and orderly competition and values the protection of intellectual property, network security and the elimination of deleterious information from the Internet."¹⁵⁴ Those who fail to maintain these lofty goals will be expelled from the group (effectively losing their license) and individuals could face severe prison terms.¹⁵⁵

Cybercafés are at the other end of the internet food chain. While some may resemble a western cybercafé, many in China tend to be in basements, attics and backrooms—partly as a cost measure and partly to offer more privacy than might be the case in a storefront operation. This is not the sort of scene a one-party state relishes. At the same time, who wanted to be seen making a frontal assault on the major source of internet access in the country? As generally happens, the opportunity to take action presented itself.

In the early hours of June 16, 2002 a fire broke out in a popular cybercafé in Beijing. Twenty-four young people died in the fire: "The cafes are often dimly lit, hidden from view and with heavy doors to deter the authorities - but which can turn them into a death trap in case of fire."¹⁵⁶

In order to prevent this sort of event in the future, China intends a thoroughgoing licensing and inspection system to enforce the safety of "Internet Bars". No such café may open or continue to operate without being licensed, and no license will issue or remain issued without ongoing safety

¹⁵³ Wingfield-Hayes, Rupert BBC News Online June 5, 2002 describes a high-tech policy unit surveilling the internet 24 hours a day, 7 days a week, the Great Firewall of China

¹⁵⁴ http://news.xinhuanet.com/english/2002-03/26/content_332182.htm

¹⁵⁵ See Yahoo! Tech Asia August 6, 2002 'China jails politically incorrect Net user for 11 years'

¹⁵⁶ BBC News, June 16, 2002

inspection and site approval. However, the licensing will also hinge on approval by the cultural authorities and will require all visitors to the café to be registered. These measures should go far to rein in unsupervised and unsavory internet use.¹⁵⁷

Can the Chinese authorities actually foster e-commerce and “proper” internet use while suppressing dissent? Some think they can¹⁵⁸ and some do not¹⁵⁹. I tend to agree with those who believe that the genie is out of the bottle— various privacy programs such as Six/Four¹⁶⁰ and Camera/Shy¹⁶¹ are almost certain to provide users in repressive societies a mechanism to communicate, visit, or even run web pages with near impunity. I also agree with those who think that the Chinese authorities are playing a brilliant game of chess, keeping the advance of free expression and thought in China to the slowest possible pace while the leadership plays out its personal agenda.

History, of course, repeats itself. In the years immediately after Caxton introduced printing to England the government limited printing presses to London (and to a lesser extent to Oxford and Cambridge) because it wanted the dissemination of printed material to be centralized and easy to rein in. Of course, as printing drove literacy and as literacy drove demand, more and more printers were required, the business became democratized and very difficult to control. The monarchy and the government of the day survived, printing and the advance of the middle class proceeded apace, the tension between chaos and oppression found an unspoken middle ground. Will the Chinese do the same? Probably. Let’s hope so.

What are the lessons for policy makers?

1. If the draconian regimes can’t keep a lid on thought, can we? Should we?
2. Should we be enabling the regimes or the aspirations of freedom seekers? Assuming the latter,
 - a. Are we better to encourage or discourage encryption and other privacy technologies?

¹⁵⁷ See somewhat word-for-word translation of Chinese government news release at http://ce.cei.gov.cn/enev/new_g1/pl00gh17.htm

¹⁵⁸ See Bodeen, Christopher news.com.au July 15, 2002

¹⁵⁹ Wingfield-Hayes, Rupert BBC News Online June 5, 2002

¹⁶⁰ Shachtman, Noah ‘A New Code for Anonymous Web Use’ Wired News July 12, 2002

¹⁶¹ Reuters July 14, 2002 ‘Hacker group targets Net censorship’

- b. What example do we set with our technopolicy?
- c. In general, how do our technopolicy choices and directions (eg. bordering technology) impact on freedom seekers in repressive regimes?

