Internet
Privacy and Surveillance

Centre for Internet and Society
Bangalore 27th June 2011

Caspar Bowden

(Director www.fipr.org 1998-2002)

[currently Chief Privacy Adviser for Microsoft,
but these are personal views, not positions attributable to Microsoft]

(selective) chronology of privacy regulation

1765: UK Entick vs. Carrington (no "general warrants")

1791: US 4th Amendment (ditto + need probable cause)

1948: UNDHR ("no arbitrary…interference" + right to protection)

1950: ECHR Art.8 (ditto)

1970: 1st DP law in Hesse (Germany)

1973: 1st national DP law in Sweden

1974: US Privacy Act (only public sector)

1978: French DP law

1980: OECD guidelines

1981: Council of Europe Convention 108

1983: German census decision ("information self-determination")

1984: UK DP law

1995: EU Data Protection Directive

2011-: consultations on new EU DP framework

2012-: new US Federal law (DoC green paper, FTC consultation)?

(selective) chronology of covert mass-surveillance

1600s- : Black Chambers, Royal Mail, Mazzini affair
1936-45: ENIGMA, Bletchley, MAGIC, Op-20-G
1945-: GCHQ, NSA, BRUSA, UKUSA
1967: UK "D-Notice" affair
1975: Church Committee
1978: US FISA law, UK "ABC" trial
1985: UK IOCA law ("certificated warrants")
1999: EU report and inquiry into ECHELON
2000: UK RIPA (s.16 authorizes domestic trawling)
2001: 9/11: US PATRIOT, UK ATCSA Pt.11 (data retention)
2003: ~~Total~~ Terrorism Information Awareness furore
2005-: "warrantless wiretapping" exposé
2005: EU Data Retention Directive
2007-: UK "Interception Modernization Program" disclosed, "PROTINT"
2007/8: Protect America 2007, FISA Amendment 2008 (*ex-post* minimisation)
2010: US CALEA 2 rumours
2011: EU DRD revision, US hearings on data retention, cyber-warfare ?

Why worry ?
….and why is this interesting ?

- formulation of constitutional and human rights predated Internet mass-surveillance
- sharp techno-legal dilemmas/dichotomies
  - encryption key escrow vs. reverse burden-proof
  - traffic data retention vs. data preservation
  - surveillance by design vs. privacy by design ?
- sudden new phenomena
  - social networks, location/mobile platforms
- normal democratic checks-and-balances don't work for covert surveillance policymaking
  - knowledge is power – rule-of-law may be bypassed
  - expedient reliance on private organisations

“normative” interception law

- “wiretap warrant” – targeted at individual, **domestic communications**
  - ISPs must maintain **“black-boxes”** tapping whole stream of Internet data
  - authorization: signed by political minister or independent judge ?
  - intelligence/security + police, military, customs agencies
- “trawling warrant” (scanning **international communications)**
  - might utilize ISPs/telcos “black boxes” or other means (direct access to cables?)
  - targeting by abstract “factors” - combo of traffic analysis + keywords + AI ?
- “oversight” – retired judge or special court ?
  - Independent technical investigative competence vs. “good chap” theory of Govt.
  - Technical means to verify that only lawfully authorised interference (audit + crypto)
  - Reporting to Parliament – or Prime Minister ?
- “redress” – investigating complaints of individuals
  - accept any complaints in connection with human rights violation (not just privacy) ?
  - Kafka-esque secret proceedings ?
  - if complaint upheld, can political wrongdoing be covered up by ”national security”?

Internet mass-surveillance

- (UK) RIPA 16(3) –
  - appears to authorize a 3rd type of warrant
    - allows GCHQ to "look inwards" at UK domestic communications for 3 months at a time
- (US) FISA Amendment Act 2008
  - for non-US persons….
  - much broader than counter-terrorism
  - surveillance of "foreign political associations"
  - applies to any data held by US corporation
  - intended expressly to cover Cloud Computing

U.S. Protect America Act 2007

- Scandal of "warrantless wiretapping": 2005-2008
  - AT&T technician discovered much US Internet traffic being tapped, triaged, diverted to National Security Agency
  - Under FISA 1978, requirement to "minimize" intrusion on U.S. persons
  - To and fro saga of US Administration officials being kept in dark, refusing to re-authorize "Terrorist Surveillance" programs
- FISA Court had rejected major authorization circa 2005: President of Court withheld facts from other judges (!)
  - substance of argument about how hard NSA had to work to prevent collection of data of "U.S. persons"
  - Protect America Act changed to doctrine of minimize-use-not-collection. FISA Court now "approves" policy of ODNI
- Obama administration not touched
  - "Get FISA right!" FB campaign fast growing 2008 election

