

Comparative Approaches in IT Regulation: Communications Surveillance

Marc Rotenberg
EPIC

“Technology, Privacy and Justice”

Toronto, Canada

29 September 2005

Communication Surveillance

— [Public policy challenge - competing interests of communications privacy and public safety

— [Legal frameworks in constitutional democracies establish presumption of privacy

— [9-11 (USA), 11-3 (ESP), July 2005 (UK)

— [Focus is on new communication networks

— [Implications for “Lawful Access” preceding in Canada

IT Regulation

— [Network standards are malleable

— [Telcos and ISP are subject to regulation

— [Problems of international coordination

— [Challenge of new technologies - VOIP, ENUM

International Norms

— [Communications privacy is presumptively protected

— [“No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.” (UDHR, Art. 12, 1948)

National Norms

- [Constitution

- Section 8, Canadian Charter Rights and Freedom

- Fourth Amendment, United States Constitution

- [Statute

- Telecommunication Act (1993) (CAN)

- Federal Wiretap Act (1968) (US)

- [Similar constitutional and statutory provisions in EU Countries

Communications Privacy (US)

[“From Constitutional decision to statutory rule”

[Katz decision (1967)

[Federal Wiretap Act (1968)

[Foreign Intelligence Surveillance amendments (1978)

[Email amendments (1986)

Communications Surveillance (US)

— [“Communications Assistance for Law Enforcement Act” (1994)

— [~~Clipper chip (1994)~~

— [“Patriot Act” (2001)

— [Federal Communications Commission regulation on CALEA
(2004)

Surveillance Approach (US)

— [Make communication networks wiretap friendly

— [Ensure ongoing viability of established investigative technique

— [Regulate IT manufacture and service provision

— [Pursue standard-setting through Communications agency

— [Reimburse industry cost for compliance

— [Communications surveillance = real-time interception

Scope of Communications Surveillance (US)

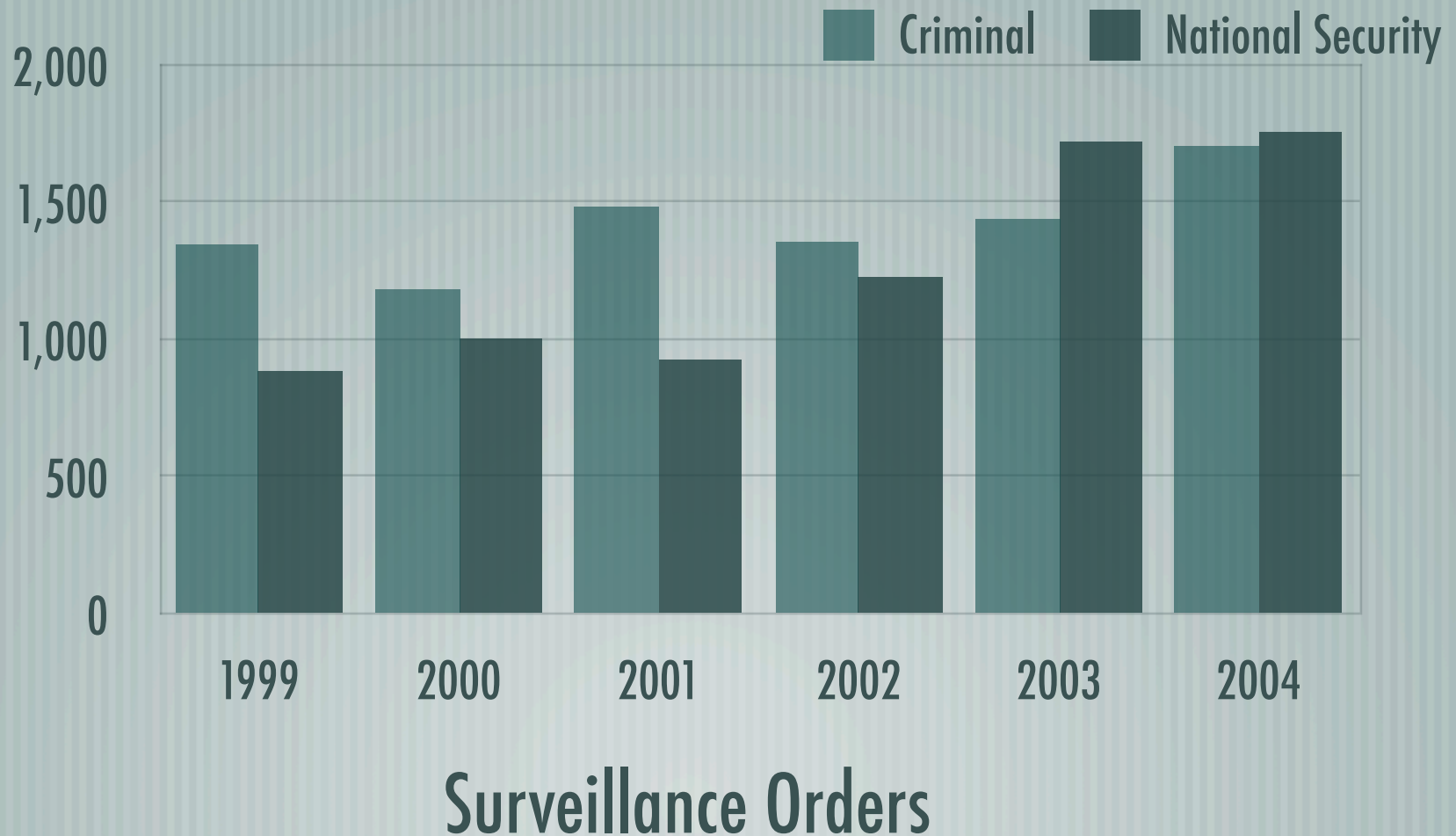
— [1994 - Obligations for telephony, not Internet