You can't say that on the Net!– controlling content

"If we don't believe in freedom of expression for people we despise, we don't believe in it at all."
Noam Chomsky

Ouch! Is Chomsky right, or is he a dreamer? We have already examined Saudi Arabia's and China's impressive attempt to put their kingdoms behind firewalls. But they're closed, repressive regimes. But even in our free societies, there are subject matters we don't want discussed publicly. Perhaps more correctly, there are subject matters which are determined by the majority to be taboo. In Canada, for instance, we have little official patience for those who hold that the Holocaust is a myth, or who are intolerant of sexual preferences.¹⁶² The Germans and the French are understandably sensitive about Nazi-related subjects, and want to limit the ability of ultra-right or neo-Nazi groups to use the web for their evil propoganda.¹⁶³ When the Vatican complained of a web site which displayed rude and blasphemous doggerel about the Virgin Mary, the Italian police quickly shut it down.¹⁶⁴ The Russian authorities, quite willing to retain accustomed autocratic power, had little difficulty granting police sweeping cyber powers.¹⁶⁵

¹⁶²Canadian Press August 8, 2002 'Human rights tribunal orders anti-gay Web site to cease and desist' Canadian Human Rights Tribunal orders virulent anti-gay website to shut down.

¹⁶³Kaplan, Carl S. The New York Times February 11, 2002 'French Decision Prompts Questions About Free Speech and Cyberspace' *Licra v Yahoo* re sale of Nazi memorabilia on internet. Although U.S. courts are unwilling to uphold French court's order over US company in US, the risk is that the US company's assets could be seized in France. See also Agence France-Press July 29, 2002 'French groups demand shutdown of Web site linked to Chirac assassination attempt' Two civil rights associations said they have asked a French court to ban a Web site run by a racist group linked to the man who tried to assassinate President Jacques Chirac.

¹⁶⁴ Yahoo! News Singapore July 10, 2002 'Blasphemous Internet sites closed after a Vatican complaint' "The *l'Osservatore Romano* paper said a special police unit "took over an Internet site due to the blasphemous nature of unrepeatable words which accompanied the name of the Madonna," adding Tuesday that four other similar sites had also been closed.

¹⁶⁵ McCullagh, Declan CNET News.com June 24, 2002 "Russia poised to restrict Net activities" In the guise of fighting extremism, Russian police given vast powers.

Each new technology of mass communications has refreshed the eternal debate: what subject matter cannot be tolerated? Why not? What must we do to prevent it within our borders? How can we prevent its import from abroad? Most of those questions had working answers, until the internet came along. The internet gave Everyman a printing press, a broadcasting station and a soapbox. Worse still, from the perspective of the censor, the net made Everyman anonymous and also made it easy for him to publish his doggerel from abroad. Concepts of restricted speech, already scrambled by the advent of the net,¹⁶⁶ are further troubled by an admixture of conflict of laws.

The reader may be disappointed that this paper will not now seek solutions to these thorny issues. On the other hand, the reader may be relieved, given that such a discussion could fill several books. It is enough for now to raise the issues so as to weave some of the threads into the fabric of an overall cyberpolicy toward the end of the paper.

Bless you, my file-- the Vatican speaks to the issues

“In this document we wish to set out a Catholic view of the Internet, as a starting point for the Church's participation in dialogue with other sectors of society, especially other religious groups, concerning the development and use of this marvelous technological instrument. The Internet is being put to many good uses now, with the promise of many more, but much harm also can be done by its improper use. Which it will be, good or harm, is largely a matter of choice—a choice to whose making the Church brings two elements of great importance: her commitment to the dignity of the human person and her long tradition of moral wisdom.”¹⁶⁷

It is not just what the Vatican has to say about the internet which is important, but the example it has set. Ultimately, good cyberpolicy must bring together more than the work of lawyers and engineers—it must include the voice of entities who bring to bear a “commitment to the dignity of the human person and (a) long tradition of moral wisdom”.