The Trouble with Pseudonymity

- examples of pseudonymous identifiers :
  - dynamic IP address
  - social security number
  - MAC address (WiFi hotspot and PCs/phones)
  - cookie identifier
  - any persistent account identifier (AOL dataset)
- re-identification by legal means
  - copyright enforcement (“3 strikes laws”)
  - court order to obtain IP address from ISP
- re-identification by technical/statistical means
  - NETflix datatset, Shmatikov 2008

EU Data Protection Directive EC 95/46

Crucial definition of **"personal data"** altered by industry and UK government lobbying 1994-5 in European Parliament. Single most important reason why EU DP not effective on the Internet

- Article 2
  - *(a) **'personal data'** shall mean any information relating to an identified or identifiable natural person ('data subject'); an **identifiable** person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;*

The central question: Identifiable by whom?

- Recital 26
  - *Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the **means likely reasonably to be used** either by the controller **or by any other person** to identify the said person; whereas the' principles of protection shall **not apply to data rendered anonymous in such a way that the data subject is no longer identifiable**.*

MORAL: pay close attention to defn. in forthcoming Indian law!

Key escrow policy US/UK 1990s

- US : “Clipper” Chip
  - intended to be embedded in every PC (and fax machine)
  - Discredited by computer scientist finding a way to circumvent
  - “key recovery in” software
  - Is it lawful to prevent publication of source code on the Internet?
  - 1st Amendment vs. munitions export control regulations
  - escrow policy dead by early 1998
- UK:
  - “Cloud Cover” for key escrow in software
  - 1997 (pre-election) consultation on “Licensing of Trusted Third Parties”
  - proposed legal privileges for crypto providers operating “key escow”
- EU
  - sinks escrow policy by decoupling dig.sig from key escrow
  - industry mobilized, policy dead in U.K. late ’98

Power to demand a password (or decryption key)

- RIPA 2000 Pt.3
- Reversal of the burden-of-proof !
  - defendant must show they do not have the password (or do not possess the key)
  - How?
  - do you remember every password you ever made up?
  - no reliable defence for the innocent
  - blackmail, coercion, false accusations, planted evidence
- 2000: major media and Parliamentary controversy in UK
  - amended somewhat, but untested still (after 11 years!)
- In practice no advantage over contempt of court and circumstantial evidence
- …since 2007 half-dozen former British colonies now copied law
  - (3 Africa , 3 Caribbean)
  - …hope they realize what they did !

“Identity Escrow” – blanket data retention

EU Data Retention Directive 2006 (EC 06/24)

Recital 3: Articles 5, 6 and 9 of **Directive 2002/58/EC** lay down the rules applicable to the processing by network and service providers of traffic and location data generated by using electronic communications services. Such data **must be erased or made anonymous when no longer needed for the purpose of the transmission** of a communication, except for the data necessary for billing or interconnection payments.

Recital 9: …. Because retention of data has proved to be such a necessary and effective investigative tool for law enforcement in several Member States, and in particular concerning serious matters such as organised crime and terrorism, it is necessary to ensure that retained data are made available to law enforcement authorities for a certain period, subject to the conditions provided for in this Directive. The adoption of an instrument on data retention that complies with the requirements of Article 8 of the ECHR **is therefore a necessary measure**.

Article 5 - Categories of data to be retained

- 1. Member States shall ensure that the following categories of data are retained under this Directive:
- (a) data necessary to trace and **identify** the source of a communication:…
- (2) concerning Internet access, Internet e-mail and Internet telephony:
  - (i) the user ID(s) allocated;
  - (ii) the user ID and telephone number allocated to any communication entering the public telephone network;
  - (iii) the name and address of the subscriber or registered user to whom an **Internet Protocol (IP) address**, user ID or telephone number was allocated at the time of the communication;
- (b) data necessary to **identify** the destination of a communication:…
- (2) concerning Internet e-mail and Internet telephony:
  - (i) the user ID or telephone number of the intended recipient(s) of an Internet telephony call;
  - (ii) the name(s) and address(es) of the subscriber(s) or registered user(s) and user ID of the intended recipient of the communication;
- (c) data necessary to identify the date, time and duration of a communication:…
- (2) concerning Internet access, Internet e-mail and Internet telephony:
  - (i) the date and time of the log-in and log-off of the Internet access service, based on a certain time zone, together with **the IP address, whether dynamic or static**, allocated by the Internet access service provider to a communication, and the user ID of the subscriber or registered user;

=> If the purpose (inter alia) of data retention is to identify users from IP addresses, it would be perverse to regard IP addresses as non-identifiable and hence not personal data !

