

United Nations
International Training Seminar
High Level Training Seminars
Seminar 6:

E-Government: The New Regulatory Paradigm

Prof. Lance J. Hoffman

Computer Science Department
The George Washington University
Washington DC 20052 USA
202 994-4955
hoffman@seas.gwu.edu

Government regulation responsibilities

- Regulating E-Commerce
- Maintaining citizen privacy rights
 - Balancing anonymity vs. accountability
- Managing intellectual property regime
 - Guaranteeing freedom of speech
- Facilitating computer system security
- Protecting critical infrastructure
- Recognize limits of regulation while ...
- Developing consistent regulatory framework that can be harmonized with other governments'

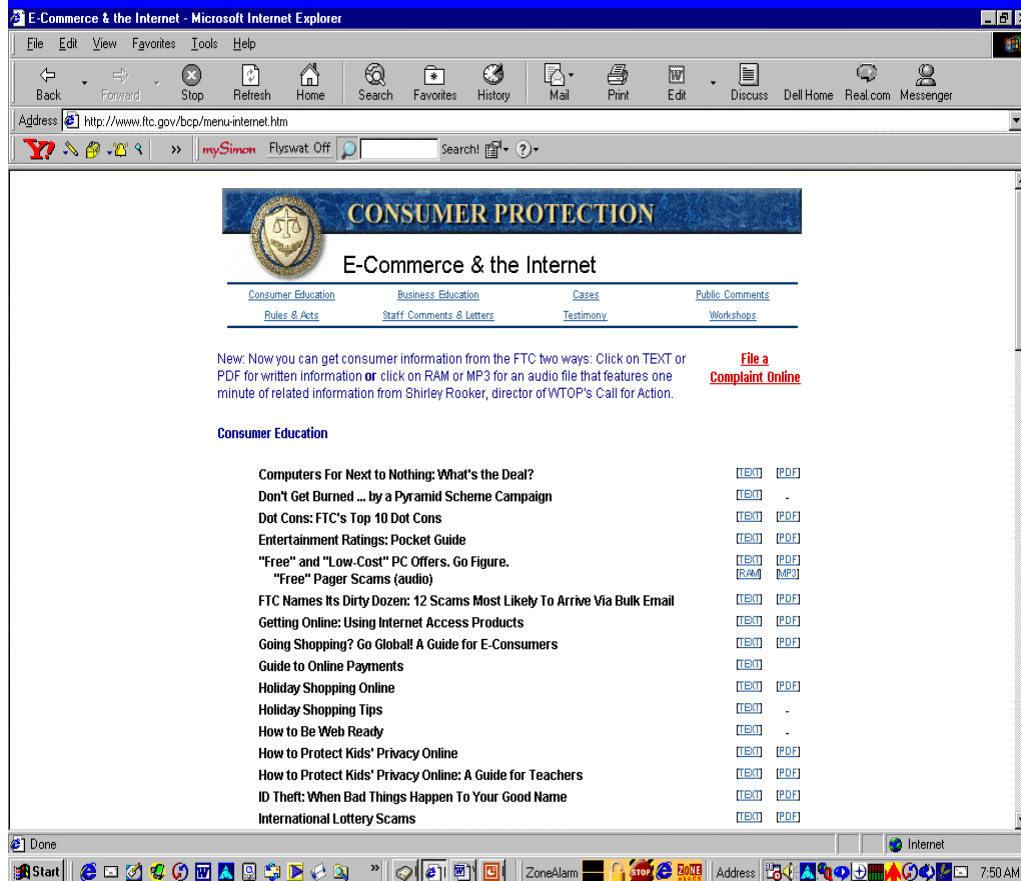
Government responsibilities

Regulating E-commerce

E-Commerce Issues

- Product Restrictions
 - Tobacco
 - What can be sold to children
 - Acceptable food products
 - Pharmaceuticals
 - Alcoholic beverages
 - Financial services
 - Textile and Wool Products
- Taxation control (customs, sales taxes, double taxation, VAT)
- Societal values
 - Language requirements (e.g., use French)
 - Accessibility standards (www.w3.org/wai) [10-20%]

Some possibly fraudulent e-commerce schemes



- Pyramid Schemes
- “Miracle” health and diet products
- Gambling and International Lottery
- Investment, Credit and securities scams
- Online Auctions
- Erotic Services

Government responsibilities

Maintaining citizen privacy rights

PRIVACY

Different meanings in different cultures
Users (consumers) want anonymity
and benefits (convenience, efficiency)
but may have to balance these



TIME Magazine, August 25, 1997

"The right to be left alone -- the most comprehensive of rights, and the right most valued by a free people." - Justice Louis Brandeis, *Olmstead v. U.S.* (1928). See also Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1891).

PRIVACY (DATA PROTECTION) COMMISSIONERS AND REGULATION WORLDWIDE

- 23 countries have data protection (privacy) commissioners
 - (See Canadian Privacy Commissioner's Annual Report at http://www.privcom.gc.ca/english/02_04_08_e.htm)
- European Union Data Directive has regulations:
 - No secondary use of data without an individual's informed consent
 - No transfer of data to non-EU countries unless there is adequate privacy protection (see, for example, www.export.gov/safeharbor)
- US still has no central regulation with respect to privacy.
Sectoral regulation in U. S.:

	Notice/ Awareness	Choice/ Consent	Access/ Participation	Integrity/ Security	Enforcement/ Redress
Financial services	Yes	Yes	Yes	Yes	Yes
Health	Yes	Yes	Yes	Yes	Yes
Online profiling	Yes	Opt-out			
Wireless	Proposed	Proposed		Proposed	Proposed

(John McCarthy, Forrester, Dec. 2000)


EXAMPLES WHERE BUSINESS HAS INVADED PRIVACY









- Unsolicited e-mail (spam):
- Online advertising agency monitored surfing of net users (DoubleClick)
- Attempted fire sales of user data, reneging on past promises (Toysmart.com)

SURVEILLANCE BY PRIVATE SECTOR

SURVEILLANCE BY PRIVATE SECTOR

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Dell Home

Address  https://www.1800ussearch.com/1800ussearch-78/mck-cgi/bsdlycos.pl?&lname= [REDACTED]

Customize Links  Microsoft  Windows Update  Windows  Yahoo!  cyberradio2000.com - It's A Whole New Way To Radio  Media  Backflip It!  RealPlayer

<http://windows.microsoft.com/isapi/redir.dll?...>



FIND OUT ABOUT:



Ron Keohane

320 [REDACTED] 4

Enter Approximate Age (if Known)

[Conduct a Search on Someone Else!](#)

HERE'S WHAT YOU GET:

Deluxe Search	Super Search
\$19.95	\$39.95
	
Current and previous addresses going back 10 years	Current and previous addresses going back 10 years
Any additional phone numbers available	Any additional phone numbers available
Family members of individual	Family members of individual
Other people at the same address	Other people at the same address
Neighbors with listed phone numbers	Neighbors with listed phone numbers
Spouses (if individual currently lives in Florida or Texas)	Spouses (if individual currently lives in Florida or Texas)

SURVEILLANCE BY PRIVATE SECTOR



Origin
Washington, DC



Destination
Alexandria, VA

Door to Door Directions

From: 1600 Pennsylvania Ave. NW Washington, DC

To: 326 [REDACTED]

