The Trouble with European Data Protection Law

Prof. Bert-Jaap Koops

e.j.koops@uvt.nl

Tilburg University

TILT
Tilburg Institute for Law, Technology, and Society

ALFRED HITCHCOCK'S

THE TROUBLE WITH HARRY

Color by TECHNICOLOR

VISTAVISION

starring

EDMUND GWENN

JOHN FORSYTHE

and introducing

SHIRLEY MacLAINE

Directed by

ALFRED HITCHCOCK

Screenplay by

JOHN MICHAEL HAYES

Based on the Novel by

JACK TREVOR STORY

A PARAMOUNT PICTURE

COUNTRY OF ORIGIN U. S. A.

Outline

- data protection reform
- fallacy 1: too much focus on informational self-determination
- fallacy 2: too much faith in controller actions
- fallacy 3: regulating everything in one statutory law
- conclusion: what to do with Harry?

Data protection reform

Objectives

1.4.1. The Commission's multiannual strategic objective(s) targeted by the proposal/ initiative

The reform aims at completing the achievement of the original objectives, taking account of new developments and challenges, i.e.:

- increasing the effectiveness of the fundamental right to data protection and putting individuals in control of their data, particularly in the context of technological developments and increased globalisation;
- enhancing the internal market dimension of data protection by reducing fragmentation, strengthening consistency and simplifying the regulatory environment, thus eliminating unnecessary costs and reducing the administrative burden.

In addition, the entry into force of the Lisbon Treaty - and in particular the introduction of a new legal basis (Article 16 TFEU) - offers the opportunity to achieve a new objective, i.e.

- to establish a comprehensive data protection framework covering all areas.

source: Proposal for a General Data Protection Regulation, COM(2012) 11 final, p. 102

Data protection reform

Objectives

1.4.1. The Commission's multiannual strategic objective(s) targeted by the proposal/ initiative

The reform aims at completing the achievement of the original objectives, taking account of new developments and challenges, i.e.:

- increasing the effectiveness of the fundamental right to data protection and putting individuals in control of their data, particularly in the context of technological developments and increased globalisation;
- enhancing the internal market dimension of data protection by reducing fragmentation, strengthening consistency and simplifying the regulatory environment, thus eliminating unnecessary costs and reducing the administrative burden.

In addition, the entry into force of the Lisbon Treaty - and in particular the introduction of a new legal basis (Article 16 TFEU) - offers the opportunity to achieve a new objective, i.e.

- to establish a comprehensive data protection framework covering all areas.

source: Proposal for a General Data Protection Regulation, COM(2012) 11 final, p. 102

Data protection reform

Objectives

1.4.1. The Commission's multiannual strategic objective(s) targeted by the proposal/ initiative

The reform aims at completing the achievement of the original objectives, taking account of new developments and challenges, i.e.:

- increasing the effectiveness of the fundamental right to data protection and putting individuals in control of their data, particularly in the context of technological developments and increased globalisation;
- enhancing the internal market dimension of data protection by reducing fragmentation, strengthening consistency and simplifying the regulatory environment, thus eliminating unnecessary costs and reducing the administrative burden.

In addition, the entry into force of the Lisbon Treaty - and in particular the introduction of a new legal basis (Article 16 TFEU) - offers the opportunity to achieve a new objective, i.e.

- to establish a comprehensive data protection framework covering all areas.

source: Proposal for a General Data Protection Regulation, COM(2012) 11 final, p. 102

Data protection reform

Objectives

1.4.1. The Commission's multiannual strategic objective(s) targeted by the proposal/ initiative

The reform aims at completing the achievement of the original objectives, taking account of new developments and challenges, i.e.:

- increasing the effectiveness of the fundamental right to data protection and putting individuals in control of their data, particularly in the context of technological developments and increased globalisation;
- enhancing the internal market dimension of data protection by reducing fragmentation, strengthening consistency and simplifying the regulatory environment, thus eliminating unnecessary costs and reducing the administrative burden.

In addition, the entry into force of the Lisbon Treaty - and in particular the introduction of a new legal basis (Article 16 TFEU) - offers the opportunity to achieve a new objective, i.e.