Romanian DRD decision (2009)
(not on grounds of proportionality)

- *The obligation to retain… as an exception or a derogation from the principle of personal data protection and their confidentiality, **empties**, through its nature, length and application domain, **the content of this principle**... it is unanimously recognized in the ECHR jurisprudence…that the signatory member states… have assumed **obligations to ensure** that the rights guaranteed by the Convention are **concrete and effective, not theoretical and illusory**… **the continuous retention** of personal data **transforms… the exception… into an absolute rule**. The right appears as being regulated in a negative manner, its positive role losing its prevailing role*
- *…the **continuous limitation** of the privacy right… **makes the essence of the right disappear**… mass users of the public electronic communication services or networks, are **permanent subjects to this intrusion** into their exercise of their private rights to correspondence and freedom of expression, without the possibility of a free, uncensored manifestation, except for direct communication, thus **excluding the main communication means used nowadays**.*
- *…justified* **use***… is **not** the one that in itself harms in an unacceptable way the exercise of the right to privacy or the freedom of expression, **but rather the legal obligation with a continuous character, generally applicable, of data retention**… regardless of whether they have committed penal crimes or not or whether they are the subject of a penal investigation or not, which is likely to **overturn the presumption of innocence** and to transform a priori all users of electronic communication services or public communication networks into people susceptible of committing terrorism crimes or other serious crimes.*
- *…the **continuous** character of the obligation to retain the traffic and localization data… is **unconstitutional in its entirety**…*

Divergences

US

- no 4th Amendment for traffic data
- "3rd party doctrine" – LEA access to private-sector data without court order
- right to be let alone + "reasonable expectation of privacy"
- vertical privacy laws, no private-sector subject access by *right*
- constitutional rights for US persons
- "warrantless wiretapping" 2001-?
  - FISA Amendment 2008 legitimized *ex-post* filtering out of US persons
  - Catch-22 on civil redress
- irreversible shift to "national surveillance state" ? (Balkin 2008)
- mantra: "control usage not collection"
- data-mining programs reported to Congress, but complexity trumps transparency

Europe

- traffic data protected (Malone v. UK ECHR 1984)
- +ve duty to minimize infringement of broad concept of "private life", privacy as human dignity
- collection of data engages privacy (Rotaru/Amann ECHR), indiscriminate collection deprecated (Marper)
- horizontal Data Protection law, comprehensive subject access right
- human rights independent of nationality
- national security (mostly) exempt from DP law
- Parliamentary and judicial oversight murky at best
- EU/member-state boundary of "national security" clear as mud (ECHELON/Prum/PNR/SWIFT/DRD)

A question of balance ?

…the cliché of first resort…

…how is the balance point decided…

…and what kind of stability?

A = Stable equilibrium.

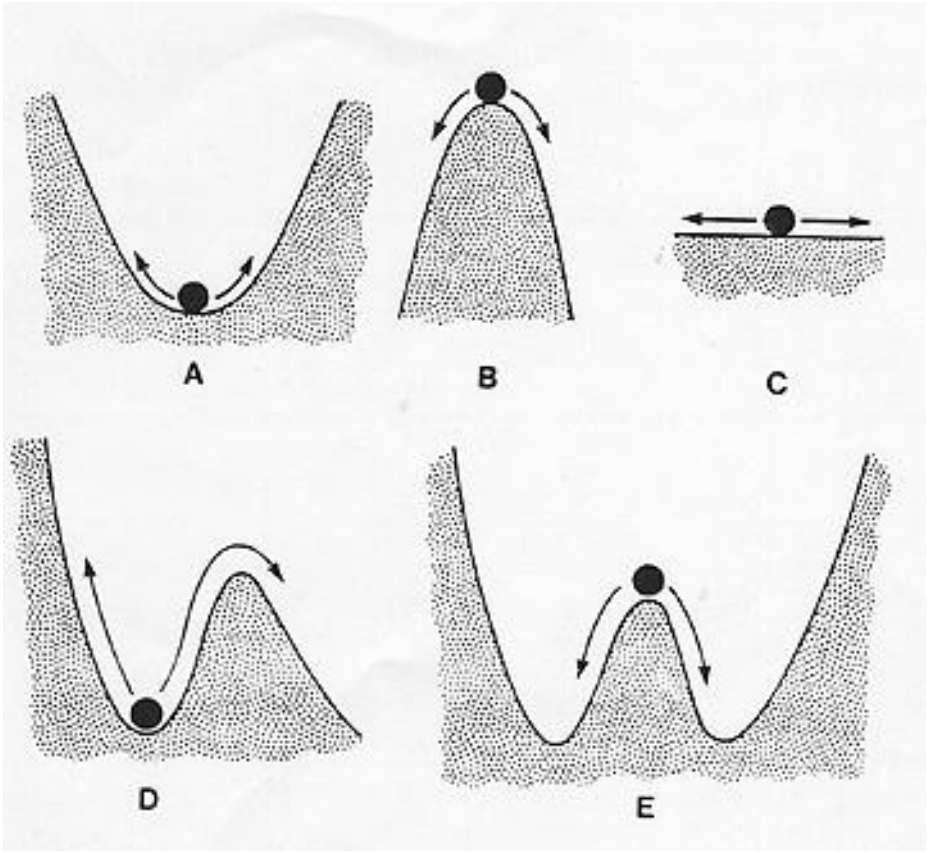
B = Unstable equilibrium.