Direction	Distance
There are 0.02 miles (0.02 km) between the start of the directions and 1600 Pennsylvania Ave. NW. Use the map above to get to .	
1: Start out going East by turning left.	0.1
2: Turn SLIGHT LEFT onto ALEXANDER HAMILTON PL NW.	0.1
3: Turn RIGHT onto 15TH ST NW.	0.1
4: Turn LEFT onto PENNSYLVANIA AVE NW.	0.1
5: Turn RIGHT onto 14TH ST NW.	0.2
6: 14TH ST NW becomes 14TH ST NW/US-1.	0.6
7: 14TH ST NW/US-1 becomes US-1 S.	0.5
8: US-1 S becomes US-1 S/I-395 S.	0.9
9: Stay straight to go onto I-395 S.	6.5

GOVERNMENT SURVEILLANCE

see www.qn.apc.org/duncan/stoa_cover.htm and www.cfp2000.org

EUROPEAN PARLIAMENT



SCIENTIFIC AND TECHNOLOGICAL OPTIONS ASSESSMENT
STOA

**DEVELOPMENT OF SURVEILLANCE
TECHNOLOGY AND RISK OF ABUSE
OF ECONOMIC INFORMATION**
(an appraisal of technologies for political control)

Part 4/4

The state of the art in Communications Intelligence (COMINT) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to COMINT targeting and selection, including speech recognition

Working document for the STOA Panel

Luxembourg, April 1999 PE 168.184/Part3/4

Directorate General for Research

DA DE EL **EN** ES FR IT NL PT FI SV

Interception Capabilities 2000 - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Fav

Address http://www.ipvreports.mosail.com/interception_capabilities_2000.htm

mySimon Flyswat Off Search! ?



Interception Capabilities 2000

Report to the Director General for Research of the European Parliament
(Scientific and Technical Options Assessment programme office)
on the development of surveillance technology and risk of abuse of economic information.

This study considers the state of the art in Communications Intelligence (Comint) of automated processing for intelligence purposes of intercepted broadband multi-language leased or common carrier systems, and its applicability to Comint targeting and selection, including speech recognition.

[Contents](#) [Summary](#) [Report](#)
[Recommendations](#) [Technical annexes](#) [Notes](#)

Report by : Duncan Campbell, IPTV Ltd
Edinburgh, Scotland April, 1999

Mailto:iptv@pcwcom.net

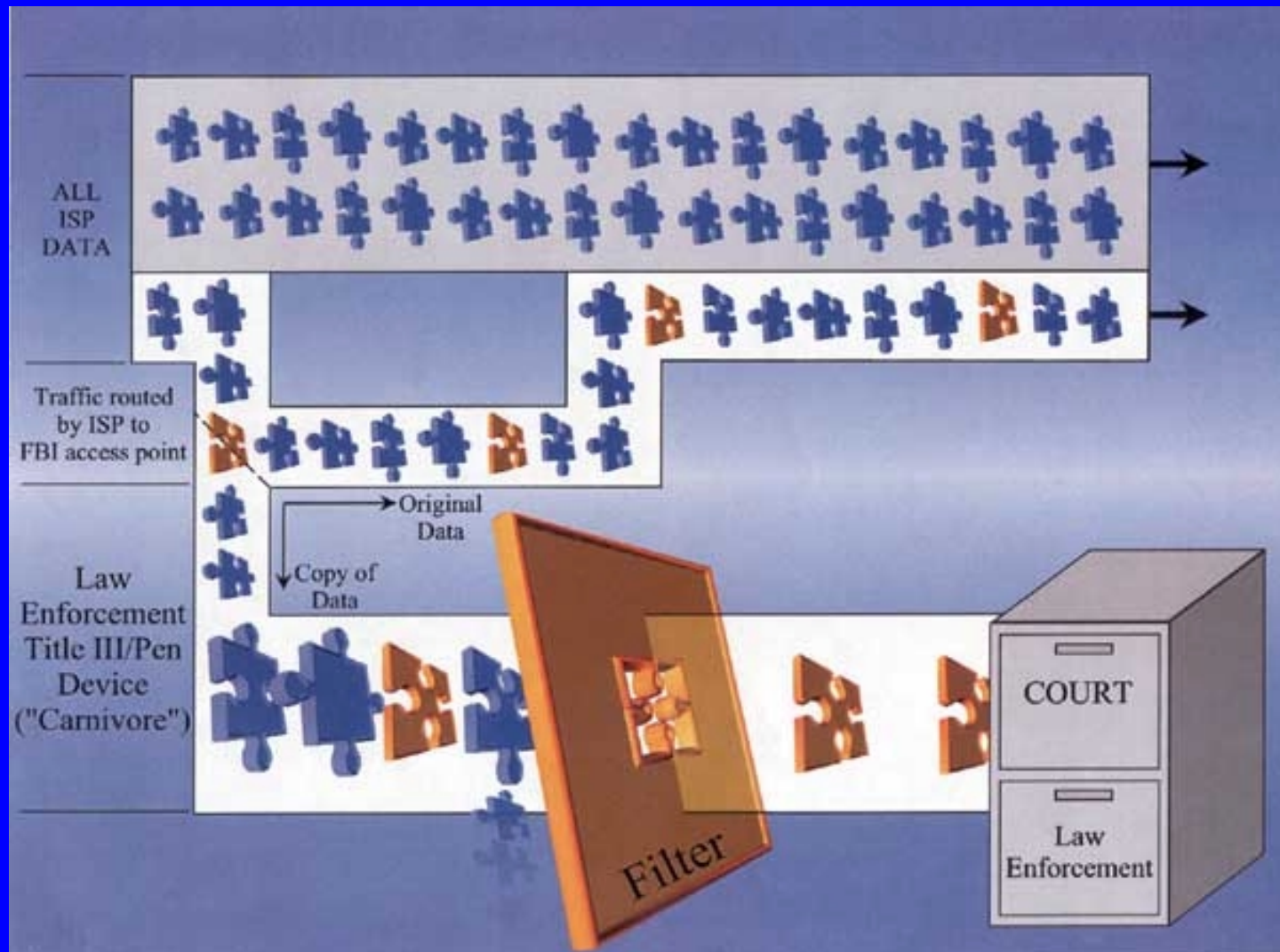
Illustration : 30 metre antennae at the Composite Signals Organisation Station, Morwenstow, England, intercepting communications from Atlantic Ocean and Indian Ocean regional satellites. (D Campbell)

