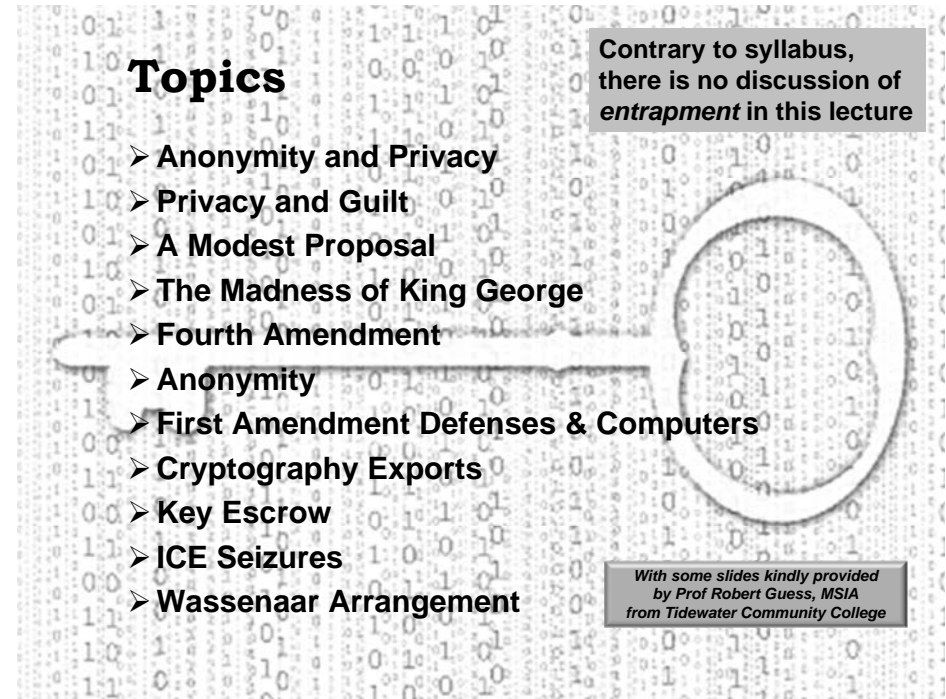


First Amendment Issues: Anonymity & Encryption

CJ341 – Cyberlaw & Cybercrime Lecture #26

M. E. Kabay, PhD, CISSP-ISSMP
<mailto:mekabay@gmail.com>
 V: 802.479.7937

Assoc Prof Information Assurance
 School of Business & Management



Contrary to syllabus, there is no discussion of *entrapment* in this lecture

Topics

- Anonymity and Privacy
- Privacy and Guilt
- A Modest Proposal
- The Madness of King George
- Fourth Amendment
- Anonymity
- First Amendment Defenses & Computers
- Cryptography Exports
- Key Escrow
- ICE Seizures
- Wassenaar Arrangement

With some slides kindly provided by Prof Robert Guess, MSIA from Tidewater Community College

Anonymity and Privacy



- Sun CEO Scott McNeely caused a furor when he stated “You have zero privacy anyway. Get over it .”
- 25 Million Surveillance Cameras are in use worldwide.
- Houston Chief of Police Harold Hurtt
 - ❑ Called for placing surveillance cameras in public areas and private homes
 - ❑ He said “I know a lot of people are concerned about Big Brother, but my response to that is, if you are not doing anything wrong, why should you worry about it?”

CLASS DISCUSSION:

- How would you answer that?

Used by gracious permission of Prof Robert Guess, MSIA
 Tidewater Community College

On Privacy and Guilt

- The issue is not whether someone *desiring* privacy has done anything wrong:
- The issue is whether those *invading* privacy are doing something wrong.
 - ❑ FBI Director J. Edgar Hoover detested civil rights workers and ordered 24-hour surveillance at taxpayer expense based entirely on his dislike of their politics *
 - ❑ President Richard M. Nixon ordered illegal surveillance of his political “enemies” by the FBI and the Secret Service at taxpayer expense



* <http://www.icdc.com/~paulwolf/cointelpro/churchfinalreportlllb.htm>

** <http://watergate.info/impeachment/impeachment-articles.shtml>

A Modest Proposal

- One possible answer to the privacy dilemma:
 - ❑ Eliminate privacy (governmental, corporate, and individual) and
 - ❑ Create a *completely open society*
- Criminal hackers chant “Information Wants to be Free” (well, for everyone *else’s* information)
- Everyone should know everything about everyone



CLASS DISCUSSION:

- *Is that a wise course of action?*
- *Imagine the consequences*

Used by gracious permission of Prof Robert Guess, MSIA Tidewater Community College

5

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

The Madness of King George

- American Colonists engaged in barter and trade to avoid paying taxes to the Crown
- In response, King George III issued “Writs of Assistance” to Colonial Governors
- This power was *widely abused* for wholesale arrests, searches, and seizures
- The founders of the United States of America deliberately decided to *include constitutional protection* from such governmental abuse



Used by gracious permission of Prof Robert Guess, MSIA Tidewater Community College

6

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

The Fourth Amendment to the US Constitution (again)

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.



