CLEARSWIFT
MIMEsweeper™
policy-based content security

Content Security
- the legal background

John Stewart
Business Manager
Central/East Europe
www.mimesweeper.com

CLEARSWIFT
MIMEsweeper™
policy-based content security

What is Content Security Risk?

- Risk of confidentiality and privacy breaches
  - Non-disclosure agreements
  - Duty of care under privacy laws
- Risk of defamation and obscenity
  - Vicarious liability for employee actions
- Risk of loss of corporate time & resources
- Risk of breach of intellectual copyright
- Risk of inadvertent contractual liability

CLEARSWIFT
MIMEsweeper™
policy-based content security

Legislation Overview

- Gramm-Leach-Bailey Act (USA)
- HIPAA Act (USA)
- Digital Commerce Act (USA)
- Safe Harbor Agreement (USA)
- Data Protection Directive (EU)
- Cybercrime Treaty (EU)
- European Convention on Human Rights (EU)
- Data Protection Act (UK)
- Regulation of Investigatory Powers Act (UK)
- Human Rights Act (UK)

CLEARSWIFT
MIMEsweeper™
policy-based content security

Digital Commerce Law

One Hundred Sixth Congress of the United States of America

AT THE SECOND SESSION

Begun and held at the City of Washington on Monday, the twenty-fourth day of January, two thousand

An Act

To facilitate the use of electronic records and signatures in interstate or foreign commerce.

Be it enacted by the Senate and House of Representatives of he United States of America in Congress assembled,

ECTION 1. SHORT TITLE.

This Act may be cited as the "Electronic Signatures in Global nd National Commerce Act".

TITLE I—ELECTRONIC RECORDS AND SIGNATURES IN COMMERCE

EC. 101. GENERAL RULE OF VALIDITY.

(a) IN GENERAL.—Notwithstanding any statute, regulation, or ther rule of law (other than this title and title II), with respect o any transaction in or affecting interstate or foreign commerce—

(1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

CLEARSWIFT
MIMEsweeper™
policy-based content security

Financial Services Modernization Act (USA)

Gramm-Leach-Bailey (1999)

CLEARSWIFT
MIMEsweeper™
policy-based content security

Privacy Policies

Gramm-Leach-Bliley (USA 1999)

- Financial Services Modernization Act

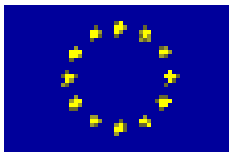
TITLE V -- PRIVACY

- Requires clear disclosure by all financial institutions of their privacy policy regarding the sharing of non-public personal information with both affiliates and third parties.
- Requires a notice to consumers and an opportunity to "opt-out" of sharing of non-public personal information with nonaffiliated third parties

Similar rules for health information (HIPAA Act)

CLEARSWIFT
MIMEsweeper™
policy-based content security

The EU Data Protection Directive



Data Protection

- EU 95/46/EC
  - Directive on Data Protection
  - Implemented in UK Data Protection Law
  - Similar laws in all EU countries
- Enforceable by Information Commissioners
- http://europa.eu.int

CLEARSWIFT
MIMEsweeper™
policy-based content security

The British Information Commissioner

United Kingdom

Mrs Elizabeth FRANCE
Information Commissioner
The Office of the Information Commissioner
Executive Department
Water Lane
Wycliffe House
UK - WILMSLOW - CHESHIRE SK9 5AF
Tel 44/1625/54.57.00

The Information Commissioner enforces and oversees the Data Protection Act 1998 and the Freedom of Information Act 2000.

The Commissioner is a UK independent supervisory authority reporting directly to the UK Parliament and has an international role as well as a national one.

http://www.dataprotection.gov.uk

8 Principles of Data Protection

- Fairness – fair play, fair process
- Limitation – only as needed
- Adequacy – relevant, sufficient
- Accuracy – correct, true
- Retention – time limited
- Respect – for human rights
- Security – kept confidential
- Protection – not transferred

CLEARSWIFT
MIMEsweeper™
policy-based content security

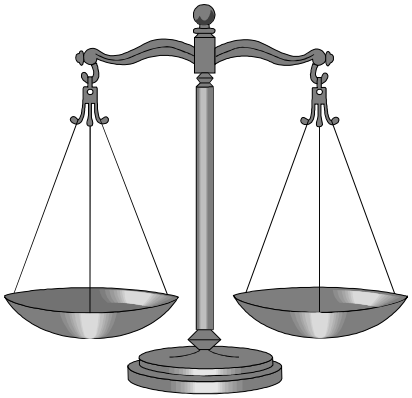
EU Cross Border Transfers

- 8th Principle Requires Data Protection in receiving country if outside EU
- Safe Harbor Legislation in USA
- Switzerland and Hungary accepted
- EU accession countries have Data Protection implemented eg in Poland..

Biuro Generalnego Inspektora Ochrony Danych Osobowych
Pl. Powstańców Warszawy 1
00-030 Warszawa

CLEARSWIFT
MIMEsweeper™
policy-based content security

Balancing Laws



- Data Protection Act
- Freedom of Information Act
- Human Rights Act
- Computer Misuse Act
- CyberCrime Treaty

CLEARSWIFT
MIMEsweeper™
policy-based content security

Who's allowed to monitor electronic communications?

Regulation of Investigatory Powers Act 2000 (R.I.P.)