Done

Start ZoneAlarm Address

GOVERNMENT SURVEILLANCE

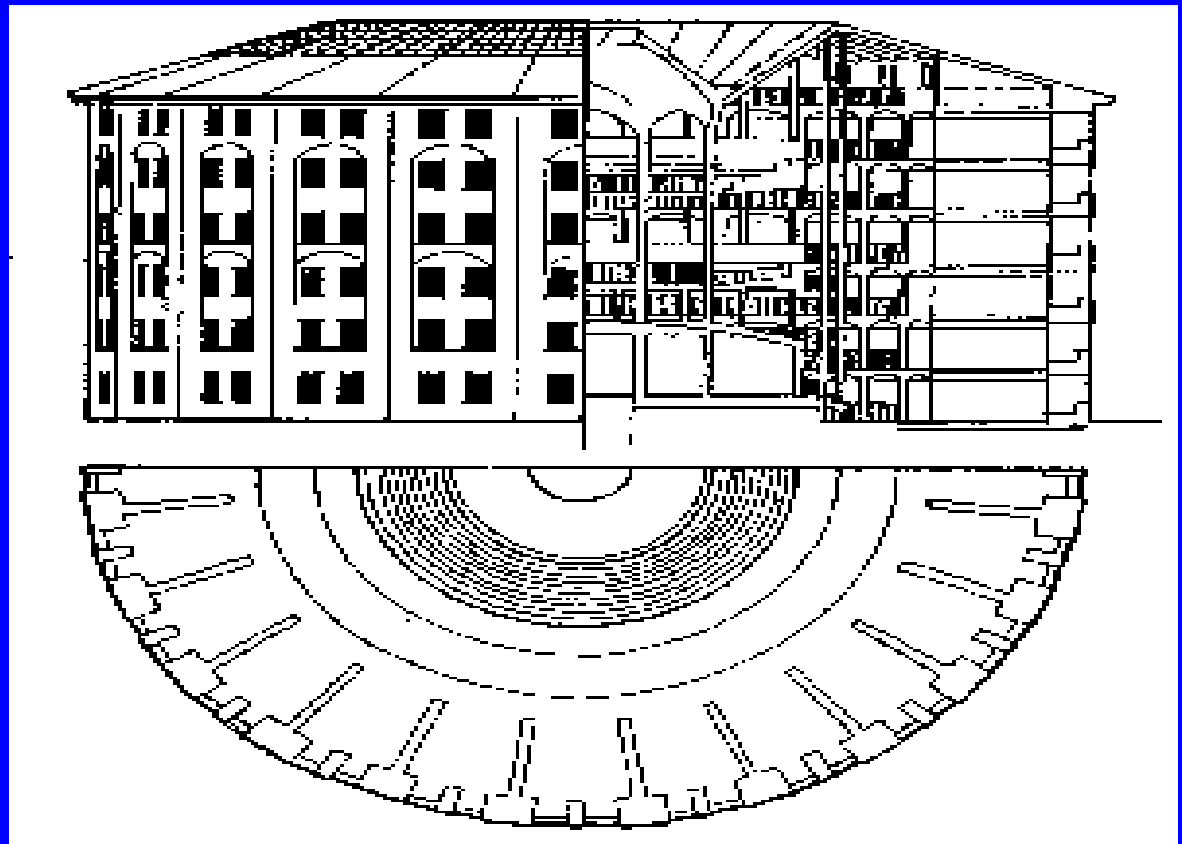
Carnivore: Net-tapping by FBI, 2000



Official FBI figure from <http://www.fbi.gov/programs/carnivore/carnlrgmap.htm>

GOVERNMENT SURVEILLANCE

Not a new idea: Jeremy Bentham argued for control by surveillance in 1791 in his design of the PANOPTICON, where every person in a building is watched from a central tower.



The Panopticon of Jeremy Bentham

From Barton, Ben F. and Marthalee S. Barton. "Modes of Power in Technical and Professional Visuals." *JBTC* 7.1, 1993. 138-62.

Government Surveillance

- When to allow monitoring?
- What safeguards to prevent abuse?

Generic Code of Fair Information Practices

This formulation of a code of fair information practices is derived from several sources, including codes developed by the Department of Health, Education, and Welfare (1973); Organization for Economic Cooperation and Development (1981); and Council of Europe (1981).

1. Openness

no secret databanks on individuals

2. Data subject view and correction

right to see and correct data on self

3. Collection Limitation

limited data collection by lawful means and, where appropriate, with knowledge or consent of data subject

4. Data Quality

only relevant, accurate, complete, and timely data

5. Finality

limits to the uses and disclosure of personal data, used only for purposes specified at time of collection, unless data subject or appropriate authority allows

6. Security

reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure

7. Accountability

record keepers accountable for complying with fair information practices

See <http://www.cdt.org/privacy/guide/basic/generic.html> for more detail.

Government responsibilities

Managing Intellectual Property Regime

Is “Copy” Still the Right Concept?

- Should access to data be controlled? Start from the basics: progress via incentive. Does a use impact incentive? Why did the current intellectual property regime come about? Is it still useful? What can be done to have it work in the digital age?
- **Can access to digital information be controlled?**
 - The DVD story – as told by a defiant Carnegie Mellon University professor: <http://www.cs.cmu.edu/~dst/DeCSS/>
 - Points to descrambling algorithm (in violation of 17 USC 1201(a)(2) ?), code on T-shirt, software code, Power Point slides on Content Scrambling System (CSS), algorithm in haiku by an anonymous poet
 - DVD/DeCSS FAQ from the Motion Picture Association of America point of view is at <http://www.mpaa.org/Press>
- **Good references on the current intellectual property regime:**
 1. National Research Council, *The Digital Dilemma: Intellectual Property in the Information Age*, http://books.nap.edu/html/digital_dilemma/
 2. *Digital Copyright* by Jessica Litman, Prometheus Books 2001, www.digital-copyright.com

Napster file sharing

The screenshot displays the Napster v2.0 BETA 9 application window. The interface includes a menu bar (File, View, Actions, Help) and a toolbar with buttons for Home, Chat, My Files, Search, Hot List, Transfer, Discover, and Help. A status bar at the top right indicates "Shop for music at CDNOW".

The main window is divided into two sections: Inbound Transfers and Outbound Transfers.

Inbound Transfers:

Filename	File Size	User	Status	Speed	Progress	Rate	Time Left
Brittany Spears - (I can't get no) Satisfaction.mp3	6,366,548	NE694Goey	File Complete!				
Heart of Oak, Rule Britannia - HM Royal Marines Band.mp3	1,464,424 of 3,477,632	Khaki1040	Downloading...	Cable	2%	5.86 k/s	00:05:43
Anthem - Italian National Anthem - (Inno di Mameli) - ESB.MP3	1,362,094	ScottSchaffer	File Complete!				

Outbound Transfers:

Filename	File Size	User	Status	Speed	Progress	Rate	Time Left
MormonTabernacleChoir-Battle_Hymn_of_the_Republic.mp3	5,695,779	sandraphelps	File Complete!				
(The Beatles)-Rock And Roll Music.mp3	2,394,240	djazzryick	Transfer Error				

The left sidebar shows a file tree with folders like "My Files\Brittany Spears" and "Music\Brittany Spears". The bottom status bar indicates "Online (pittsburghboy): Sharing 280 files." and "Currently 11,751 users sharing 2,322,105 files (9,876 gigs)".