7

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Anonymity

- Major challenges to criminal law
 - ❑ Ability to exist *anonymously* in cyberspace
 - ❑ Identity & *pseudonymity*
 - ✓ Are these people really who they claim to be?
 - ❑ Technology
 - ✓ E.g., anonymous remailers
 - ✓ Ability of LE/legislators/gov’t/attorneys to keep pace with technology



8

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

Ban Anonymity?

- Would a ban on Internet anonymity reduce crime?
- See <http://www.p2pnet.net/story/10336>
 - ❑ Brazilian politician called for ban on anonymity in 2006
 - ❑ His proposed bill, if made into law, would have made it a crime for *anyone to anonymously send an email, join a chat, write a blog, download content, disseminate virus or Trojans, and access banks or networks without proper authorization*
- Do you think this is a good idea for citizens of
 - ❑ China?
 - ❑ the USA?

Why or why not?



Circumventing Anonymity

- Users are not always as “anonymous” as they think
 - ❑ Social network users sometimes believe they are in a private space
 - ✓ Reveal confidential information
 - ✓ Show pictures of crimes (e.g., underage drinking of alcohol, consumption illegal drugs)
 - ✓ Attack others in cyberbullying
 - ❑ But most social networks allow open access
 - ✓ School administrators
 - ✓ Potential employers
- Technology
 - ❑ Tracking programs
 - ❑ Forensic tools

Interesting article (April 2008):
<http://tinyurl.com/5q6xox>



First Amendment Defenses & Computers

- First Amendment of US Constitution (again)

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.

- Citing 1st Amendment principles, attorneys have tried to argue that certain computer-related activities are *protected*
 - ❑ Computer programs in general
 - ❑ Viruses
 - ❑ Encryption

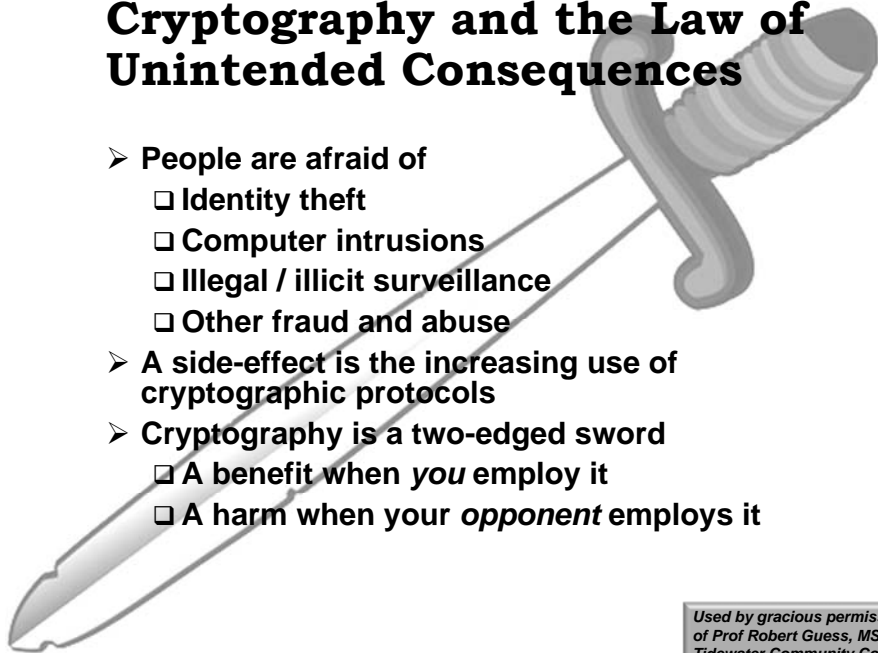


Computer Programs & Cryptography

- Not easily lumped into protected speech category
- Gov't usually can't prevent creation of code or dissemination
 - ❑ Limitations can exist and be enforced if necessary to protect human welfare, but not easy to do so
- In criminal cases, no bright-line rule about characterizing computer programs & conduct as protected
 - ❑ E.g., *US v. Mendelsohn*, no valid first amendment claim where computer program was only directed to committing a crime, and not directed to any ideas or consequences
 - ❑ In other cases, defendant's conduct *could* be deemed protected expression
 - ❑ But 1st amendment does not protect *deeds*, especially if they damage property or infringe rights