C = Neutrally stable equilibrium.

D = Metastable equilibrium.

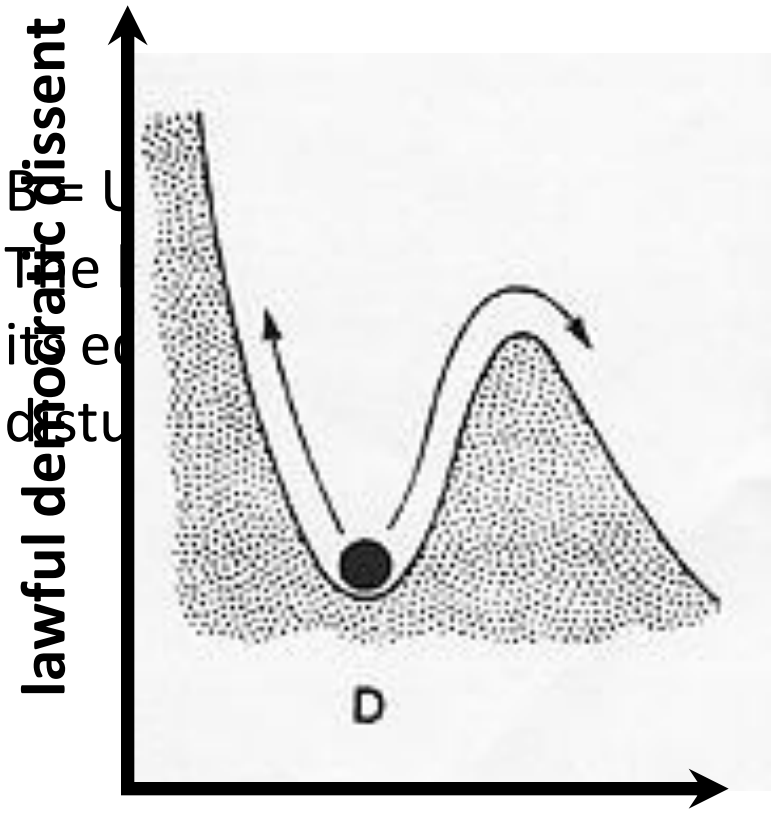
E = Metastable equilibria with multiple stable states.

http://classes.entom.wsu.edu/529/Stability.htm



Slippery slope

…of two kinds…



D = Metastable equilibrium.

if surveillance power increases beyond a critical point, lawful democratic dissent is chilled

intelligentsia will not risk "getting their name on a list"

MORE INSIDIOUS EFFECT THAN "PANOPTIC" CONFORMITY OF OVERT SURVEILLANCE

Conclusions

- **technically competent oversight or "oversight theatre"?**
  - obsolete laws govern transfers of data, **not modalities of analysis**
  - IoCC (etc.): risibly vacuous reports, no credible technical capacity
  - IPT: Kafka-esque secret procedures, mysterious status wr.t. IoCC etc.
  - I&SC: no role examining operational policies, few actual investigative powers
- (*quis custodiet* etc..) **beware** temptation to avoid political controversy of overt surveillance by substituting politically "invisible" covert measures
  - UK amongst most consistently privacy-mediocre Western governments, since Younger (72), Lindop (78), CoE, R87, DPD, SSBFA, Caldicott, DPA, RIPA, DRD,…
  - as if: UK policy captured by a surveillance-industrial-media complex ?
- democracy is like a Test Match (cricket)
  - no agent can win legitimately if any agent is too powerful (no Leviathan)
  - UK seems to think *"we wrote ECHR, and Art.8 doesn't apply to us" ?*
  - as if: *no public/political understanding => no chilling effect, no problem* (!?!?)

Q & A