Search Results:

Freq	Length	User	Connection	Ping
44100	3:23	cajbw2...	Unknown	91
44100	3:23	luvdala...	Unknown	117
44100	3:21	luvdala...	Unknown	117
44100	3:31	MasterC...	Cable	144
44100	4:25	NE694...	Cable	262
44100	3:37	NE694...	Cable	262
44100	3:27	nappyh...	Cable	345
44100	3:22	bubba3t...	56K	361
44100	3:23	bubba3t...	56K	361
44100	3:33	Slimsha...	Cable	366
44100	3:24	texaste...	Cable	378
44100	3:27	laryan02	Unknown	378
44100	3:33	laryan02	Unknown	378
44100	3:33	playboy...	Unknown	389
44100	4:06	teriske...	56K	391
44100	3:33	FroggyA...	14.4	394
44100	3:27	Golden...	Cable	397
44100	3:23	tesa62	56K	406
44100	2:48	folts23	Unknown	430
44100	4:15	folts23	Unknown	430
44100	0:51	folts23	Unknown	430
44100	3:27	snorting...	56K	518
44100	4:02	killwoody	Unknown	526
44100	3:07	Luigi19...	56K	529
44100	1:49	violet_10	T1	546
44100	3:23	Toonaoot	Unknown	555
44100	1:56	derivicus	ISDN-128K	556
44100	3:27	Spearin...	56K	556
44100	3:19	tammykj	56K	574
44100	3:21	tammykj	56K	574
44100	4:06	Katherin...	Cable	578
44100	5:10	Katherin...	Cable	578
44100	3:27	c-roc-a-f...	Unknown	583
44100	3:23	princess...	Unknown	596
44100	3:27	blakemi...	56K	601
44100	3:23	blakemi...	56K	601
44100	3:33	aLBIND...	Cable	678

The bottom status bar indicates "Online (pittsburghboy): Sharing 278 files." and "Currently 11,899 users sharing 2,342,222 files (9,970 gigs)".

Napster, Jefferson's Moose, and the Law of Cyberspace

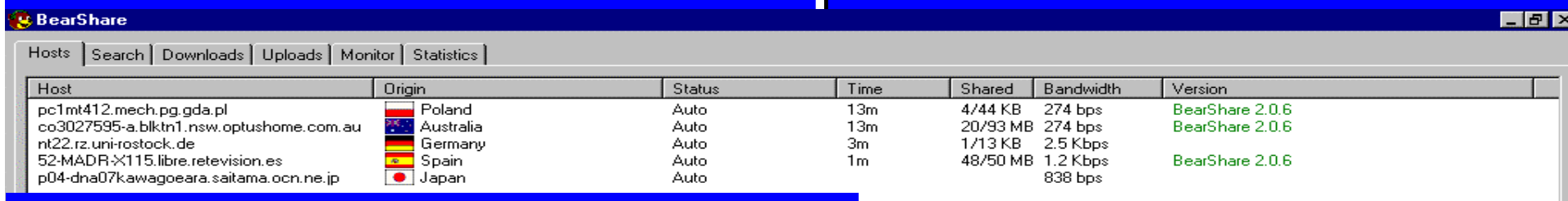
David G. Post, June 8, 2000

www.temple.edu/lawschool/dpost/Napster.html

- But that takes property created *here* and brings it *there*.
Is that sharing or smuggling?
- Does copyright law protect this? Should it? Who decides?
Why?
- Is Cyberspace a *new* place? Is there a *here* and a *there*?
- Jefferson would not ask if Napster infringes Sec. 512 of US Copyright Act, but whether and how it opens new possibilities.

Peer-to-Peer Won't Go Away!

This is NOT Napster:



The screenshot shows the BearShare application window with a menu bar (Hosts, Search, Downloads, Uploads, Monitor, Statistics) and a table of hosts. The table has columns for Host, Origin, Status, Time, Shared, Bandwidth, and Version.

Host	Origin	Status	Time	Shared	Bandwidth	Version
pc1mt412.mech.pg.gda.pl	Poland	Auto	13m	4/44 KB	274 bps	BearShare 2.0.6
co3027595-a.blktn1.nsw.optushome.com.au	Australia	Auto	13m	20/93 MB	274 bps	BearShare 2.0.6
nt22.rz.uni-rostock.de	Germany	Auto	3m	1/13 KB	2.5 Kbps	
52-MADR-X115.libre.retevision.es	Spain	Auto	1m	48/50 MB	1.2 Kbps	BearShare 2.0.6
p04-dna07kawagoeara.saitama.ocn.ne.jp	Japan	Auto			838 bps	

•How about Napsters for

- poetry?
- Real estate listings?
- Articles about law and cyberspace?
- Government efficiency and effectiveness tips?
- information about genetic sequences
- making up the human genome?

“Despite Napster's demise, P2P's legal struggle lives on -- certain to battle RIAA further in the coming months, as the industry continues to wage a war to cripple the technology it cannot control and attempts to wrestle music distribution away from the people at the expense of freedom of speech and innovation.” – Robin Gross, EFF Staff Attorney, March 5, 2001,
<http://www.eff.org/effector/HTML/effect14.04.html>

- Publius, a censorship resistant, tamper evident, WWW-based publishing system, already exists (see www.cs.nyu.edu/~waldman/publius.html).
- Each server can't tell type of content it is hosting, and any
- modification can be detected.



Recommendations for Policymakers

National Research Council, The Digital Dilemma: Intellectual Property in the Information Age,
http://books.nap.edu/html/digital_dilemma/

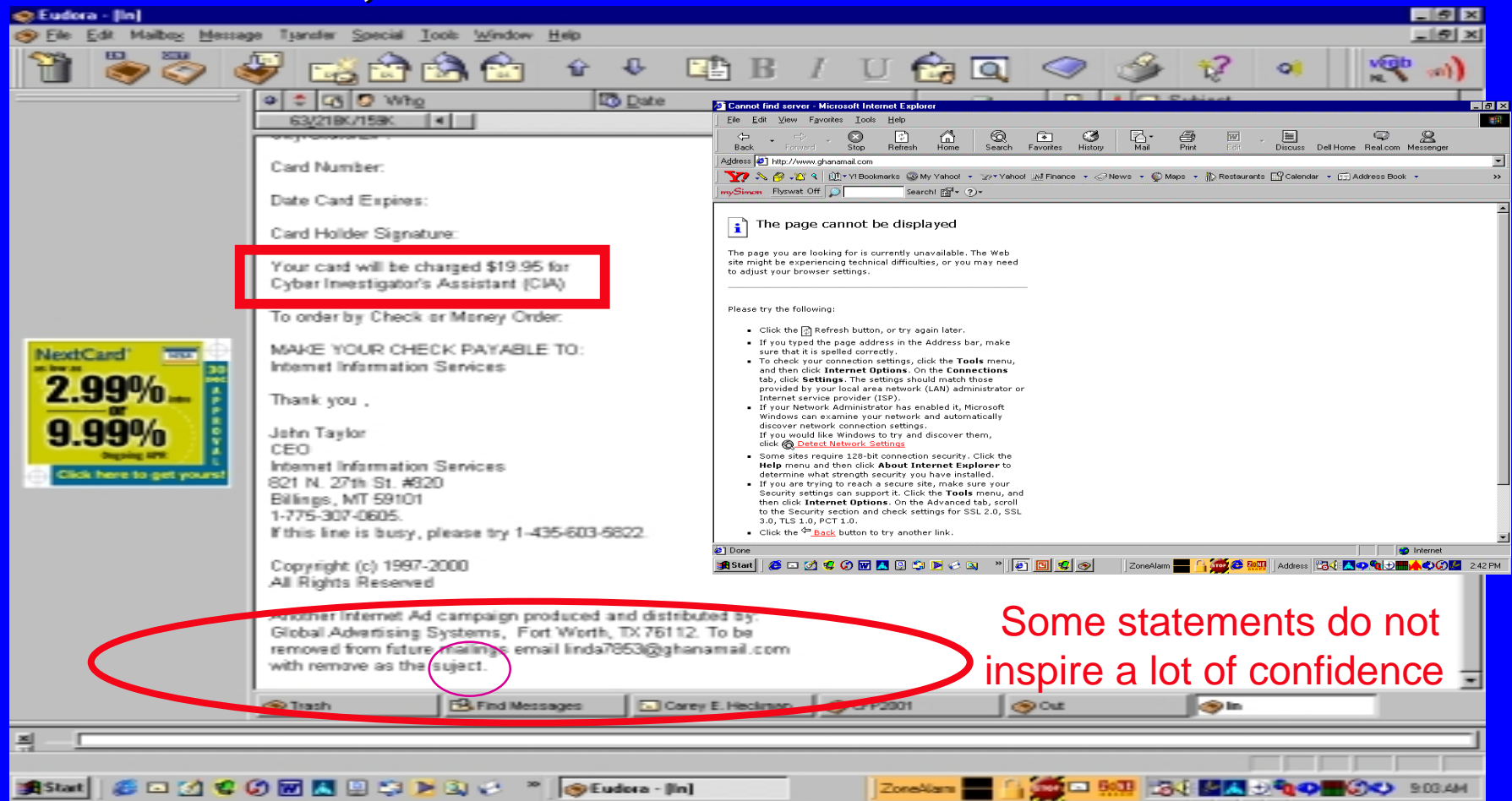
- Aim for technology independence
- Keep it simple
- Keep it flexible
- Keep cool