Cryptography and the Law of Unintended Consequences



- People are afraid of
 - ❑ Identity theft
 - ❑ Computer intrusions
 - ❑ Illegal / illicit surveillance
 - ❑ Other fraud and abuse
- A side-effect is the increasing use of cryptographic protocols
- Cryptography is a two-edged sword
 - ❑ A benefit when *you* employ it
 - ❑ A harm when your *opponent* employs it

Used by gracious permission of Prof Robert Guess, MSIA Tidewater Community College

Cryptoanarchy



- Cryptoanarchy: “the proliferation of cryptography that provides the benefits of confidentiality protection but does nothing about its harms” (Denning)
- This view led to the Clipper Chip fiasco (see below)
 - ❑ Failure to provide crypto keys in Britain ~2-5 yr sentence
 - ❑ France requires registration of crypto keys
- But crypto not a major problem for LE because
 - ❑ Strong crypto algorithm built on a weak platform (OS) or poorly written may be weak and subject to penetration
 - ❑ Progress in cryptanalysis makes crypto less of a problem for LE
 - ❑ Massively parallel applications like AccessData DNA help cryptanalysis (see EFF projects on DES)
- Many argue that to criminalize crypto would be an INFOSEC disaster

Used by gracious permission of Prof Robert Guess, MSIA Tidewater Community College

US Legal Status of Encryption



- The ITAR
- The Zimmerman Case
- The Clipper Chip & Key Escrow
- The Bernstein Case
- The EAR
- ICE Seizures
- Wassenaar Arrangement

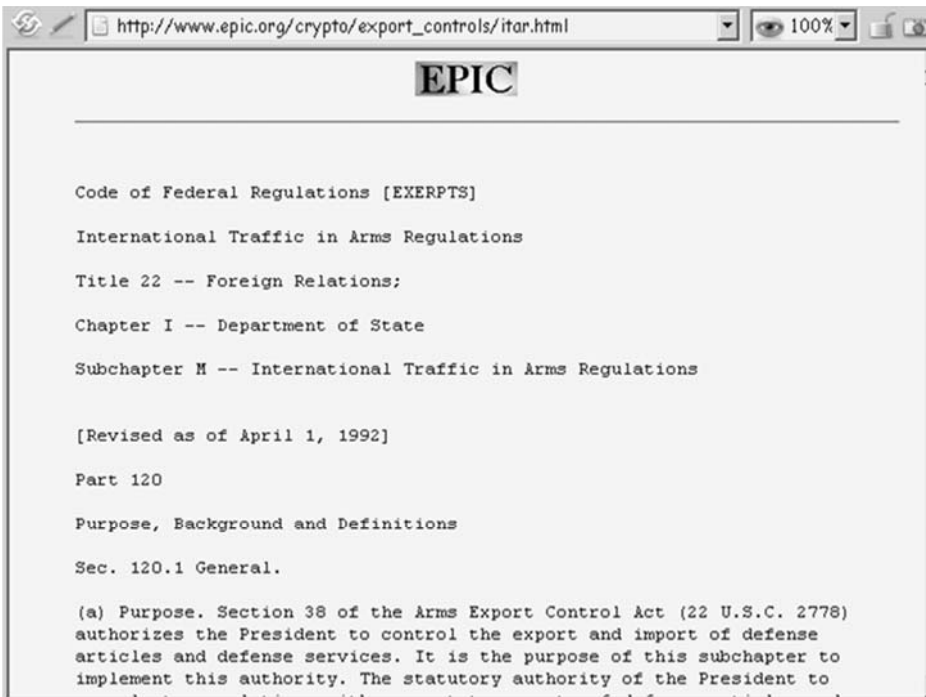


The ITAR



- *International Traffic in Arms Regulations*
- Administered by Department of State
- *Until 1996*, severely restricted export of cryptographic hardware and software as *munitions*
- Constant protests from cryptographers and companies
 - ❑ Nonsensical restriction
 - ❑ Interference with trade
 - ❑ Putting US suppliers at disadvantage

