

# Data Subject Rights & Data Controller Obligations

Bart Custers PhD MSc LLM  
Associate professor/head of research  
eLaw – Center for Law and Digital Technologies  
Leiden University – The Netherlands

INFORM WORKSHOP  
Leiden University  
3<sup>rd</sup> December 2018  
16:30-17:30



INTRODUCTION OF THE DATA PROTECTION  
REFORM TO THE JUDICIAL SYSTEM  
**INFORM** 



Universiteit Leiden

# Contents

- The value of personal data
  - What is happening with my data?
- Data subject rights
  - What rights do you have?
- Data controller obligations
  - How else are you protected?
- Conclusions, wrap-up



# The value of personal data

What is happening with my data?

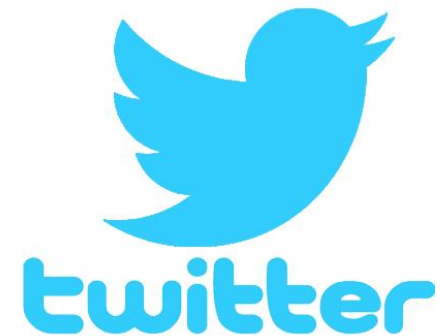
# The data economy

- Whom of you is using any of these service?



# The data economy

- Have you ever wondered why these and other services are for free?



# The data economy

- Have you ever wondered why these and other services are for free?



# There is value in (your) data...

- A variety of business models:
  - Targeted advertising
  - Digitalization, efficiency, cost saving
  - Discovering/entering new markets
  - Extract value from data via analyses
    - Discovery of novel patterns
  - Selling/trading/leasing data
    - Raw data
    - Information
    - Knowledge



# What is in it for consumers?

## Incentives for disclosing personal data



- Monetary
  - Free stuff: digital content, digital service, offline service, etc.
  - Discounts
- Non-monetary
  - Counter services, increased functionality
  - No incentives (sometimes: no choice)



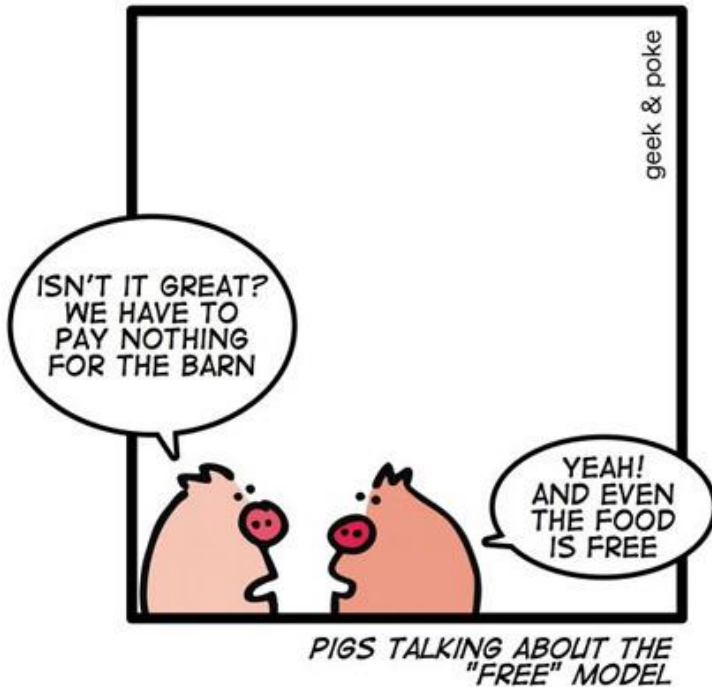
**Table 1 – Examples of companies using different business models based on different transaction structures and different use cases.**

Provision \ Incentives	Monetary		Non-monetary	
	Savings	Earnings	Personalization	No incentives
Digital Content	Spotify		Spotify	iTunes
Digital Service	Wi-Fi in public spaces, Antivirus	Brave	Google, Facebook	Groupon
Offline Service	Hancock insurance	Handshake	Experian	Traditional insurance, etc.



