Australian Government
Australian Institute of Criminology

Crime Control in the Digital Age
Human Rights Implications

Russell G Smith
presented by Kiah McGregor

Introduction

The "Digital Age"

- Information and communications technologies (ICT) which make use of data streams and 1s and 0s, transmitted by wire or radio waves

New Crimes

- Hacking, viruses, phishing, spam, encryption, cyber-stalking, online piracy

New Solutions

- Neural networks, biometrics, imaging, data-matching, encryption, surveillance, e-courtrooms, electronic monitoring

Human rights concerns (and benefits)

- From government legislation and activities
- From corporations and other citizens

Focus on cybercrime and criminal justice agency responses

What are Human Rights?

United Nations instruments

- Universal Declaration of Human Rights (1948)
- International Covenant on Civil and Political Rights (1966)
- International Covenant on Economic, Social and Cultural Rights (1966)
- Optional Protocol to the International Covenant on Civil and Political Rights (1966)

Conventions and constitutional documents

- European Convention for the Protection of Human Rights and Fundamental Freedoms
- United States Constitution
- Canadian Charter of Rights and Freedoms
- Magna Carta (1215)
- Declaration of Rights (1689)

Some Australian sources

- Human Rights and Equal Opportunity Commission Act 1986 (Cth)
- Cybercrime Act 2001 (Cth)
- Human Rights Act 2004 (ACT)
- Human Rights Commission Act 2005 (ACT)

What Human Rights are at Risk in the Digital Age?

Human Rights	Sources of Possible Derogation
Human freedom and dignity *(UDHR art 1,* *ICCPR art. 10)*	Surveillance (listening devices, CCTV) DNA analysis Data matching by government agencies Identity smart cards Electronic tagging of offenders
Freedom from discrimination *(UDHR art 2, ICCPR art. 26)*	Cyber racism Computer addiction
Freedom of thought and expression *(UDHR art 18, 19,* *ICCPR art 18, 19)*	Maintenance of databases Surveillance and listening devices Spam / Denial of service attacks Online content restrictions

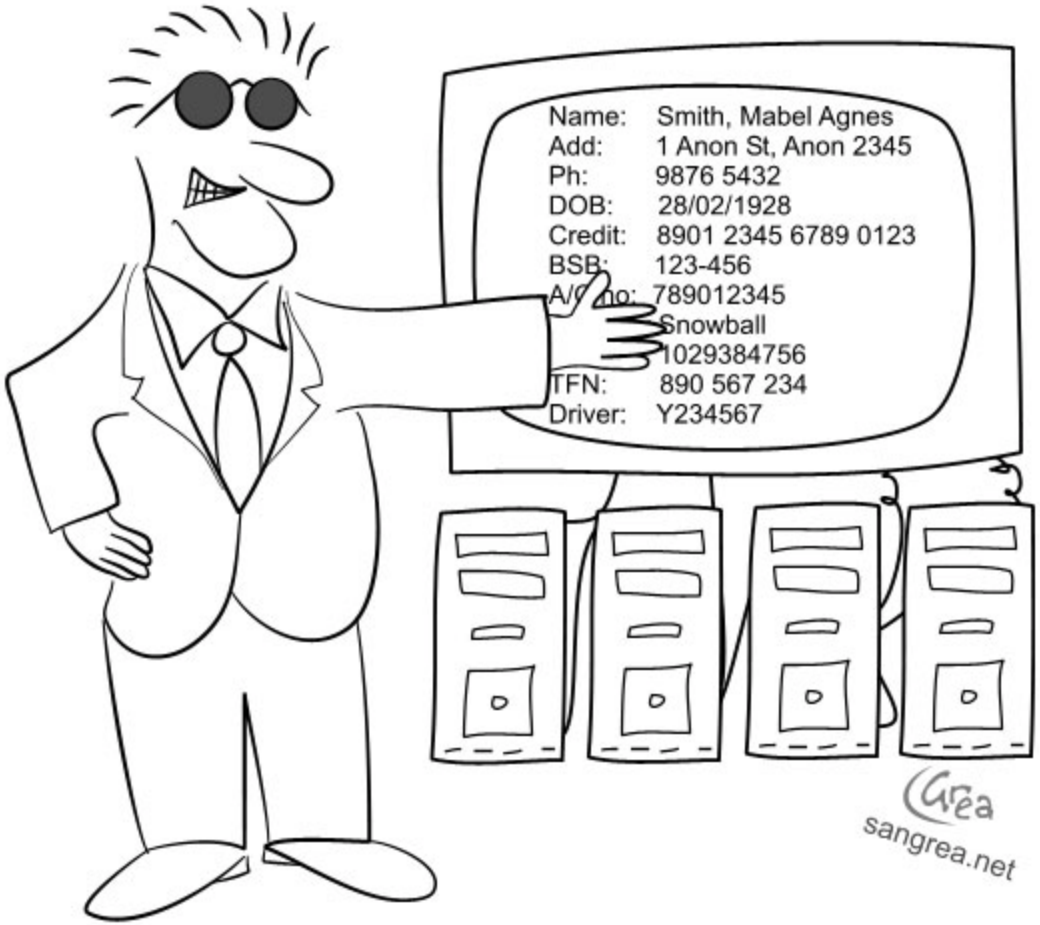
What Human Rights are at Risk in the Digital Age cont.?