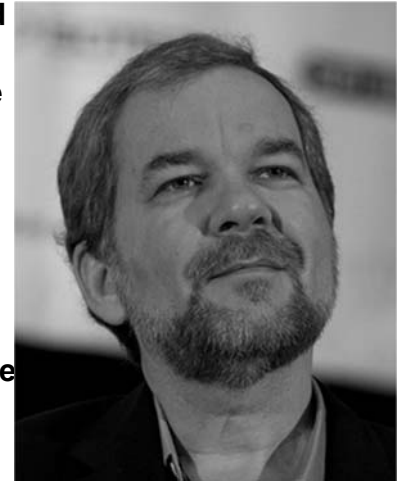




The Zimmermann Case



- Phil Zimmermann created PGP* in early 1990s
- Code was freely available
- Someone posted code to BBS overseas
- US government accused Zimmermann of violating the ITAR
- World-wide protests
- Phil Zimmermann Defense Fund
- Eventually dropped the prosecution



*PGP = *Pretty Good Privacy* (named after *Ralph's Pretty Good Grocery Store from Lake Wobegone*)

18

The EAR

Export Administration Regulations Database



- Export Administration Regulations
- Administered by Department of Commerce
- Encryption shifted from ITAR to EAR in 1996
- Welcome change – liberalized regulations
- Updated 2008-10-03: see <http://www.bis.doc.gov/encryption/default.htm>

☐ See next slide

http://www.access.gpo.gov/bis/ear/ear_data.html

19

Copyright © 2011 M. E. Kabay, J. Tower-Pierce & P. R. Stephenson. All rights reserved.

COMMERCIAL ENCRYPTION EXPORT CONTROLS

Export and reexport controls on commercial encryption products are administered by the Bureau of Industry and Security (BIS) of the U.S. Department of Commerce. Rules governing exports and reexports of encryption items are found in the Export Administration Regulations (EAR), 15 C.F.R. Parts 730-774, Sections 740.13, 740.17 and 742.15 of the EAR are the principal references for the export and reexport of encryption items.

Regulations - encryption rules published by BIS since export control jurisdiction was transferred from the State Department to the Commerce Department in 1996.

Guidance - step-by-step instructions and guidance to help exporters when preparing a review request for >64-bit mass market encryption or License Exception ENC, applying for a license, or submitting a notification for NLR, data test software or "publicly available" source code (and corresponding object code). For exporters who are exploring whether their products are subject to these review or notification requirements, a basic "checklist" on encryption and other "information security" functions is provided.

Advisory Opinions - advisory opinions related to encryption items may be reviewed on the advisory opinions web page.

Encryption Simplification Rule of October 3, 2008 (73 FR 57495)

Summary of Amendments to the Export Administration Regulations

Restructures license exception ENC based on what type of review and waiting period are required.

- Adds Bulgaria, Canada, Iceland, Romania, and Turkey to the list of countries that receive favorable treatment under License Exception ENC (Supplement 3 to Part 740).
- Removes obsolete License Exception KMI.
- Removes notification requirements for certain items classified as 5A992, 5D992, and 5E992.

(Much more below)

Cryptographic Regulations

- NSA / Department of Commerce study found that regulation had “a negative effect on US competitiveness”
- No domestic limitation on use or sale
- Bureau of Export Administration (BXA) License required for export of strong crypto
- No export to Cuba, Iran, Iraq*, Libya, North Korea, Sudan, and Syria
- Code as Speech - Bernstein V US State Dept (next slide)



Used by gracious permission of Prof Robert Guess, MSIA Tidewater Community College