- only the state authorities

+ businesses complying with Data Protection Act and laws to prevent computer misuse ("***lawful business practice***")

CLEARSWIFT
MIMEsweeper™
policy-based content security

Privacy v Lawful Practice?

Who's listening in on whom?

CLEARSWIFT
MIMEsweeper™
policy-based content security

Rules for *Lawful Business Practice* Monitoring

- Board level decision
- Employees must be informed
- Purpose must be for business compliance
- Technical measures must be based on acceptable use policies
- Code of practice published by UK Information Commissioner

CLEARSWIFT
MIMEsweeper™
policy-based content security

ISO 17799 (BS7799:1)

Standard for information security

– you must

1. have a **security policy document**
2. allocate **security responsibilities**
3. have information security **education & training**
4. **report** security incidents
5. **control viruses**
6. have a **business continuity plan**
7. have **control over proprietary** copying
8. **safeguard company records**
9. comply with **Data Protection Laws**
10. **show compliance** with security policies

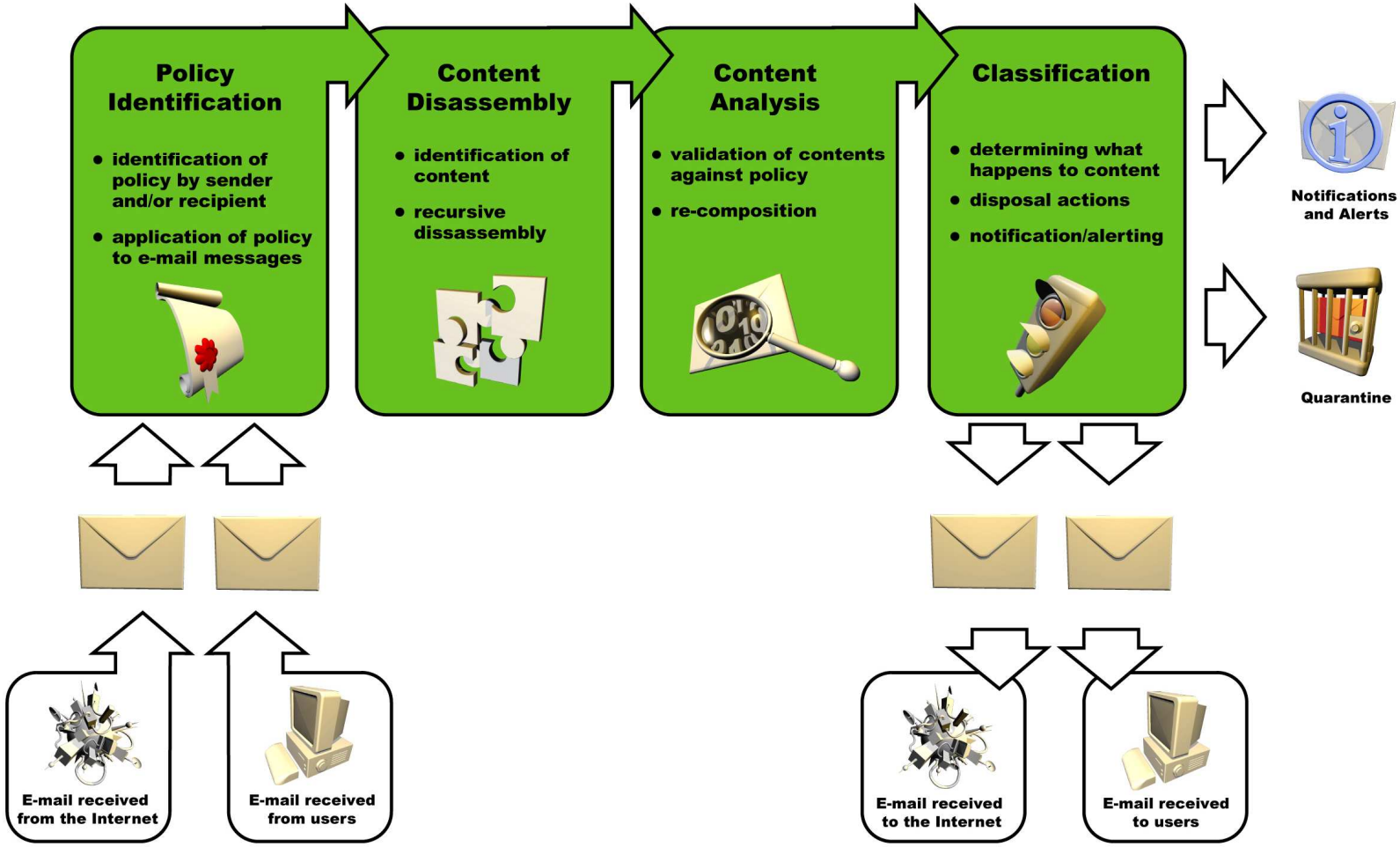
CLEARSWIFT
MIMEsweeper™
policy-based content security

The typical practice in UK

- All major UK organisations monitor employee email & web traffic for acceptable use
- The main reason is the protection of reputation, the second is compliance with law
- Company lawyers and personnel managers make the corporate policy - not the CIO
- 80-90% use MIMEsweeper as the preferred technical solution

CLEARSWIFT
MIMEsweeper™
policy-based content security

What does MIMEsweeper do?



(Technical presentation later ..)

Thanks for listening!

John.Stewart@safecomms.com

Presentation Slides (.ppt) and IDC White Paper (.pdf) available from www.cc.com.pl later this week.