# For free, right?

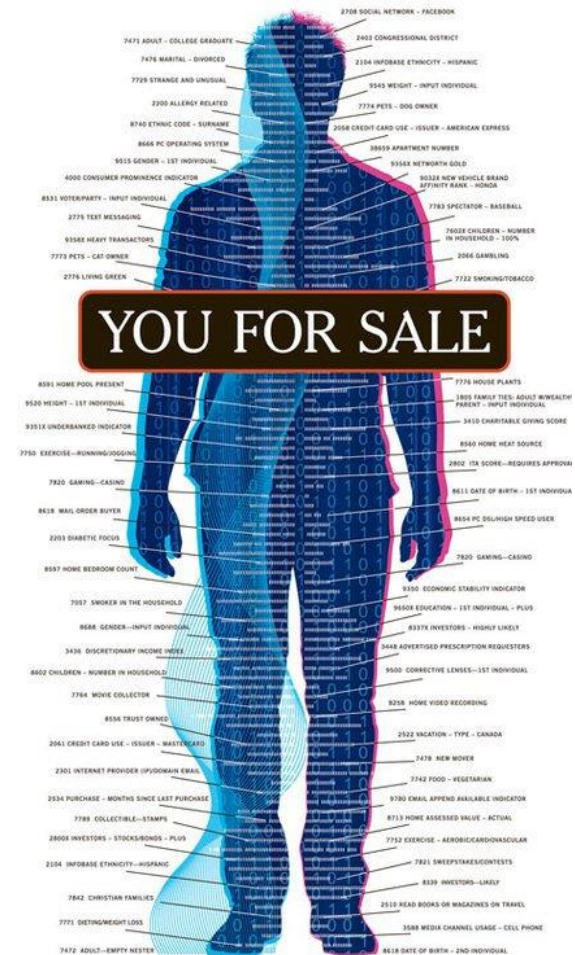
So: For Free  $\neq$  For free...



IF IT'S FREE  
THE PRODUCT  
IS **YOU**

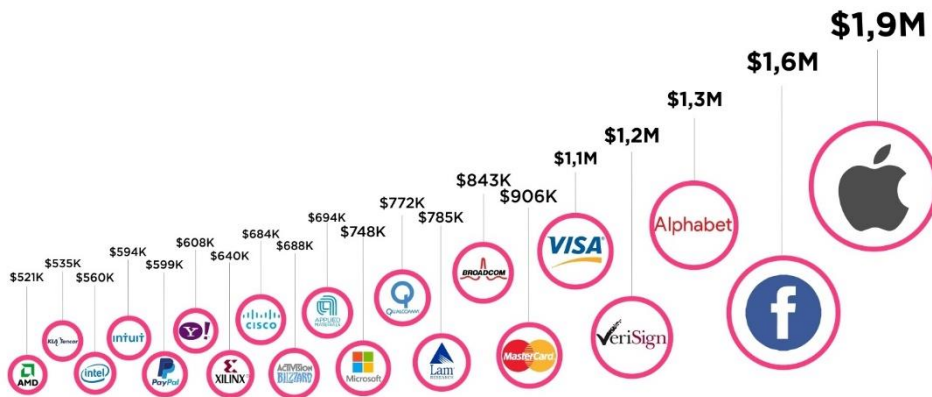
# The value of your data

- What is your data worth?
- **Standard ads ~0,01 cent**
- Personal advertising is worth roughly 10 times more than standard advertising
- **0,05 cent to 0,1 cent each**
- Average user: ~100 ads/day
- **Revenue: \$1-\$3 per month**



# The value of your data

Another way to calculate the value of your data:



Market value : number of users = value per user

# The right to know?

- The right to know the value of your personal data...



... does not exist in EU data protection law

- But may contribute to:
  - Increased transparency
  - Increased fairness
  - Increased control - informational self-determination



# The right to know?

## complications:

- Practical problems
  - Which pricing model? who should do the pricing?
  - Supervision/enforcement? Some data is already public.
- Moral problems
  - Commodification of privacy (human right)
  - Some data more valuable (social segregation, ex ante discrimination)
- Cognitive problems
  - Taking notice, understanding information
  - Social pressure



# Read more?

- More on the right to know the value of your personal data:



Available online at [www.sciencedirect.com](http://www.sciencedirect.com)

ScienceDirect

[www.compseconline.com/publications/prodclaw.htm](http://www.compseconline.com/publications/prodclaw.htm)

Computer Law  
&  
Security Review

## Pricing privacy – the right to know the value of your personal data

Gianclaudio Malgieri <sup>a,\*</sup>, Bart Custers <sup>b</sup>

<sup>a</sup> Law, Science, Technology and Society studies (LSTS), Vrije Universiteit Brussel, Belgium