Freedom of speech

Content control and access

- When is speech “chilled”?
- Traditional areas of controversial or forbidden speech
 - Sedition
 - Pornography
- Censorship vs. User Choice
 - Communications Decency Act and relatives
 - German anti-Nazi provisions
 - French terroristic provision
 - Technological disclosure controls
- Commercial speech and advertising get same protections? Spam?

TRUST ME, I WILL TAKE YOU OFF THE SPAM LIST



- See www.junkbusters.com for anti-spam tools.
- Monitor www.cdt.org and www.epic.org for more information on (U.S.) legislation.
- And what about wireless and location-based spam?

HATE SPEECH SITES

White Aryan Resistance - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit Discuss Dell Home Real.com Messenger

Address <http://www.resist.com/>

Y! Y! Bookmarks My Yahoo! Yahoo! Finance News Maps Restaurants Calendar Address Book

mySimon Flyswat Off Search!

White Aryan Resistance

Racist Cartoons

Nigger	Spic	Jew
Whigger	Heterophobes	Anti-Government
Nigger Defendant	Bad Jew	What's On the Mind
Sink The Boat	NiggerBall	America On A Platter
Aryan Might	Proud Aryan	We're Surrounded
Don't Get Screwed	Alien meet Negro	American Dream
Agitate	Who is behind this?	Who writes this stuff?
Too much Black Crime	Giddy Up Jewboy	Fight Back
Tinted Windows	Jews Bug Me	

Subscribe
Tom Metzger
Aryan Update
Don't Talk
Our Positions
Racist Cartoons
Merchandise
Contact Info
E-Mail
HOME

P.O. BOX 65
Fallbrook, CA 92088
(760) 723-8996

Start ZoneAlarm Address 6:26 AM

TECHNOLOGICAL DISCLOSURE CONTROLS

PICS: Platform for Internet Content Selection

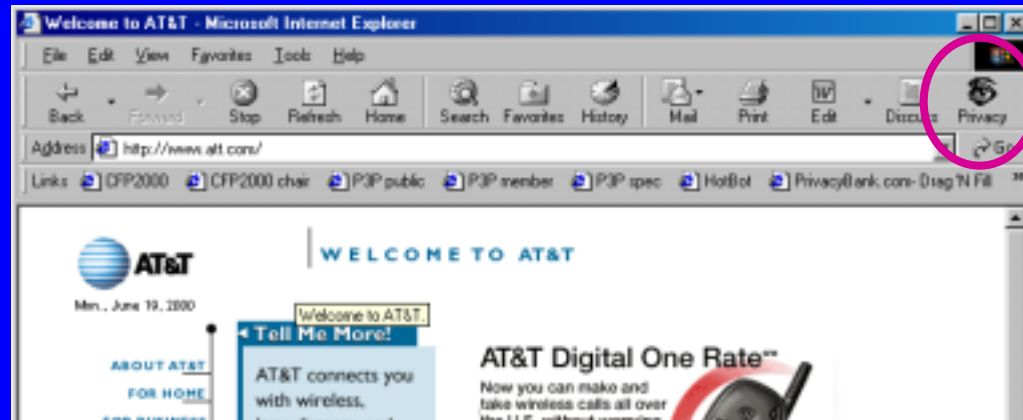
RSACi Content Advisory Levels

LEVEL 0	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4
	VIOLENCE: content may include			
Harmless conflict; some damage to objects	Creatures injured or killed; damage to objects;fighting	Humans injured or killed with small amt of blood	Humans injured or killed; blood and gore	Wanton and gratuitous violence; torture; rape
	NUDITY: content may include			
No nudity or revealing attire	Revealing attire	Partial nudity	Non-sexual frontal nudity	Provocative frontal nudity
	SEX: content may include			
Romance; no sex	Passionate kissing	Clothed sexual touching	Non-explicit sexual activity	Explicit sexual activity; sex crimes
	LANGUAGE: content may include			
Inoffensive slang; no profanity	Mild expletives	Expletives; non- sexual anatomical references	Strong, vulgar, or hate language; obscene gestures	Crude, explicit sexual references; extreme hate language

RDF: Resource Description Framework; P3P: based on RDF
More info at <http://www.w3.org/?> where ?=PICS, RDF, or P3P

P3P informs Web surfers

(will be in Microsoft Internet Explorer 6.0)



privacy
manager
button



Government responsibilities

Facilitating Computer System Security

Security Controls Should Maintain CIA (Confidentiality, Integrity, Availability)

SOME TYPICAL SECURITY MECHANISMS

- Authentication
 - Something you know (examples: password, encryption key)
 - Something you have (examples: token, capability)
 - Something you are (picture, fingerprint)
- Cryptography (Example [very simple]: `lwdoa` → ?)
 - Traditional, single key (DES, PGP, AES)
 - Public key (two keys, public and private: RSA)
 - Digital signatures
- Risk Analysis
 - Expected value
 - Worst case
 - Insurance

Security Controls Should Maintain CIA (Confidentiality, Integrity, Availability)

SOME TYPICAL SECURITY MECHANISMS

- Authentication
 - Something you know (examples: password, encryption key)
 - Something you have (examples: token, capability)
 - Something you are (picture, fingerprint)
- Cryptography (Example [very simple]: **lwdoa** → **ITALY**)
 - Traditional, single key (DES, PGP, AES)
 - Public key (two keys, public and private: RSA)
 - Digital signatures
- Risk Analysis
 - Expected value
 - Worst case
 - Insurance

Internet Worm (Nov 1988) shut down 6,000 machines

MALWARE GENERATORS

Vbs Worms Generator (Vbswg) 1.50b - [K]Alamar

Options

Worm name:

Your name:

Worm backup

Copy worm to:

File name:

Leave the .vbs at the end.