Bernstein v. US State Dept

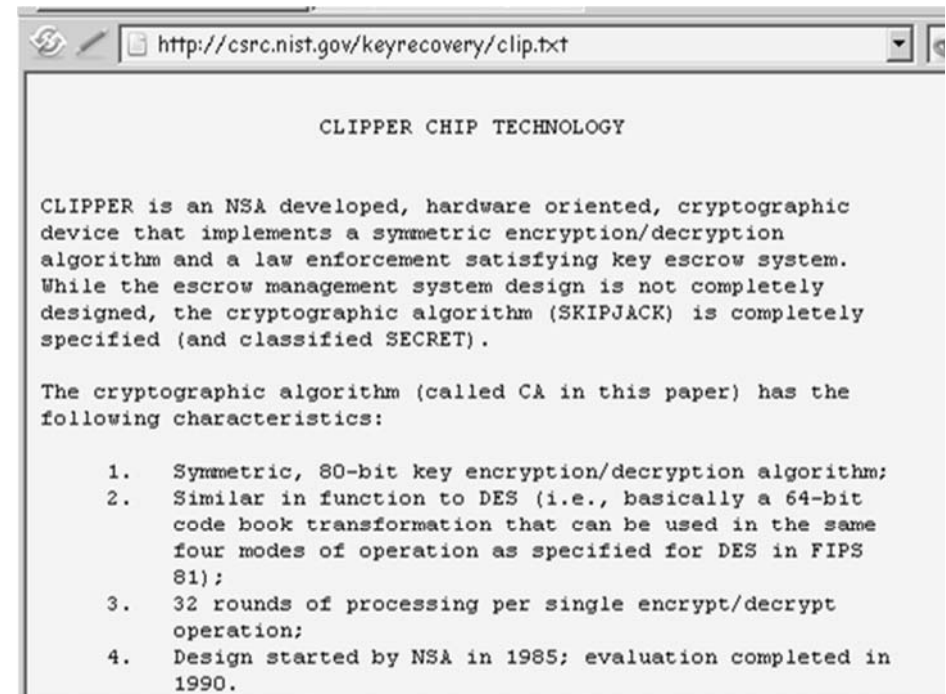
- ❑ UC Berkeley student Daniel Bernstein wanted to post *Snuffle* encryption technology online
 - ✓ Gov't feared spread of technology
 - ✓ Act enacted restricting export
- ❑ Bernstein challenged Act, claiming source code for computer cryptography program was protected under 1st Amendment
- ❑ Court found code = language, which = speech
 - ✓ Gov't could not restrict dissemination (disovulation??)
- ❑ Case rendered moot when gov't switched to EAR instead of ITAR – Bernstein lost standing in court



Used by gracious permission of Prof Robert Guess, MSIA Tidewater Community College

Key Escrow

- When users encrypt critical data, must have way of decrypting
 - ❑ User leaves
 - ❑ User becomes non-cooperative (or dies)
- Can store versions of key or alternate keys
 - ❑ Public Key Cryptosystem (PKC) allows encryption to multiple *public keys*
 - ❑ Any owner of corresponding *private key* can decrypt the *ciphertext*
- Modern cryptographic products (e.g., PGP) offer escrow functions for corporate users



Clipper Chip & Key Escrow (1993)

- Encryption had been domain of military (esp NSA) for decades
- By early 1990s, personal computers made enough computational power available for general use by the public
- Pretty Good Privacy implemented PKC
- April 1993: Clinton administration proposed Clipper Chip
 - ❑ Phones, fax, modems to be equipped with special chip (Clipper) to implement SKIPJACK algorithm
 - ❑ Government would access LEAF (Law Enforcement Access Field) to decrypt



Clipper Chip (cont'd)



Technologies for Government, Defense, Finance and Business

- Reaction overwhelmingly negative
 - ❑ Secret algorithms contemptible
 - ✓ Details of the Clipper Chip were found thrown out in trash of manufacturer
 - ✓ Committee of experts eventually given access to the code; pronounced OK
 - ❑ Proposal would be meaningful only if other encryption were made illegal
 - ✓ “Mandatory key escrow”
 - ❑ Key escrow proposal said to be open to abuse
 - ✓ But required collusion of people in 2 separate agencies of US government
- Proposal finally abandoned in 2000

SAFE Act of 1997 (failed)

- SAFE Act (Security and Freedom through Encryption) of 1997
- Attempted amendment to 18 USC by adding new Chapter 123 with
 - ❑ §2801. Definitions
 - ❑ §2802. Freedom to use encryption
 - ❑ §2803. Freedom to sell encryption
 - ❑ §2804. Prohibition on mandatory key escrow
 - ❑ §2805. Unlawful use of encryption in furtherance of a criminal act
- Failed to pass into law
- Currently, there are *no restrictions whatever* on the use of encryption *inside* the USA



US ICE Seizures: Boucher

- Dec 2006: Sebastian Boucher
 - ❑ Canadian citizen
 - ❑ Legal resident of USA
 - ❑ Crossed US border at Derby Line, VT
- US ICE (Immigration & Customs Enforcement)
 - ❑ Inspected computer with permission
 - ❑ Found adult pornography
 - ❑ Then found some child pornography on Z: drive
 - ❑ Z: drive encrypted using PGP disk encryption



(cont'd on following slide)

US ICE and Encryption [2]

- 2007: Grand Jury issues subpoena
 - ❑ Required Boucher to divulge decryption key for Z: drive
 - ❑ Judge Jerome J. Niedermeier then overturned subpoena on 5th Amendment grounds against self-incrimination



- Issues:
 - ❑ Forcing revelation of *information* held in mind of accused is protected by 5th Amendment.
 - ❑ But there is case law where self-incrimination protection forfeited by *permission* for search
 - ❑ What about
 - ✓ National security?
 - ✓ Corporate info?