<sup>b</sup> eLaw, Center for Law and Digital Technologies, Faculty of Law, Leiden University, The Netherlands

**Keywords:**  
Privacy  
Personal data  
Data subject rights  
Big data  
Digital identities  
Data economy

### ABSTRACT


The commodification of digital identities is an emerging reality in the data-driven economy. Personal data of individuals represent monetary value in the data-driven economy and are often considered a counter performance for "free" digital services or for discounts for online products and services. Furthermore, customer data and profiling algorithms are already considered a business asset and protected through trade secrets. At the same time, individuals do not seem to be fully aware of the monetary value of their personal data and tend to underestimate their economic power within the data-driven economy and to passively succumb to the propertization of their digital identity. An effort that can increase awareness of consumers/users on their own personal information could be making them aware of the monetary value of their personal data. In other words, if individuals are shown the "price" of their personal data, they can acquire higher awareness about their power in the digital market and thus be effectively empowered for the protection of their information privacy. This paper analyzes whether consumers/users should have a right to know the value of their personal data. After analyzing how EU legislation is already developing in the direction of propertization and monetization of personal data, different models for quantifying the value of personal data are investigated. These models are discussed, not to determine the actual prices of personal data, but to show that the monetary value of personal data can be quantified, a *conditio-sine-qua-non* for the right to know the value of your personal data. Next, active choice models, in which users are offered the option to pay for online services, either with their personal data or with money, are discussed. It is concluded, however, that these models are incompatible with EU data protection law. Finally, practical, moral and cognitive problems of pricing privacy are discussed as an introduction to further research. We conclude that such research is needed to see to which extent these problems can be solved and mitigated. Only then, it can be determined whether the benefits of data

# Data subject rights

What rights do you have?



# Data subject rights – overview

## GDPR – Chapter III

- Right to transparent information (art. 12)
  - Data obtained directly from the data subject (art. 13)
  - Data obtained indirectly from the data subject (art. 14)
- Right of access (art. 15)
- Right to rectification (art. 16)
- Right to erasure (right to be forgotten) (art. 17)
- Right to data portability (art. 20) 



## GDPR – Chapter VIII

- Right to lodge a complaint at supervisory authorities (art. 77)
- Right to an effective remedy
  - Against supervisory authority (art. 78)
  - Against controller/processor (art. 79)
- Right of representation (art. 80) 
- Right to compensation (art. 82) 



# Data privacy => control

- Data privacy as control

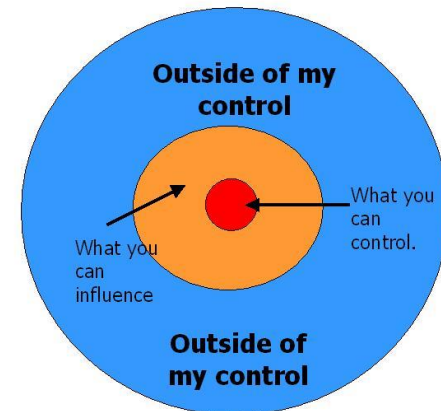
informational self-determination (Westin, 1967)

People control who gets their data and for which purposes

- Control:
  - Transparency
  - Consent
  - Other data subject rights

Consent => informed consent

## The 3 Spheres of Control



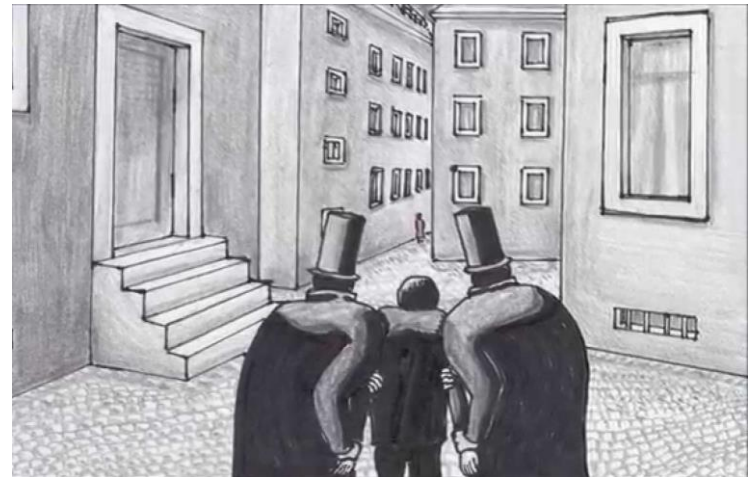
# Right to transparent information

In how many databases  
are your data?