- to establish a comprehensive data protection framework covering all areas.

source: Proposal for a General Data Protection Regulation, COM(2012) 11 final, p. 102

Fallacy 1: too much focus on information self-determination

- starting point of ISD has two main components:
  - consent as an important (or primary) legitimating ground
  - data subject rights
- problem 1: mythology of consent
- problem 2: exercising control of data is extremely difficult
- problem 3: ISD does not work in the public sector
- conclusion
  - there is little informational self-determination in the private sector
  - informational self-determination is at odds with the public sector
  - fallacy of relying on ISD and focusing on user empowerment

Fallacy 2: too much faith in controller actions

- problem 1: data protection law is pretty complex
- problem 2: more *ex ante* obligations… on paper
- problem 3: more *ex post* regulation… on paper
- conclusion
  - complexity of the law is increasing instead of decreasing
  - more *ex ante* and *ex post* paperwork and checklist obligations
  - controllers will likely be rule-compliant without understanding much about data protection
  - fallacy of creating more rules leads to data protection law being a zombie: it seems to live, but lacks a vital spirit

Fallacy 3: regulating everything in one statutory law

- problem 1: huge disconnect between law and reality
- problem 2: response to regulatory disconnection is… more of the same law
- problem 3: data protection has a communication problem
  - wrong frame
  - poor expectation management
  - underlying: too narrow focus on command-and-control law
- conclusion
  - regulatory disconnection will only be enlarged by stretching the scope of data protection law
  - too little attention for other regulatory tools
  - fallacy of believing every problem of Internet data flows can be addressed by data protection law

Conclusion

What do to with Harry?

"The trouble with Harry is that he's dead, and everyone seems to have a different idea of what needs to be done with his body..."

(synopsis of Alfred Hitchcock, *The Trouble with Harry*, 1955)

The future of data protection law
(if it is to have a future)

- the reform: 'a comedy about a corpse'

The future of data protection law
(if it is to have a future)

- the reform: 'a comedy about a corpse' or a zombie horror movie?

source: http://www.fanpop.com/clubs/zombie-movies/images/6425644/title/zombie-photo

The future of data protection law
(if it is to have a future)

- the reform: 'a comedy about a corpse' or a zombie horror movie?
- with the current reform objectives, data protection law is moribund or dead
- what to do with data protection law's body?
  - resurrect
    - going back to the roots – a framework of basic principles
    - showing the *spirit* of data protection, not the rules – the forest, not the trees
    - investing in DPA resources
  - or R.I.P. and look for protection elsewhere
    - sui generis frameworks for particular challenges, e.g. profiling
    - consumer protection, administrative law, public procedure law
    - regulating decision-making
  - and/or commemorate and keep its spirit alive
    - role models
      - administrations and regulators showing data collection restraint
      - (really) adopt Privacy Enhancing Technologies and privacy by default

Thank you for your attention

B.J. Koops, 'The Trouble with Data Protection Law',
International Data Privacy Law, doi:10.1093/idpl/ipu023,
http://idpl.oxfordjournals.org/content/4/4/262.full.pdf+html / http://ssrn.com/abstract=2505692

Time for discussion

follow-up questions and suggestions: e.j.koops@uvt.nl

Tilburg University

Back-up slides

Fallacy 1

too much focus on informational self-determination

Informational self-determination

- an important precondition ‘for ensuring that individuals enjoy a high level of data protection’ is ‘the retention by data subjects of **an effective control over their own data**’

European Commission, 'A Comprehensive Approach on Personal Data Protection in the European Union‘ (Brussels: European Commission, 2010), p. 7 (emphasis in original)

- two main components
  - consent as a legitimating ground
  - data subject rights

Problem 1: the mythology of consent

- consent is one of the main (although not only) legitimating grounds for data processing, ensuring data subject control
  - particularly in the private sector
- but consent has no practical meaning
  - just ticking boxes
  - not understanding consequences
  - bounded rationality
  - not having a real choice
  - practical limitations
- there is a trade-off between practical consent and meaningful consent
- can ticking a consent box really ‘ensur[e] that individuals are aware that they give their consent to the processing of personal data’ (recital 25)?

Problem 2: exercising control over data is extremely difficult

- welcome to the 21st century: large-scale databases, Big Data, profiling
- the complexity of data processing:
  - multiple data controllers and processors
  - data sharing practices
  - multiple, often fuzzy, purposes
  - automated operations on data
- exercising data subject rights to
  - be informed: need to know where to look and how to read
  - request information: need to know this right and to make controller comply
  - request correction or erasure: need to know whom to ask
- do you actually know which of your data are being processed in what ways by which data controllers, and do you think you have effective control over most data-processing operations you are subjected to?