Random words lenght:

Replication

Fast acces

<input checked="" type="checkbox"/> Outlook Atta.	<input type="checkbox"/> Outlook Msg	<input checked="" type="checkbox"/> Mirc	<input checked="" type="checkbox"/> Pirch
<input checked="" type="checkbox"/> Start with Win.	<input checked="" type="checkbox"/> Infect files	<input type="checkbox"/> Search Mirc	<input type="checkbox"/> Search Pirch
<input type="checkbox"/> Show Msg	<input type="checkbox"/> Goto Url	<input type="checkbox"/> Crash system	<input type="checkbox"/> Crash system 2
<input checked="" type="checkbox"/> Anti Deletion	<input type="checkbox"/> Crypt code	<input type="checkbox"/> Download and run file	

Payloads

Payloads

☒ Use payloads

Show a message

☒ Message:

☐ Picture:

Goto url

☐ Url:

Crash system

☐ Creates 1Mb variables till system crash.

Crash system 2


☐ Run notepads until system crash

When?

Month: Day:

Love Bug (May 2000) infected 15,000,000 machines

Zapatistas revolutionary website



Ejército Zapatista de Liberación Nacional

Año 18 de la lucha y octavo de la guerra contra el olvido y la mentira

¡Ya Basta! ha recibido más de 1,000,000 de visitas.

Contenidos

- ★ **Comunicados**
Última revisión: 03/feb/2001
- ★ **Noticias**
Última revisión: 31/ene/2001
- ★ **Derechos indígenas y los Acuerdos de San Andrés**
- ★ **Municipios autónomos**
- ★ **Mapas y miscelánea**

Con el EZLN al DF

En una conferencia de prensa, el 2 de diciembre de 2000, el EZLN fijó su posición en torno al nuevo gobierno federal encabezado por Vicente Fox y fijó **3 condiciones para regresar a la mesa del diálogo**: el cumplimiento de los Acuerdos de San Andrés, la liberación de todos los zapatistas presos y el retiro del ejército de 7 de las 259 posiciones que ocupa en Chiapas.

Los zapatistas viajarán en febrero de 2001 a la capital de México para argumentar, frente al Congreso de la Unión, la iniciativa de reformas constitucionales en materia de derechos y Cocopa.

Comunicados recientes:

- "México 2000: ventanas abiertas, puertas por abrir." (02/dic/2000) [español](#), [portugués](#)
- Carta a Vicente Fox. (02/dic/2000) [español](#), [English](#), [portugués](#), [français](#)
- Comunicado sobre el posible reinicio del diálogo. (02/dic/2000) [español](#), [English](#), [portugués](#)

alta vista:
Home | Media/Topic Search | Email & Tools

World: translation

BABEL FISH
Click the "World Keyboard" link for a convenient method of entering accented or Russian characters.
Use the new **Racing Babel Fish** to print your translations.
Download **SYSTRAN Personal** and translate your private documents in seconds.
Questions? Check out our [FAQs](#).
Like this new version? Send us your [comments](#).

Translate Anything
Powered by **SYSTRAN technologies**

In English:

With the EZLN to the DF In a press conference, the 2 of December of 2000, the EZLN fixed their position around the new federal government headed by Vicente Fox and fixed 3 conditions to return to the table of the dialogue: the fulfillment in the Agreements of San Andrés, the liberation of all the imprisoned zapatistas and the retirement of the army of 7 of the 259 positions that occupy in Chiapas. The zapatistas will travel in February of 2001 to the capital of Mexico to argue, in front of the Congress of the Union, the initiative of constitutional reforms in the matter of rights and indigenous culture presented/displayed by Cocopa. Recent official notices: " Mexico 2000: opened windows, doors to open. " (02/dic/2000) Spanish, português Letter to Vicente Fox. (02/dic/2000) Spanish, English, português, français Communicated on the possible resumption of the dialogue. (02/dic/2000) Spanish, English, português, français Communicated on the trip of 23 commanders and Subcomandante Marcos to the Federal District. (02/dic/2000) Spanish, English, Português Communicated on the establishment of the Information center Zapatista. (03/ene/2001) Spanish, português important Data on the trip of the EZLN to the D.F. (06/ene/2001) Spanish, português Letter on mail and the page Web (12/ene/2001) Spanish Publication of the route and itinerary for the trip to the D.F. (24/ene/2001) Spanish Of senders and addressees. (24/ene/2001) Spanish Clarifying to doubts on the march to the DF and the three conditions for the dialogue. (27/ene/2001) Spanish The EZLN, through the new Information center Zapatista, makes a call to national and international solidarity so that they support economically this initiative of peace depositing any contribution in the following banking account: BANCOMER. Plaza 437. Number -5001060-5, (five, zero, zero, one, zero, six, zero, script, five) To name of Mrs. Maria de Rosario Ibarra. San Cristóbal of

Start

ZoneAlarm

Address

8:00 PM

Government responsibilities

Protecting Critical Infrastructure

Critical Infrastructure Sectors

(President's Commission on Critical Infrastructure Protection)

- Information and communications
- Physical distribution
- Energy
- Banking and finance
- Vital human services

Critical Infrastructure Sectors

(President's Commission on Critical Infrastructure Protection)

- Information and communications
 - Local and long-distance telephone carriers
 - Cellular networks
 - Satellite services
 - Internet
 - Computers used for home, commercial, academic, and government use
- Physical distribution
- Energy
- Banking and finance
- Vital human services

Examples of Attacks

- Information and Communications
 - Distributed Denial of Service attacks on major Internet sites
- Physical
 - Disrupting air traffic control systems
 - Japanese subway system
- Energy
 - Computer access to power grid (service people dial in from home modem)
 - Oil pipelines run through countries (in Middle East) (what if countries are fighting?)
- Banking and Finance
 - Money laundering
 - Malicious code that reroutes money into a specific account
- Vital human services
 - Water disputes
 - Attacks on treatment plants
 - Rerouting emergency (911) calls to locations across country
 - Changes to hospital records

CONTROL MECHANISMS

www.ciao.gov

- Entitywide security: Plan for emergencies, create security procedures
- Access controls to critical information, systems, and people
- Segregation of duties: no single person has control over all essential information or operations
- Continuity: have plans to restore service and to not lose critical information
- Change control and life cycle management: be able to make changes without significant service interruptions
- System software controls: critical software only can be accessed by certain people and their uses should be monitored and logged.