— [2004 - FBI: Obligation for Internet?

— [2005 - FCC: Obligation for Internet!

— [Implications - VOIP (Skype, Vonage), IPv6 ?

"Patriot Act" Impact on Communications Surveillance (US)



Data Retention

- [Communications businesses create customers records

- [Digital communications networks create transactional records

- CPNI - Customer Proprietary Network Information

- Web logs, Email traffic

- Implications for anonymity and political expression

- [Digital data is searchable - "Applications chase data"

Data Retention I (EU)

— [25 member state rules vary from no requirement to 3 year requirement

— [Issue left open by EU Communications Directive

— [Favor: UK, FRA, IRE, SWE, Justice Ministers

— [Oppose: Telcos and ISPs (cost), NGOs (human rights), EP (legality - "third pillar"), EU Data Protection Supervisor (legality - compliance with EU Data Directive)

Data Retention II (EU)

- [European Commission Proposal (9-2005)

- Response to member states push for greater control

- Fixed-line and mobile phones - 1 yr

- Email traffic - 6 months

- Reimburse telcos and ISPs

Data Retention III (EU)

— [Regulatory challenge




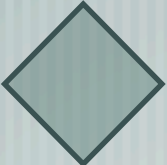
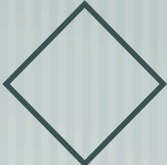

— [Cost

— [Legal compliance

Comparison - Outcomes

- [Wiretap friendly network
 - US - Require design meet FBI goals
 - EU - No comparable requirement
- [Access to communications data
 - US - Require data “preservation” (data for specific investigation)
 - EU - Require data “retention” (data for all customers)

IT Surveillance Regulation

	U.S.	E.U.	CND
Rule			
Cost			
Harmonize			

Still Ahead I

- [**New Technologies**

- **VOIP**

- **IPv6**

- [**Regulatory Challenges**

- **Cost**

- **Technical success**

- **Coordination**

Still Ahead II

— [Legal challenges - does IT regulatory goal comply with legal rules and Constitutional norms?

— [Problem of prospective searches

— [Techniques evade judicial review

Lawful Access Debate I (CND)

— [Criminal Code makes the unlawful interception of private communications a criminal offense

— [Police are required to obtain a court order and interception is only authorized in cases "where other investigative procedures are unlikely to succeed."

— [Supreme Court stated that in order to obtain a wiretapping warrant police must show that "there is no other reasonable alternative method of investigation." (2000)

Lawful Access Debate II (CND)

- [Ministry of Justice and Industry Canada released a consultation document on implementing the Cybercrime Convention into Canadian law. (2002)
- [The "Lawful Access Consultation" document proposed legislative amendments to various acts regulating lawful access in preparation for ratifying the Convention
- [Privacy commissioners allege that proposal lacks adequate privacy safeguards and grants excessive powers to intercept communications

IT Surveillance Regulation

- [Systems of identification

- Biometric cards

- [Systems of transportation

- GPS

- [Systems of commerce

- RFID

Constitutional norms must guide IT regulation

Resources and Credits

— [EPIC, Data Retention web page [www.epic.org/privacy/intl/data_retention.html]

— [EPIC, Wiretap web page [www.epic.org/privacy/wiretap]

— [EPIC, Privacy and Human Rights: An International Survey of Privacy Laws and Developments (2004)

Note: Presentation made possible in part with the support of the Social Science and Humanities Research Council of Canada and the Anonymity Trail Project of the University of Ottawa School of Law