Drawing it together— a working approach

What we have seen so far is that humankind faces a host of thorny issues which tangle together in

¹⁶⁶See the provocative commentary of my former colleague, Kim von Arx in “LitOral: A New Form of Defamation Consciousness” (2002) 1 (Issue 2) Canadian Journal of Law & Technology

¹⁶⁷ PONTIFICAL COUNCIL FOR SOCIAL COMMUNICATIONS ETHICS IN INTERNET
http://www.vatican.va/roman_curia/pontifical_councils/pccs/documents/rc_pc_pccs_doc_20020228_ethics-internet_en.html

a dense thicket of convergence. Lurking amongst the thorns are powerful, opportunistic interests who seek to preserve and expand in cyberspace those privileges they enjoy in real space. Anyone who doesn't tremble at least a little just doesn't understand the problem.

Getting to this point has necessarily been tough sledding, but one needs the full tour to appreciate that cyberpolicy cannot be approached casually or on an *ad hoc* basis. But while the issues may be complex, the foundations of good cyberpolicy need not (and should not) be complex. They must, however, respond to elementary logic, for "... no system of law can be workable if it has not got logic at the root of it." In the following (and final) sections we propose some essential principles and a few pragmatic applications of those principles.

Principles

The essential principles of cyberpolicy should be few and simple. Effective cyberpolicy requires two feet firmly planted— one in technological understanding, the other in wisdom.

Inserted from mid-section:

What are the absolute essentials? They are few and simple:

- preserve and enhance freedom of thought and expression
- preserve and enhance privacy of the person
- preserve and enhance democratic institutions
- ensure the integrity of the cyber infrastructure
- ensure the truthfulness of the record

It is not likely that these key principles will lead to much controversy in a free and democratic society. The greater risk, though, is that they become little more than lofty preambles, the stuff of valediction, but ineffectual. In order to ensure that the principles have robust application, cyberlaw must have certain characteristics. It should:

- be big-picture in scope
- be transparent in objective
- be flexible, proportionate and accommodative in application
- require full accountability
- where erosion of historic rights can be rigorously justified, such erosion must be limited in time and application

Always ask of those who seek an extension of existing privilege:

- what is wrong with the current situation?
- how will the proposed extension of privilege fix what is wrong?
- what are you willing to give up in exchange?
- what guarantees will you give that it will work?
- what price will you pay if your guarantee doesn't hold?
- how long will the privilege last? What will trigger the end of the privilege?

Principle One: Wisdom

Cyberpolicy will irreversibly determine the nature of our humanity. As we move forward, we must hold firm to the highest and best principles which have made our civilisation what it is. This is neither trite nor maudlin, nor is it optional. Some of the features of this principle will be:

- proceeding from the high ground. This will be frequently, but not exclusively, a constitutional discussion. Given the international scope of cyberspace, however, the discussion will increasingly have to rise beyond the local specifics to the essential principles which underlie western democracies.¹⁶⁸
- taking the big-picture view
 - understanding and responding appropriately to the various agendas and interests. Law reform commissions and similar bodies need to sponsor wide discussion with dialogue across the spectrum from pure mathematicians to theologians— anyone who has something relevant to say about the Brave New World.
 - “It’s a big world, after all”— the West, and the US in particular, will not maintain an indefinite lock on technology.¹⁶⁹
 - respond to crises in a measured fashion^{170, 171}

¹⁶⁸ Yaman Akdeniz: No Chance for Key Recovery: Encryption and International Principles of Human and Political Rights <http://webjcli.ncl.ac.uk/1998/issue1/akdeniz1.html>

¹⁶⁹ Cockburn, Christina A., WHERE THE UNITED STATES GOES THE WORLD WILL FOLLOW--WON'T IT? 1999 21 Houston Journal of International Law 491