A number of excellent presentations on this are at
<http://www.ciao.gov/Audit/SummitLibrary/SummitLibrary.htm>

Critical Infrastructure Protection: National Plan for Information System Protection

U. S. General Accounting Office Report AIMD-00-90R

Latest: http://146.145.203.59/CIAO_Document_Library/2001CongReptSummary2.htm, February 2001

- Prepare and Prevent
 - 1 Identify Assets and Shared Interdependencies and Address Vulnerabilities
- Detect and Respond
 - 2 Detect attacks and unauthorized intrusions
 - 3 Develop robust intelligence and law enforcement capabilities to protect critical infrastructure systems, consistent with the law
 - 4 Share attack warnings and information in a timely manner
 - 5 Create capabilities for response, reconstitution, and recovery

Critical Infrastructure Protection: National Plan for Information System Protection

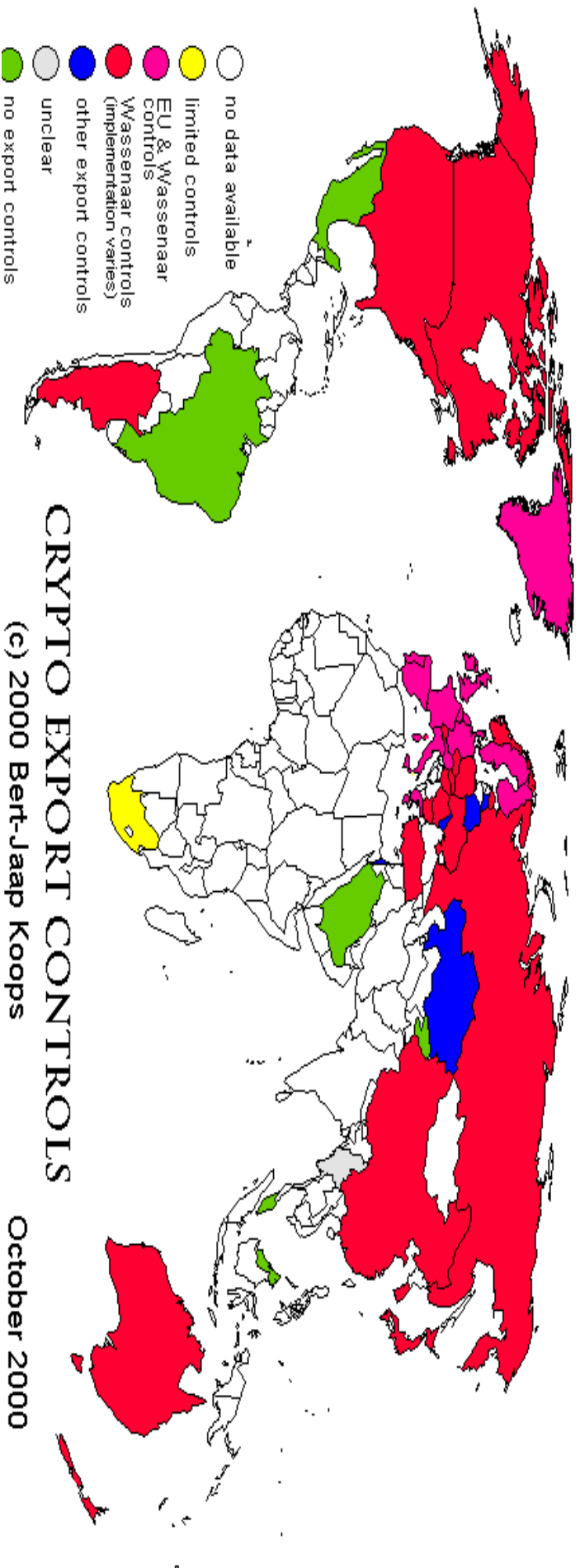
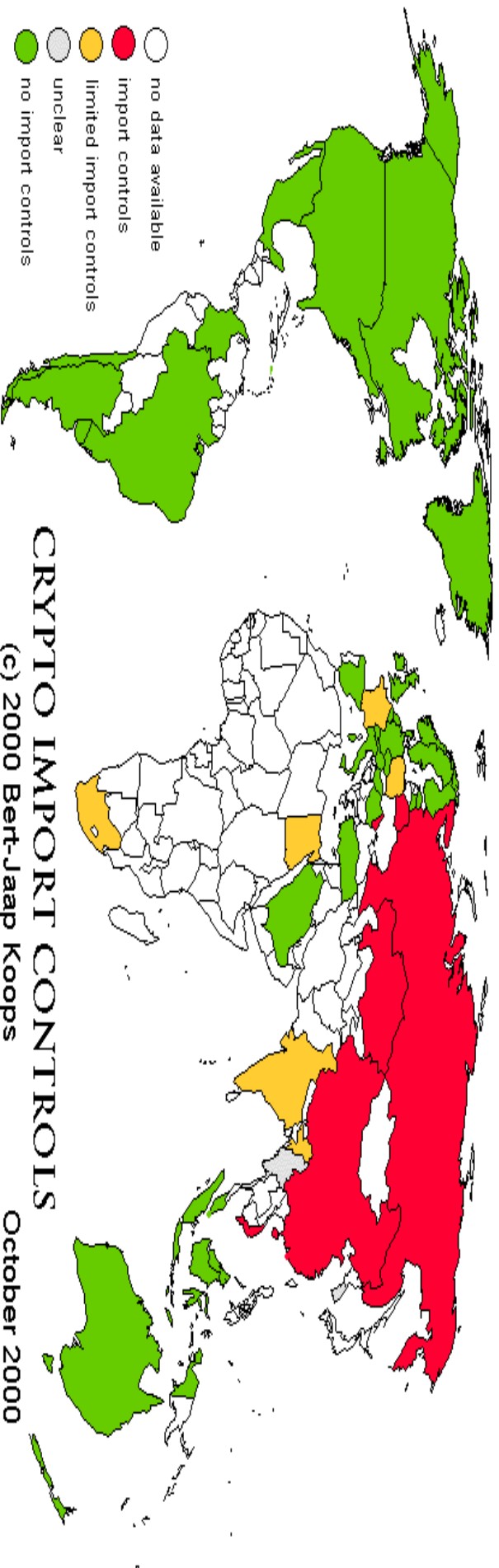
U. S. General Accounting Office Report AIMD-00-90R

Latest: http://146.145.203.59/CIAO_Document_Library/2001CongReptSummary2.htm, February 2001

- Build Strong Foundations
 - 6 Enhance research and development to support 1-5
 - 7 Train adequate numbers of Infosec specialists
 - 8 Outreach/Awareness of Improved Cybersecurity
 - 9 Legislation and funding supporting 1-8
 - 10 “In every step and component of the plan, ensure the full protection of American citizens’ civil liberties, their rights to privacy, and their rights to the protection of proprietary data”

Government responsibilities

Recognizing Limits of Regulation



Example of the Limits of Regulation: Non-U. S. Crypto Products (Dec 2000)

835 products from 39 countries

491 non-US 379 US crypto companies produce and distribute in 76 countries

<http://www.pgp.com/research/nailabs/cryptographic/cryptographic-products.asp>

See also Steven Levy, *Crypto*, Viking, 2001.

Crypto Survey 2-22-01.pdf



NAI Labs Advanced Research



PROJECT PROFILE

Worldwide Survey of Cryptographic Products

Summary

Cryptography plays an essential role in protecting information systems throughout the world. The availability of cryptographic products within and outside the United States impacts global deployment, interoperability, and export controls.