Human Rights	Sources of Possible Derogation
Right to bodily security and freedom from inhuman punishments *(UDHR 3, 5, ICCPR 7)*	Electronic tagging of offenders Embedded computer chips in humans Biometric identification
Right to a fair trial, presumption of innocence, freedom from self-incrimination *(UDHR 11, ICCPR 9, 14)*	Disclosure of encryption keys / passwords Use of electronic evidence in court Co-mingling of electronic evidence Juror access of online information
Right to own property and protect intellectual property *(UDHR art 17, 27.1)*	Digital piracy Computer hacking Electronic espionage

What Human Rights are at Risk in the Digital Age cont.?

Human Rights	Sources of Possible Derogation
Right to privacy *(UDHR art 12, ICCPR art 17)*	Electronic surveillance (e.g. CCTV) Maintenance of databases Data matching by government agencies Identity smart cards e-commerce marketing and spam
Right to life *(UDHR art 3, ICCPR art 6)*	Cyber terrorism Capital punishment for cybercrime
Right to participate in government and vote *(UDHR art 21, ICCPR art 25)*	Online indoctrination Electronic surveillance Digital monopolies Invasions of privacy Surveillance of electronic voting activities

Examples of Potential Human Rights Infringement in the Digital Age



Hey, wanna buy some data? Only slightly used! Heap of clicks left in it. Its last owner was a little old lady who only used it for shopping ...

The charming simplicity of Australian privacy law

Privacy

- Legislatively protected in Australia

  E.g. Privacy Act 1988 (Cth), Privacy Amendment (Private Sector) Act 2000 (Cth), and state legislation

- Monitoring of computer useage
- Collection of communications traffic data by IPSs and carriers

  E.g. Council of Europe *Convention on Cybercrime* art. 20-21

Privacy cont.

Concerns from electronic identity cards and data-matching

Privacy cont.

Risks from biometric technologies

- Gathering biometrics without permission
- Function creep
- Sharing information without permission
- Amalgamating information across databases

Additional protections required


C-could I buy some security p-p-please?
Of course, sir. That will cost you 5 privacies.
I ♥ BB
sangrea.net

Search and Seizure and Criminal Trials

- Legislative requirements to disclose encryption keys to police

  e.g. *Criminal Code Act 1995* (Cth) s. 3LA,
  Customs Act 1901 (Cth) s. 201A
- Potential infringement of the right to a fair trial, the presumption of innocence, and freedom from self-incrimination *(UDHR art. 11, ICCPR arts. 9, 14)*
- Police use of "key-stroke logging" to obtain evidence

  e.g. *United States* v *Gorshkov and Ivanov* (2001)
- Potential infringement of USA Fourth Amendment right against unreasonable search and seizure
- Co-mingling of evidentiary data
- Access to online information by jurors

Discrimination

- Internet crime caused by mental disorder

  e.g. *Re Seneca College and Ontario Public Service Employees Union*, (Ontario, 2002)

Freedom of Thought and Expression

- Surveillance of email and mobile phone calls
- Dissemination of spam, denial of service attacks
- Dissemination of racist material online
  e.g. *Jones* v *Toben* (HREOC, Federal Court 2001-2)
- Obscene and defamatory materials
- The need to balance competing rights
- USA 1st Amendment right to free speech
  e.g. *United States* v *Mitnick* (US Court of Appeal 1998)
- Infringement of the right to vote where online voting systems used

Cruel and Unusual Punishment

- Capital punishment for online crime
  - e.g. Chinese hacker sentenced to death
- Electronic monitoring of offenders
  - Must comply with legislation and *Standard Guidelines for Corrections*
- Computer chips embedded beneath the skin
- Control orders for terrorist suspects
  - e.g. *Criminal Code Act* 1995, Division 104.

Preventing Human Rights Abuses

- Enactment of compliant legislation
- Assess human rights implications of new technologies before they are created

  The longer a technology is used, the more entrenched in life it becomes. When technologies are new, or are used in newer ways... their uses are easier to modify and their consequences easier to control. If we wish to question the unintended consequences of these developments, now is the time to do so (Casella 2003)
- Development of technological protections in hardware and software
- Conduct evaluative research
- Publicise infringements

Questions or comments?

Russell.Smith@aic.gov.au