

# Data Protection, Privacy & Anonymization: Definitions, Standards & Rights

Carole Lucock, LLB, LLM

LLD candidate

Faculty of Law, University of Ottawa

# Roadmap

- Data Protection, Privacy, Anonymity: Definitional/Conceptual Issues
- Right of Control Concerning the *Act* of Anonymizing
- Rights Concerning Information that has been Anonymized

## Definitional/Conceptual Issues: Identifiability

- “identifiability” is gatekeeper concept re: whether information is protected or not
  - ✓ Data Protection Legislation
  - ✓ Ethics Codes & Guidelines

## Definitional/Conceptual Issues: Reasons for De-identification?

- a) to preserve privacy
- b) to remove information from jurisdiction of legislation/ethics codes, guidelines

## Definitional/Conceptual Issues: Sufficiently Anonymised?

- Risk of re-identification (Latanya Sweeney)
- Grades of identifiability (CIHR Guidelines)
- Approaches:
  - UK Data Commissioner
  - US HIPA

## Right of Control Concerning Act Of Anonymizing

- Is the *act* of anonymizing personal information governed by data protection legislation/ethics codes, guidelines?
- Consent/control is at issue in legislation/codes/guidelines in case of *processing* and *use*
- Is act of anonymizing processing? A use?
  - Source Informatics

## Rights Concerning Information that has been Anonymized

- Pragmatic/Practical Concern re: risk of Re-Identification
  - Who decides how much risk is acceptable?
  - Disclosure of risk? Consent to accept the risk?
- Adverse impact on group or community

## Rights Concerning Information that has been Anonymized

- Standard definition of informational privacy: “Right to control what happens to our information” Westin
  - Right engaged even if zero risk of reidentification;
  - Right engaged even if no potential adverse impact on individuals or group;
  - Cases: Class clicks; Abortion records