In order to determine how widespread cryptography is throughout the world, NAI Labs, The Security Research Division of Network Associates (formerly Trusted Information Systems (TIS)) has been conducting a survey of domestic and foreign products that employ cryptography. We have assembled a unique, comprehensive database with, where possible, verification of product availability.

Originally commissioned by the Software Publisher's Association (SPA) in May 1993 and conducted in cooperation with Dr. Lance Hoffman and students at the George Washington University, we have been conducting the survey for over seven years. We continue to learn information about cryptographic products on a daily basis, and we periodically release summary information.

As of December 2000, we have identified a worldwide total of 1238 cryptographic products. We've obtained numerous products and are examining them to assess their functionality and security. On average, the quality of foreign and U.S. products is comparable. Both foreign and U.S. manufacturers vie to have products that meet accepted worldwide standards, including IPsec, SSL/TLS, SSH, S/MIME, and OpenPGP. A number of the top foreign products are quite competitive in strength, standards compliance, and functionality.

U.S. export controls have been modified recently to allow export of strong commercial cryptography. International customers who need cryptographic security for their sensitive information can now turn to both U.S. sources as well as foreign sources to fulfill that need.

Our survey results show continued growth and expanded development of strong, standards-compliant cryptographic products throughout the world. Internet communications-related cryptographic products are experiencing high growth, especially IPsec, VPN, and secure e-mail products.

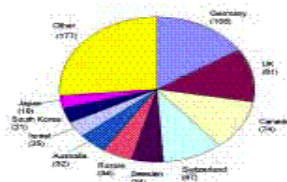
Crypto Survey Results

(As of December 2000)

FOREIGN PRODUCTS: We identified 835 cryptographic products developed in 39 countries outside the United States:

Australia	Austria	Belgium
Canada	China	Costa Rica
Czech Republic	Denmark	Egypt
Finland	France	Estonia
Greece	Hong Kong	Germany
India	Iran	Iceland
Isle of Man	Israel	Ireland
Japan	Mexico	Italy
New Zealand	Norway	Netherlands
Portugal	Romania	Poland
South Africa	South Korea	Russia
Sweden	Switzerland	Spain
United Kingdom	Uzbekistan	Turkey

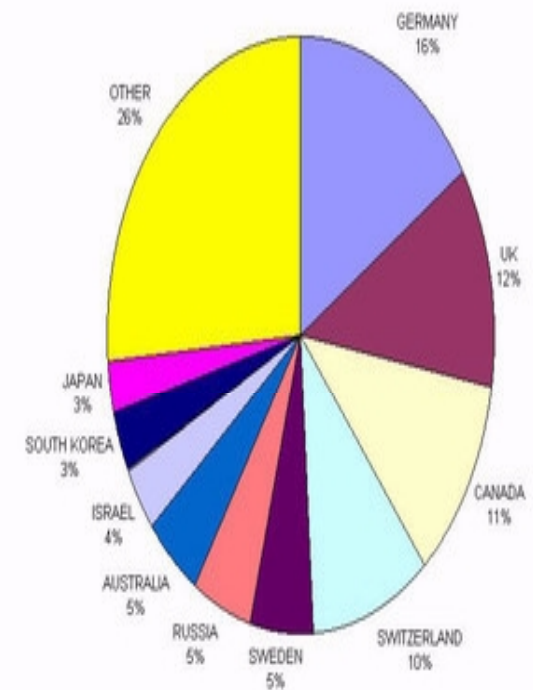
The most foreign cryptographic products are produced in Germany, followed by the United Kingdom, Canada, Switzerland, Sweden, Russia, Australia, Israel, South Korea, and Japan.



At least 259 of these foreign cryptographic products implement "strong" cryptographic algorithms, including Triple DES, IDEA, BLOWFISH, RC5, or CAST.

DOMESTIC PRODUCTS: We identified 568 cryptographic products developed in the United States, 201 that implement "strong" cryptographic algorithms.

TOTAL PRODUCTS: Worldwide total of 1238 cryptographic products produced and distributed by 870



8.5 x 11 in

Government Responsibilities



Donley's Wild West Town

From the “Law of the Net” (above) to
Developing consistent regulatory
framework that can be harmonized with
other governments’




Other New Technologies Government Has Dealt With

- Air Traffic Control
 - safety, security, convenience, commerce
- Telephones
 - universal service, interoperability
- Broadcast Television
 - free speech, commercial speech, appropriate content
- Internet
 - all of the above: security, convenience, commerce, universal service, interoperability, free speech, commercial speech, appropriate content

**Internet Presents Similar Opportunities
to Strike Balance for the Public Interest,
and Government has the Responsibility to do this**

Advisory Committee on Online Access and Security

The Federal Trade Commission has established an Advisory Committee on Online Access and Security. The purpose of the Advisory Committee is to provide advice and recommendations to the Commission regarding implementation of certain fair information practices by domestic commercial Web sites. In particular, the Advisory Committee will address providing online consumers reasonable access to personal information collected from and about them and maintaining adequate security for that information.

- **Public Comments**
 - [How to Submit a Comment](#)
- *Subgroup Option Papers*
 - **Access Issues**
 - Degree of Access, and Terms and Conditions of Access
 - The Entities Covered and the Ability to Correct or Edit the Data
 - [Authentication and Technology Issues](#)
 - [Options Paper](#) [PDF 101K] 
 - [Theme Piece](#)
 - **Security Issues**
 - [A Continuum of Security Options](#)
- **March 31st Meeting of the Advisory Committee**
 - [Agenda](#) of the Meeting
 - *Federal Register* [Notice](#) Announcing the Meeting (03/16/00) [PDF 117K] 
- *Preliminary Draft Outlines of Subgroups*
 - **Access Issues**
 - [Scope and Categories Subgroup Draft Outline](#)
 - [Entities Subgroup Draft Outline](#) [PDF 15K] 

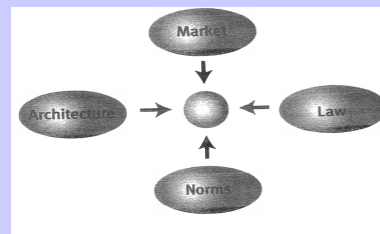
Three Mistakes About Regulation

Prof. Larry Lessig, Stanford Law School

- “The Net cannot be regulated.”
- “The Net was born without regulation.”
- “The Net is not now being regulated.”

REGULATION

Lessig, L., *Code and Other Laws of Cyberspace*, Basic Books, 1999



Architecture, law, market, norms

FIVE CHALLENGES FOR REGULATING THE GLOBAL INFORMATION SOCIETY

Prof. Pamela Samuelson

from Chris Marsden, ed., *Regulating the Global Information Society*, 2000
downloadable from <http://www.sims.berkeley.edu/~pam/papers.html>

1. Can existing laws and policies be applied, or are new laws or policies needed to regulate Internet conduct?
2. How can reasonable and proportional responses can be formulated when new regulations are needed?
3. How can flexible enough laws be crafted to adapt to rapidly changing circumstances?
4. How can fundamental human values be preserved in the face of economic or technological pressures tending to undermine them?
5. How can governments coordinate in Internet law and policy making so that there is a consistent legal environment on a global basis?