Problem 3: ISD does not work in public sector

- can, or should, citizens exercise effective control over how the government processes their data?
  - consent can not be an important legitimating ground
    - what is there to choose?
  - data subject rights apply only to some basic standards of fair processing (e.g., data accuracy)
  - but there is no control over
    - the purpose of data processing
    - the means of data processing
- calling the exercise of rights to be informed, access, correction and, perhaps, erasure in citizen-government relations ‘having control over one’s information’ is a travesty of the word ‘self-determination’

Conclusion

- there is little informational self-determination in the private sector
- informational self-determination is at odds with the public sector
- fallacy of relying on ISD and focusing on user empowerment

Fallacy 2
too much faith in controller actions

Problem 1: data protection law is pretty complex

- evaluations of Dutch Data Protection Act (1995; 2007-2008)
  - lack of clarity and vagueness of concepts and open-ended terminology
  - general, comprehensive character causes problems to understand concrete obligations
  - a complex law for specialists
- can controllers make sense of the regulatory obligations?
  - data protection law triples
    - DPD 34 articles, 12,500 words
    - GDPR 91 articles, 35,000 words
  - interlocking constructions
    - e.g., right to erasure of article 17(1)(c) applies when data subjects object on the basis of article 19, which refers to the grounds of article 6(1)(d-f), except when article 80, 81, 83 or 17(4) apply, the latter being the case when for example article 18(2) applies; and the Commission can adopt further rules to specify the criteria and requirements pertaining to all this for specific sectors and situations

Problem 2: more *ex ante* obligations

- the DPD: prevention of unnecessary data processing
  - really? I don't see it in practice
- GDPR: more preventive measures
  - Data Protection Impact Assessment
  - data protection by design and by default
- how many controllers will seriously limit the envisioned data processing on the basis of a DPIA?
  - works only if data protection is perceived not as an obstacle but as an asset
  - how can we reach the hearts and minds of data controllers?
    - carrots rather than sticks, but GDPR focuses more on sticks
- high risk that DPIAs will only be paper exercises that do not change practices

Problem 3: more *ex post* regulation

- reduction of administrative burdens?
  - some are taken away, but more others are imposed
- strong focus on accountability and oversight
  - 'be able to demonstrate that the processing of personal data is performed in compliance with this Regulation' (art. 22)
  - keep documentation (art. 28)
- often focused on formalities rather than spirit of data protection
  - accountability only works if controllers have a *data protection rationale* mindset, rather than a data protection *rule* mindset
- enforcement by DPAs
  - will DPAs be able to enact effective oversight?

Conclusion

- complexity of the law is increasing instead of decreasing
- more *ex ante* and *ex post* paperwork and checklist obligations
- controllers will likely be rule-compliant without understanding much about data protection
- fallacy of creating more rules leads to data protection law being a zombie: it seems to live, but lacks a vital spirit

Fallacy 3
regulating everything in one statutory law

Problem 1: disconnect between law and reality

- recital 30:

  'The data should be adequate, relevant and limited to the minimum necessary for the purposes for which the data are processed; this requires in particular ensuring that the data collected are not excessive and that the period for which the data are stored is limited to a strict minimum. Personal data should only be processed if the purpose of the processing could not be fulfilled by other means.'

- article 23(2)

  'The controller shall implement mechanisms for ensuring that, by default, only those personal data are processed which are necessary for each specific purpose of the processing and are especially not collected or retained beyond the minimum necessary for those purposes, both in terms of the amount of the data and the time of their storage.'

- have a look at reality
  - how many databases contain your data? and how many of your data?
  - Big Data, 'the new oil'?
- who dares to claim that a principle of data minimisation exists in reality?

Problem 2: response to regulatory disconnection is… more of the same law

- the scope of data protection law expands
  - online identifiers
    - R-identifiers (recognition) rather than L-identifiers (look-up)
    - should they have the same regime as L-identifiers?
  - profiling
    - does this regulate creating profiles based on non-identifiable persons?
      - » yes: natural persons have the right not to be subjected to decisions based solely on profiling (art. 20(1))
      - » no: rest of art. 20 talks about 'data subjects' and 'controllers'
      - » no: the scope of GDPR is 'the processing of personal data' (art. 2)
  - data portability
- underlying problem: most Internet-related problems are seen through lens of data protection, not through other possible lenses
  - fair data processing (administrative law, unfair business practices)
  - consumer protection law
- as a result, to cover new issues data protection law is stretched so much that it risks becoming void of meaning

Problem 3: data protection has a communication problem

- data protection is often seen as an obstacle
  - data protection *restricts*, rather than *enables*
- reframing is needed: data protection canalises rather than prohibits data processing
  - but focusing on sticks instead of carrots will not help reframing
- poor expectation management
  - the false suggestion of creating 'control' over one's personal data
  - the 'right to be forgotten' label
- underlying problem: too narrow focus on (command-and-control) law
  - using technology ('code'), but through legal obligations
  - self-regulation ('consensus') is stimulated, but only within a strong legal framework; and so far hardly works
  - competition and communication are underdeveloped tools in data protection

Conclusion

- existing regulatory disconnection
- will be enlarged by stretching the scope of data protection law
- too narrow focus on command-and-control law
- fallacy of believing every problem of Internet data flows can be addressed by data protection law