¹⁷⁰ A. ALAN BOROVOY (General Counsel, Canadian Civil Liberties Association): Since September 11th...While it always behooves us to keep an open mind about any new measures, our open mind should be accompanied by a cool head and a skeptical disposition. If we were to

- national policy makers can no longer make law in isolation¹⁷²
- except in the rarest cases, principles of democratic process, free expression and human dignity trump all other factors.¹⁷³¹⁷⁴

needlessly surrender any of our precious freedoms, we could wind up awarding the terrorists a gratuitous victory. See also the thoughtful essay of Professor Patricia J. Williams “This dangerous patriot's game” The Observer December 2, 2001 <http://www.observer.co.uk/libertywatch/story/0,1373,610367,00.html>

¹⁷¹Featherly, Kevin Newsbytes April 3, 2002 “Support For Government Surveillance Slips— Harris Poll” Support for expanded high-tech government surveillance has diminished during the six months following the Sept. 11 terrorist attacks, new Harris Poll figures show. Supporters for surveillance of cell phones and e-mail traffic are now in the minority.

¹⁷²A wider issue— most governments, even of democratic nations, have a different view of privacy for their own citizens and/or internal matters than they do of foreigners and/or external matters, viz the nonchalant approach of customs officials, frequently reported. See US Customs Border Security Act which will extend the right of search to any mail going into or out of the US without a search warrant. (US customs officials can be sued civilly for wrongful searches, but not if they perform the search in good faith). More important, security agencies of western nations have excellent working relationships— given the interconnected world, what is to stop the agency of one country conducting surveillance against citizens of another in ways which would be off-side in the home country?

¹⁷³Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety. - Ben Franklin, "Historical Review Of Pennsylvania

" We are in the process of doing things in defense of our society which may very well produce a society which is not worth defending." - John LeCarre

¹⁷⁴ Jaffey, John The Lawyers Weekly July 5, 2002 ‘No need to restrict human rights in protecting security: Graham’ ‘Canada’s minister of foreign affairs sees no need to restrict human rights in order to protect public security.’ “When appropriately conducted, the protection of public security should not undermine respect for human rights; rather it can and must enhance those rights.” “The fight against terrorism must not be used as a pretext for repression.” ‘Apart from preventing terrorism, Graham said our most compelling challenge “is to uphold the values and norms we cherish— democracy, respect for the rule of law and human rights.” Since the whole point of the fight is to defend freedom, the government’s method cannot deprive citizens of freedom of speech, freedom to organize and freedom of dissent.

- rarely is it necessary to legislate in the closet— as a rule, consult widely¹⁷⁵ where issues impact on questions of democracy, freedom of expression and human dignity. In those cases where it is deemed necessary to legislate with haste, a very early (and absolute) sunset is essential.
- there is a moral imperative to set an example to despotic societies and to allow the winds of technological freedom to blow from our shores¹⁷⁶

Principle two: Technological understanding

Cyberpolicy is too often characterized by reactive, ill-considered lawmaking by policymakers who don't get the big picture and who are being pushed too hard and too fast by this or that interest group. This is far less likely to occur if the policymaker has a grasp of the technology, the trends and the implications.

- understand the trends, appreciate where they may lead in a world of converging technologies (this calls for courts, and more so legislators, to be well informed) (suggestion re Wired, etc.)
- wherever possible, take a minimalist approach
- similarly, the best law is generally technologically neutral. As a rule, let technology solve its own problems¹⁷⁷

¹⁷⁵ For example, the Canadian government published (August 25, 2002) “Lawful Access— Consultation Document, available at http://www.canada.justice.gc.ca/en/cons/law_al/law_access.pdf. The paper begins with the Council of Europe’s *Convention on Cyber-Crime*, discusses some of the key issues with respect to data interception, preservation and production and calls for input from the full range of stakeholders from law enforcement through civil liberties organizations. Notwithstanding my fundamental difficulties with many of the proposals, the consultative approach (assuming that it’s more than token) is correct and welcome.