- Which data?
- What kind of analysis?
- What kind of decision-making?



Big Brother?



Kafka?

# Right to transparent information

## Consent: make your own decisions...

- Privacy policies (Solove, 2013)
  - Few people read these
  - Even fewer people understand these
  - Even fewer people grasp consequences
  - Preferred options are often missing
- What information to provide?
  - Data controller identity, purposes, legal basis, recipients, third country transfers, duration of storage, etc.
- How to provide information?
  - Concise, transparent, intelligible, easily accessible, clear and plain language



# Access, rectification and erasure

## ■ Access

- In how many databases are your data?

## ■ Rectification

- In case of inaccurate data

## ■ Erasure (right to be forgotten)

(Also see the Google Spain Case)

- When data is no longer necessary
- When consent is withdrawn



### Practical issues:

- Awareness about who collects/processes their data
- Awareness about data subjects rights
- Awareness about how to enforce your rights

# The Google Spain case

- Meet Mario Costeja Gonzales...



- Bankrupt in 1998, forced sale in the newspaper and on the internet
- In 2009, he asks for removal of the announcement (newspaper) and links (Google)
- After a long trial, the CJEU rules (2014)
  - Removal of search results is appropriate when these are inadequate, irrelevant, no longer relevant or excessive
  - Right to be forgotten



# Complaints, remedy, sanctions

## Complaints, remedies:

- Right to lodge a complaint (art. 77)
- Right to an effective remedy
  - Against supervisory authority (art. 78)
  - Against controller/processor (art. 79)
- Right of representation (art. 80)
- Right to compensation (art. 82)



## Powers of Data Protection Authorities (art. 58)

- Investigative powers
- Corrective powers
  - Warnings, reprimands, orders to comply, fines
- Advisory powers



## Sanctions (art. 83): Administrative fines

- up to 10/20 million euro or (for companies) up to 2/4 % of the worldwide annual turnover (whichever is higher)

# Practical issues

There are several practical issues with data subject rights:

- Awareness about who collects/processes your data
- Awareness about your data subjects rights
- Awareness about how to enforce your rights



As a result, there is little case law on data protection law in many countries.



# Data controller obligations

How else are you protected?

# Data controller obligations – overview

## GDPR – Chapter IV

- Obligation of data protection by design and by default (art. 25) **New!**
- Obligation to keep processing records (art. 30)
- Obligation to cooperate with supervisory authorities (art. 31)
- Obligation to take security measures (art. 32)
- Obligation to notify data breaches
  - To supervisory authorities (art. 33) **New!**
  - To data subjects (art. 34)
- Obligation to perform impact assessments (art. 35) **New!**
- Obligation to install a data protection officer **New!**

Not mandatory, but encouraged are:

- Codes of conduct (art. 40-41)
- Certification (art. 42-43)



# Data protection by design/default

- Privacy by design (PbD) (see also Code as Law)
  - Designing technology in such a way that privacy is protected.
- Examples
  - Restricted queries
  - Anonymization, blurring faces
  - Privacy preserving data mining



# Adequate security measures

## Adequate security measures

### ■ Factors:

- State of the art
- Costs of implementation
- Nature, scope, context and purposes
- Risks involved



### ■ Techniques

- Pseudonymization, encryption
- Ensuring confidentiality, integrity, availability and resilience
- Restoring availability and access, audit trails
- Regular testing, assessing and evaluating

# Breach notification

## ■ Notification to supervisory authorities

- Nature of the breach
- Type/number of data subjects/records concerned
- Contact details of data protection officer/contact point
- Consequences of the breach
- Measures taken/proposed



Personal data breach (art.4 (12) GDPR): not only hacking, also accidents, loss, alteration, etc.

