TRUST AND PRIVACY : WHO'S IN CONTROL?

JULIET LODGE

Internet Privacy –
A Culture of Privacy and Trust on the Internet

March 26, 2012 – HumboldtCarré, Behrenstr. 42, 10117 Berlin

Starting point : the end of privacy

- Quantum surveillance
- Biometrics and tracking e-IDs
- Mission creep from territorial border security to body invasion
- US v EU defin of biometrics
- Legitimising PPPs, data blending
- Insufficiency of scope of ethical codes apps
- Inadequate or obsolete politico-legal controls

Now : ICT ethics beyond DP and privacy?

Selling behaviour

- Quantum surveillance in public space (security rationale) and in private and space via m- play (conven+com)
- Mining,mash-ups to visualisation
- Multiple clouds and & data blending
- Geo-referencing and map-making

Withstanding q-surveillance

- Privacy as a right
- Stronger data protection
- PETs/PEDs – pseudo technical fixes

= **online definition of reality affects real world choices : mediates power; ethics and societal acceptability of ICT applicatns**

The 'who dunnit' Regulatory Challenge

'who dunnit' burden of proof and responsibility

Technical fixes

- forensic genomics, biometrics neuro-imaging, digi tracking
- georeferencing
- IP, Censorship, Anonymity

Politico-legal agency

- Locus of authority+dm
- Responsibility /accountability
- DP + Forgetting + linkage
- Legitimacy and surveillance PPPs/privatising sec/and DP
- Redefining Private sphere
- Mobiles and vanishing interfaces
- Morality and Ethics – access
- Human dignity; transhumanism & roboethics

Moral and legal status of delegated decisionmaking and denial of service

- Surveillance society ; ID theft; ID presence online outside real-time genuine human presence ;
- Convergent Technologies (Nano, Bio, Info, Cogno) Vanishing interfaces; Ubiquitous Computing
- Robotics
- Privacy and the end of secrecy
- ICT-Implants and Enhancements
- AI algorithms replacing tasks previously performed by humans—the AI algorithm inherits the associated social requirements; must be predictable, transparent, robust ag.manipulation

New questions? The body as a resource

Does the concept of the autonomous self have meaning when we're online and inter-connected when asleep/forever?

What values are embedded by default in ICT design and internet use?

How does this link to the governance of science and society?

Identity in digi-space

- Lack of territoriality
- Who's who?
- How do you know you are who you say you are?
- How do I know? How do you know?
- Genuine v bogus ID claims
- citizen multiple IDs :- infinitely manipulable, costly, exclusionary, risky and out-sourced
- Avatar v biometrics
- Problems of invisibility and trust

PETs – ethical or criminal?

Privacy enhancing technology as a crime

- Ethical implications of automating CCTV surveillance
- retrospective data mining

Choice of technology reflects ethical/moral concerns or lack of concern

PETs as PRIVACY...looks for behavioural deviation rather than tracking, and so greater privacy might follow from automated surveillance

Balancing rhetoric and practice with hierarchy of ethics and morals

Risky biometrics or trusted, credible IDs
mirroring behaviour v deception : border between natural and artificial

Beyond the Security – liberty continuum

- privatising human security by shrinking private space

Risks of privatising accountability , trust and responsibility

Steering behaviour for honest and dishonest purposes

Forensic genomics

- Dimensions of linkage from known kinship and ‘facebook friends’ through blood lines, DNA etc over many generations
- Right to be forgotten – depends on the requirement to be known to the ‘authorities’
- Right to be forgotten is not credible and cannot be trusted
- How can we protect ourselves and the vulnerable against abuse?

Mission creep

- TWRI
- RFID apps
- Biometrics
- Dual use : domestic policy towards surveillance, tracking, info sharing ….becoming a tool of foreign policy?
- Cyber-libertarian ideals (free use everywhere and no censorship) clash with regulatory approach to limiting sales of sensitive stuff to undesirable or repressive regimes, and with advocacy of self-regulation and self-checking by IT companies by requiring them to check afterwards that their goods are actually in the state to whom they sold the equipment (IP address tracking)…what sanctions? Who enforces them?

(un)ethical human (in)security?

Risky deployment of biometrics leads to

1. Naïve commodification of citizens in the name of security/risk minimisation for diverse purposes (such as eIDs)
2. mission creep and raises serious ethical issues about the impact on human dignity and society
3. imperils citizens' rights
4. Biom for security disrupt e-life impelling innovation
5. AMI shrinks private space so we focus on human security not state security

Personal responsibility or corporate duty or legal requirement?

- **Scanning:** Enhancing technology that scans the Web to reveal tracking
- **Education:** Helping people see how much information they share
- **Control:** Improving software that helps people control sensitive information
- LAW : a "privacy bill of rights" that would give people greater control over their data

Conclusions

- ICTs are not neutral in impact or in application : they are divisive, disruptive & their failings risk weakening trust in technology and in govt
- The transformative impact of biom apps is extensive and expanding, driven by commerce and a security/safety discourse
- PETs and PEDs are temp fixes
- looking to a relatively amoral industry like ICTs to act as a human rights guardian is asking for trouble and misses the point...DP Regn step in right direction
- Allowing non-EU states to define acceptable use is not acceptable if any western values and ethics are to retain meaning and credibility
- Biometric parameters of the self : Who's in control?

Communicating control

'Citizens must be able to understand the system so that they can identify its problems, criticise it, and ultimately control it.'

Final report of the Convention on the Future of Europe

Working Group IX on Simplification 29 Nov 2002

[CONV 424/02 WGIX 13]

Juliet Lodge Papers and evidence to:

European Parliament, national parliaments, data supervisors etc

- EU freedom, security and justice, Europol, automated decisionmaking and data exchange, border management and controls, security, biometrics, ethical standards, procedures, management, compliance with law & democracy
- Parliamentary powers, transparency, legitimacy , accountable egovernance in security and internal market of EU27
- Fp6 (Challenge; r4eGov; ejustice) f7p ICT Ethics; BEST;
- Advisory role in fp6 RISE;HIDE (& f6p Mediated Citizenship)
- EU-China programme (EU funded on multilateralism and soft diplomacy); 17+ books; 240 published peer reviewed papers
- EU citizenship in e-digital spaces