¹⁷⁶ Krebs, Brian Newsbytes February 19, 2002 “Lawmakers Urge Russians to Drop Surveillance Plans” US Congressional delegation spoke out against proposals in Russian lower house to allow government to monitor online activity and require access to encrypted documents through use of key-escrow accounts. Duma members argued that government must retain ability to access computers and monitor online activity of its citizens in order “to ensure stability”.

¹⁷⁷For instance, JVC and partners in Japan have developed “Root” technology which records a special encryption key at the time a CD-ROM is pressed. The disc can be copied, but an attempt to use the copied disc will return an error message.

- preserve and foster the e-infrastructure and e-commerce

Pragmatism

- apply and expand existing tort¹⁷⁸ and equitable principles¹⁷⁹. Move accountability to where it will be effective^{180 181 182} Given the very similar balancing issues, the models of the Anton Pillar order and Mareva injunction can be used, particularly the prima facie right to civil damages, obligatory disclosure and high cost consequences of getting it wrong.
- give *Rylands*, nuisance and trespass clearer application in cyberspace

¹⁷⁸ What standards? See Lemos, Robert CNET News.com July 16, 2002 ‘Group offers computer security standard’ Describes Center for Internet Security establishment of benchmarks for security standards for computers to test if able to withstand various attacks. See also Wired News July 16, 2002 ‘Government’s Seal of Security’ Group of US government agencies have established standards and a software program to help computer users configure systems for maximum security against hackers and thieves. Proposing it be mandatory for all government computers.

¹⁷⁹ The Privacy Torts:How U.S. State Law Quietly Leads the Way in Privacy Protection A Special Report Issued by Privacilla.org <http://www.privacilla.org> July, 2002 http://www.privacilla.org/releases/Torts_Report.pdf

¹⁸⁰ McCarthy, Ellen Washington Post July 24, 2002 ‘Executives Advised to Take Role in Internet Security’ Internet Security Alliance recommends that executives adopt 10 key practices to protect organization’s vulnerable networks and content. Copy Bush’s auditor & CEO accountability concepts.

¹⁸¹ Yahoo! News August 7, 2002 ‘Two Laptops Missing from Central Command HQ’ At least one was believed to contain classified material. Chairman of Joint Chief of Staffs General Richard Myers: “In the end, security comes down to individual responsibility. It comes down to your trust and confidence in the people that work there. And you do all the appropriate checks and all that sort of thing to ensure that the people have the right background and motivations.” See also Wired News/Associated Press August 5, 2002 ‘Fed Lax with Laptops’ US DOJ has lost over 400 laptops, over half of which have sensitive law enforcement of national security information.

¹⁸² Brian McWilliams Wired News Aug. 28, 2002 “Website Security Flaw Costs ZD” Ziff Davis Media has agreed to revamp its website's security and pay affected customers \$500 each after lax security exposed the personal data of thousands of subscribers last year. <http://www.wired.com/news/business/0,1367,54817,00.html>

- create new causes of action and new heads of damages
- limit recovery in the case of those who fail to mitigate or otherwise fail to act prudently— for instance, failure to use firewalls or encryption, etc.¹⁸³ Tailor insurance law in the same fashion.
- use licensing as a policy device
- taxation can also be used as a policy tool
- expand the scope of accountability specifically to include public servants and public authorities who are found, on a balance of probabilities, to have used or authorized technology to infringe on the liberties of the citizen. In egregious cases, personal liability should be permitted¹⁸⁴
- as well as a general expansion of accountability and damages, expand the scope of compensation, costs, punitive and exemplary damages.¹⁸⁵
- cybersnooping must be treated analogously to wiretapping and searches. However, since it can be done so much more surreptitiously, there must be increased levels of disclosure and accountability

¹⁸³ Reuters, January 8, 2002 “U.S. Cyber Security Weakening” “US computer systems are increasingly vulnerable to cyber attacks, partly because companies are not implementing security measures already available, according to a new report released Tuesday. ‘Even without any new security technologies, much better security would be possible today if technology producers, operators of critical systems, and users took appropriate steps.’ said the Computer Science and Telecommunications Board of the National Research Council.