See article by John Curran of Associated Press about case: <http://tinyurl.com/668v2u>
 Articles by Prof Kabay about implications of case: <http://tinyurl.com/5cs8yt> <http://tinyurl.com/68keob> <http://tinyurl.com/6g2ly5>
 Blog by Debbie Schlusel: <http://tinyurl.com/2hfofx>

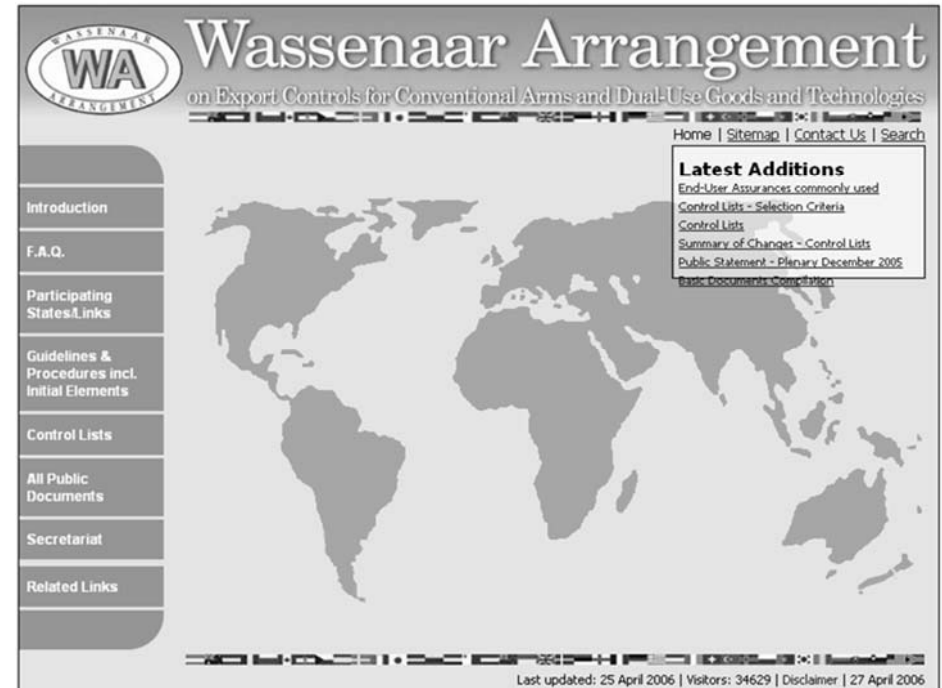
Wassenaar Arrangement

- Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies <http://www.wassenaar.org/>
 - ❑ Named after town in Netherlands
 - ❑ Established in 1995 by 28 countries
 - ❑ Follow-up to the Coordinating Committee for Multilateral Export Controls (COCOM)
 - ✓ Intended to prevent export of encryption to “dangerous” countries (Soviet bloc)
 - ❑ Completed 1998
- Provides *framework* to be implemented by signatory countries



Wassenaar (cont'd)

- Liberalized restrictions on encryption
- No restrictions on export of encryption products for personal use
- No restrictions on Internet publishing of encryption algorithms
- Public domain encryption software freely exportable

The screenshot shows the homepage of the Wassenaar Arrangement website. At the top, there is a logo with 'WA' and 'WASSENAAR ARRANGEMENT' and the title 'Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies'. Below the title is a navigation bar with links for Home, Sitemap, Contact Us, and Search. A sidebar on the left contains a menu with items: Introduction, F.A.Q., Participating States & Links, Guidelines & Procedures incl. Initial Elements, Control Lists, All Public Documents, Secretariat, and Related Links. The main content area features a world map and a 'Latest Additions' box listing: End-User Assurances commonly used, Control Lists - Selection Criteria, Control Lists, Summary of Changes - Control Lists, and Public Statement - Plenary December 2005. At the bottom right, it says 'Last updated: 25 April 2006 | Visitors: 34629 | Disclaimer | 27 April 2006'.