## ■ Notification to data subjects (high risk)

- Same information, in clear and plain language

# Privacy Impact Assessments (PIA)

	Risk	Risk description	Probabil.	Impact
Step 1: collection	1.1	Incorrect or incomplete data	Medium	Medium
	1.2	Insufficient transparency (collection)	Medium	Small
	1.3	Non-equal treatment	Small	Small
	1.4	Elasticity ('waterbed effect')	Medium	Large
	1.5	More theft of license plates and vehicles	Large	Large
	1.6	Identity fraud	Small	Large
	1.7	Chilling effects	Small	Medium
Step 2: Storage	2.1	External security (hacking and leaking)	Small	Large
	2.2	Data overload	Small	Small
Step 3: Consulting and using the data	3.1	Privacy violations	Large	Small
	3.2	Function creep/détournement de pouvoir	Large	Large
	3.3	Internal security (unauthorized employees)	Large	Large
	3.4	Insufficient transparency (data use and rights)	Large	Small
	3.5	Interpretation errors/presumption of innocence	Small	Large
Step 4: Deletion	4.1	No timely deletion of data	Medium	Medium

# Risks

Definition of a risk:

**Risk = Probability x Impact**

Size of a risk:

	<b>Very likely</b>	<b>Very unlikely</b>
<b>Large impact</b>	<b>Large risk</b>	<b>Potentially large risk</b>
<b>Small impact</b>	<b>Potentially large risk</b>	<b>Small risk</b>

# Results: risk mitigating measures

	1.1	1.2	1.3	1.4	1.5	1.6	1.7	2.1	2.2	3.1	3.2	3.3	3.4	3.5	4.1
Sunset provisions and periodical evaluations	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Evidence-based approach									X		X				X
Limited type of crimes							X			X	X				
Limited data retention								X		X	X				
Selective deployment			X	X	X		X		X		X				X
Turning cameras off	Not applicable														
Random locations			X	X											
Breach notification								X			X				
Security against hacking and leaking						X		X		X					
Internal authorization rules (need to know)										X		X			
Criminalization of hacking								X		X					
Legal (personal data) protection	X	X						X	X	X	X		X		
Clear legal basis for LPR		X	X							X	X		X		X
Transparency and rectification (where possible)	X	X				X							X	X	X
Human factor in decision chain						X								X	
Adequate camera plan	X		X	X	X										
Providing information		X					X								
Independent supervision	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X



# Wrap-up

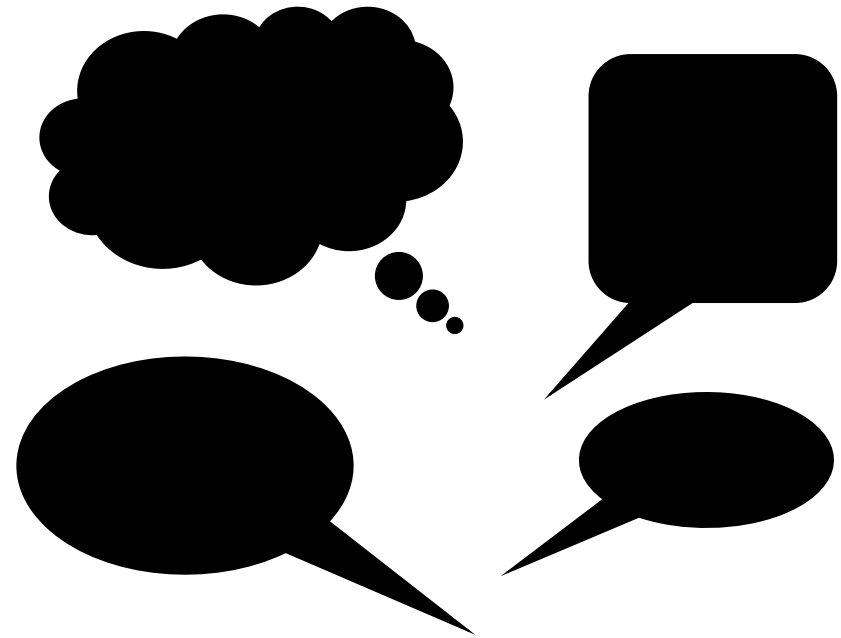


# Wrap-up



- There is value in your personal data
- You do not have a right to know the value of your personal data...
- ... but the GDPR does offer protection, via:
  - Data subject rights
  - Data controller obligations
- However, there are practical issues with data subject rights:
  - Awareness about who processes data, data subject rights, and how to enforce them
- Increased protection is expected from:
  - High administrative fines
  - Data controller obligations

# Questions?



Thank you for your attention!

Or contact me later: [b.h.m.custers@law.leidenuniv.nl](mailto:b.h.m.custers@law.leidenuniv.nl)