¹⁸⁴ Barton, Chris The New Zealand Herald March 21, 2002 “Passwords access for police” Proposed Terrorism Act will require New Zealand computer users to hand over passwords and encryption keys when asked. The law is in addition to rules which would ‘impose a duty to assist’ on ISP’s, on a cost-recovery basis (costs to be upon application to district court so as to avoid “trifling claims”). Law Commissioner Donald Dugdale said the thinking behind the obligation was that it was a civic duty. “The good citizen will help the police.”

¹⁸⁵ Hilzenrath, David S. Washington Post, May 23, 2002 “2 FBI Agents Charged in Internet Fraud Scheme” Two special agents charged with selling confidential information about investigations of companies to participants in stock-manipulation scheme. See also Krebs, Brian Newsbytes February 22, 2002 Sites Revealed Passwords For Thousands Of Ameritech Users Discusses how unsecured Ameritech site contained alphabetical, hyperlinked listing of dial-up users, complete with username, password, and dial-up phone number, unencrypted passwords, addresses....

- tampering with electronic data and records must have particularly severe civil consequences, in addition to criminal remedies
- other forms of snooping such as CCTV surveillance, random scans, and the like should be limited to specific events, on judicial warrant, specific purpose, time limited, the records to be sealed and destroyed after specific time
- cyber crimes:¹⁸⁶
 - redefine to create three classes:
 - crimes committed via the internet¹⁸⁷ and within this class:
 - crimes which are magnified because of the internet
 - crimes which are otherwise essentially the same as traditional crimes
 - e-crimes (that is, crimes which require the internet to commit)
 - crimes which harm the internet
 - deal with cyber crime realistically: if there is some evil, deal with deterrent penalty, rather than using the specter of the crime as an excuse to reduce civil liberty
- special periods of emergency such as terrorist acts or acts of war do present a special case, but can only permit limited amounts of temporary extraordinary measures.

Conclusion

It's time— rather, it's past time— that the body of lawmakers take up their rightful place and solemn responsibility to steer our fragile planet into a good cyberspace and not an evil one. Legislators,

¹⁸⁶ SiliconValley.com July 15, 2002 'House moves to increase penalties for cybercrime' House voted 385-3 to increase penalties for computer crimes and make it easier for ISPs to disclose dangerous material to government agencies. Appears to be narrowly focussed on national peril, has requirement for court orders, accountability. Follow up and see actual bill, following: Cyber Security Enhancement Act of 2002

¹⁸⁷See BusinessWeek online SEPTEMBER 2, 2002 "The Underground Web— Drugs. Gambling. Terrorism. Child Pornography. How the Internet makes any illegal activity more accessible than ever"
http://www.businessweek.com:/print/magazine/content/02_35/b3797001.htm?mainwindow

academics, judges, practising lawyers have, with hardly an exception, yielded the field of cyberpolicy to scientists, marketers and security agencies, each of whom has a legitimate but too narrow agenda. Lawmakers are conditioned by training and by experience to see the bigger picture, to understand the implications of the law and to build in contingencies and safeguards. We should be at the forefront of cyberpolicy. But we are not.

We are not at the forefront because, as a profession, we have failed to inform ourselves about the new technologies and their implications. We have left technology to the IT department and to the scientists. We are so unfamiliar with the territory that the special interests can tell us whatever they like and we have no idea we are being flummoxed. Yet, a '101' level understanding of the nuts and bolts of today's technology is not beyond the grasp of any law-school student or graduate, even the most technically challenged of them.

Cyberlaw and cyberpolicy are no longer specialties— they are part of the regulation of everyday life. The world we pass on to our children will have its shape because of our choices today. As lawmakers, we must move the discussion into the mainstream.