

Data Protection

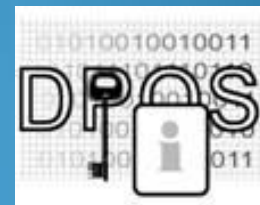
An Appropriate Framework For Personal Information Ethics?

David Erdos

Centre for Socio-Legal Studies, Faculty of Law
University of Oxford

david.erdos@csls.ox.ac.uk

<http://www.csls.ox.ac.uk/dataprotection>



Background & Research Question

- Part of broader three-year project on **Data Protection and the Open Society (DPOS)**.
- Asking a very focused question:

Is **Data Protection (DP)** a good framework for treating personal information ethically?

- Related to two other distinct questions :

Does legal enforcement of DP lead to more ethical use of personal information?

Can ethical theory help frame a better DP law?

Overview

1. Briefly introduce **Data Protection (DP)**
2. Examine reasons why might DP might be ethically useful from **internal** and **external** perspective.
3. Explore **ethical problems** with **core structure** of DP.
4. Explore **ethical problems** with DP's **special purpose provisions (in private sector)**
5. Look at **deeper reasons** why DP is inadequate ethically and offer some **final conclusions**.

What is Data Protection?

- Body of law regulating the use (and potential misuse) of **personal data (i.e. information being processed)**
- Developed from late 1960s onwards with origins in **Council of Europe (CoE)** and the **EU**:
 - **1968** CoE Parl. Assembly Recommendation 509
 - **1973-4** CoE Resolutions on private & public sector
 - **1981** CoE Convention 108 on personal data protection
 - **1995** EU Data Protection Directive 95/46/EC
- Going to focus on **Directive 95/46/EC** especially as transposed in UK law via **Data Protection Act 1998**.

Structure of Data Protection (Act 1998)

1. Fair and Lawful Processing
2. Limited, specified and compatible purposes

3. Relevant (adequate and not excessive)
4. Time limited
5. Accurate (and where relevant up-to-date)
6. Subject' Rights Adherence

7. Secure
8. No export without “adequate protection”

- Plus **purpose specific provisions** limiting the above.

DP as a Ethical Frame: Internal Evidence

1. **Focus** – Misuse of data

2. Grounding in **principles**

3. **Origins**: Ethical debate & Voluntary Guidelines
(Younger Committee, 1972)

3. **Good practice** focus remains important
(s. 51 (1-2)), DPA 1998)

DP as a Ethical Frame: External Evidence

- **Broad theories** of privacy risen to fore & **chime** with DP:

1. Solove's **pragmatic taxonomy** of privacy problems (2008)

2. Nissenbaum's augmented **contextual integrity** theory (2010)

3. Mayer-Schönberger's **Delete** develops from third DP principle (time limitedness) (2009)

- But does **jar** with more traditional narrower theories:

4. Inness' theory of privacy as **intimacy** (1992)

DP Problems at Core – Personal Data

“any information concerning [or which “relates to”] an identified or identifiable person” (s. 26 Dir. 95/46/EC)

- Interpreted very broadly:

“the question of whether the data are “public” or “private”, however these terms are defined, has no bearing...this is a matter of law, not common sense” (UK Library Assoc. 1985)

- Endorsed during drafting of Dir. 95/46/EC and subsequent decisions of ECJ also conform to this:

e.g. Satamedia (2008)

DP Ethical Problems – General

- Specific problem with personal data definition:

“there is a significant amount of information identifiable to us that we do not deem as private...[it]provides **no reasonable limitation** in scope” (Solove, 2008)

- Perhaps reflects a **broader hubris** in approach?

In this vein, Nissenbaum generally rejects **omnibus** DP approach – difficult to embody information norms relevant to “specific sectors” through this - US **sector specific** approach “**may be the more promising one**” (2010)

DP Problems at Core: Transparency (1, 2, 6)

1. Necessary for **data controllers** to place name, address etc. on **register** or **available on request** (A. 48 & A 21 Dir.)

2008: Photojournalist prosecution; NUJ concern about privacy and safety.

2. Necessary to provide data subjects with **fair information notice** when data collected/processing (A. 38, Dir.)

Jay to Socio-Legal Studies Assoc.: covert/deception research “almost certainly” illegal (2004)

3. Necessary to provide data subjects with **full information** about data and processing concerning them.

U Birmingham to staff & students: “**all** emails must be disclosed to person about whom they are written” (2009)

DP Problems at Core: Sensitive Data

Sensitive Data definition **problematic** – **broad** and **categorical**

Any information as to:

- racial/ethnic origin
- political opinion
- religion (or similar)
- trade union membership
- health or condition
- anything do with crime (including allegations and proceedings)

Extremely restrictive special regime:

• **Default is prohibition**

“Member States shall prohibit the processing of [sensitive] personal data” (A. 8 (1), Dir)

• **Exceptions narrowly tailored and onerous.**

DP Purpose Specific Sols?: General

JOURNALISM, LITERATURE AND ART

“Member States shall provide for exemptions or derogations from the [main] provisions [of the Directive] for the processing of personal data carried out **solely for journalistic purposes or for the purposes of artistic or literary expression** only if they are necessary to reconcile the right to private with the rules governing freedom of expression.” (A. 9, Dir. 5/46/EC)

HOUSEHOLD PURPOSES

“This Directive shall not apply to the processing of personal data....by a **natural person** in the course of a **purely personal or household activity**.” (A. 2, Dir. 95/46/EC)

DP Purpose Problems: JLA

1. JLA held to apply to **material published in newspapers**
2. But generally not to **academic research**

Severe restrictions on academic activity & spread of **audit culture** in academic institutions.

3. Or to **social speech**:

Quinton v. Pierce (2009) High Court (Eady J)

- Politician's election leaflet held not to be within JLA

United Food and Commercial Workers', Local 401 (Alberta PIPA) (2009)

- Production of picket line video could not claim JLA exemptions

DP Purpose Problems: Household Purposes

Household

- Household use totally exempt from DP.
- Covers:
 - Self-selected Friends ✓
 - Friends of Friends [?]
 - Publication ✗

Data disclosed to
“**indeterminate number** of
persons” excluded (Common
Position, 1995 & Lindqvist,
2003)



Public

- Exclusivity of JLA means generally inapplicable.

Van Alsenoy et. al. find:

- need for **unambiguous consent** to process,
- obligation to **remove on request**
- obligation to be **open about real identity**

- Some enforcement esp. in Spain, Italy and Norway.

DP: Key Ethical Failures

1. Failure to take into account the rights of **Data Controllers**

DP is **out of date!**

2. **General rules** governing data processing **over restrictive** in some cases.

DP reflects **emotional not rational response** to data challenges
(Bergkamp, 2002)

3. Special purpose provisions also often **narrow** and **arbitrary**.

DP attempts to provide an unfeasible general rigid (yet underspecified) **code for data processing**

Some final conclusions

- DP flags a **wide-range of issues** which need consideration from ethical point of view.
- On other hand, **code-like** baggage of DP prevents necessary **balancing** between values.

“We live in an “age of balancing”...Because privacy conflicts with other fundamental values...we should engage in a candid and direct analysis of why privacy interests are important and how they ought to be reconciled with other interests.” (Solove, 2008)

- Need to **return to first principles** in order to construct a coherent ethical and legal framework.