Locating Information Privacy

Yola Georgiadou
University Twente
Lecture @ Department of Informatics, University of Oslo, Norway
6 December 2018

Based on Georgiadou, Y., Kounadi, O. and de By, R. (2018) **The Ethics of Where**.
In *The Manual of Digital Earth*, editors Huadong Guo, Michael Goodchild, Alessandro Annoni (invited contribution)

GIScience

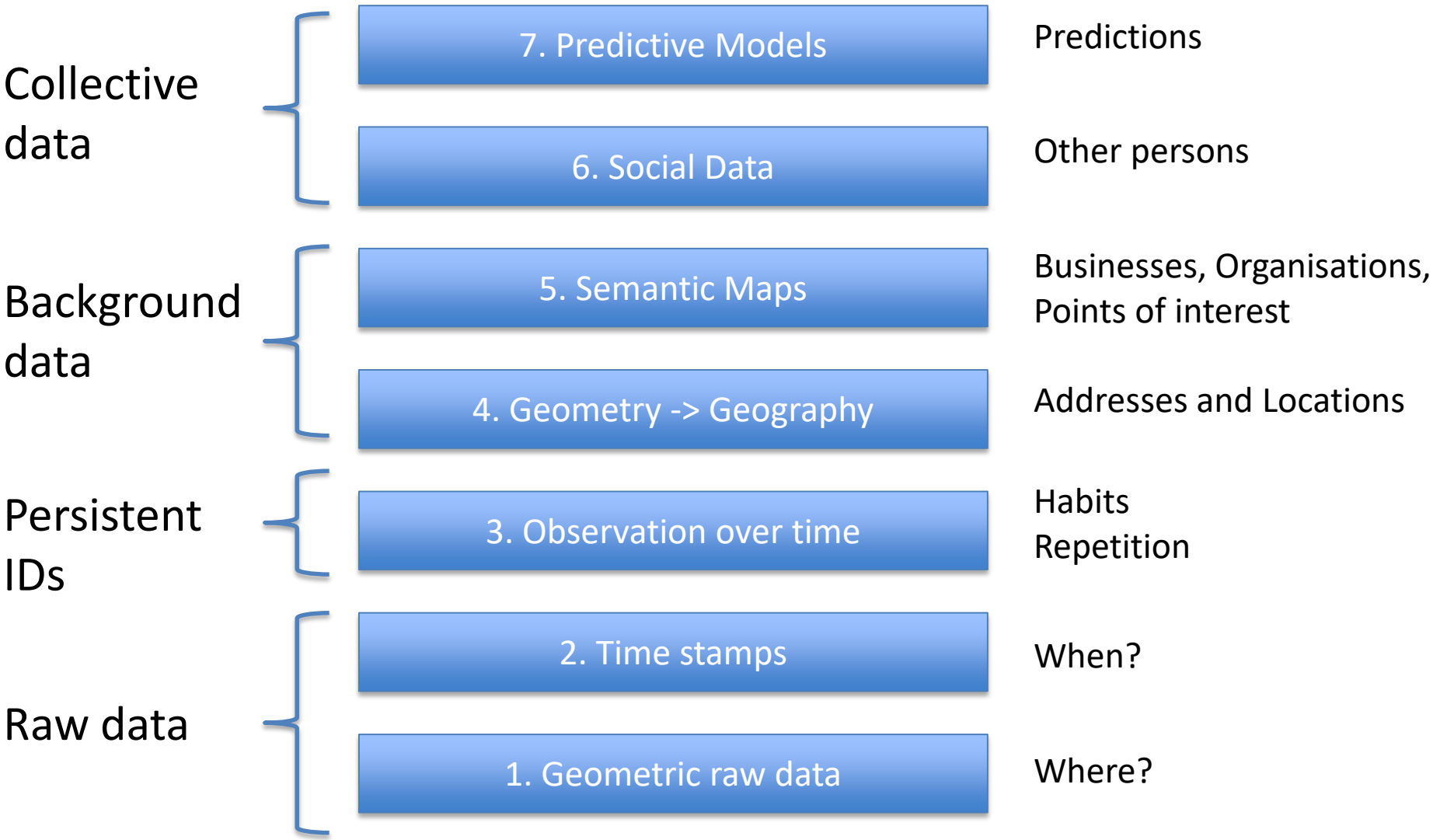
The Science of Where

What can my data tell me about here?

The Ethics of Where

What can my data tell you about me?

Hofmann‘s step model



Privacy – contested concept (1)

- 1999 - Scott McNealy, the founder & CEO of Sun Microsystems: *“you have zero privacy…get over it”*

- 2010 - Mark Zuckerberg: *“people have really gotten comfortable not only sharing more information […] more openly and with more people […] The [privacy] social norm is just something that has evolved over time.”*

- 2018 - Apple CEO Tim Cook:*“the poor privacy practices of some tech companies […] threaten to undermine technology’s awesome potential to address challenges such as disease and climate change.”*

Privacy – contested concept (2)

- Ancient Greek: ἰδιώτης (idiotes) = a private man, an ignoramus, as opposed to δημόσιος (demosios), a person of public distinction
  - Now "idiot"
  - Now "democracy"
- Latin: Private = 'deprived' of public office– privacy = a state of deprivation
  - a private in the army has no rank or distinction, and very little privacy

Privacy – contested concept (3)

- Negative or positive right
- Instrument for Kantian ethics—human dignity and personal autonomy
- Instrument for Aristotelean virtue ethics—personal development and human flourishing

Privacy

- Privacy as a positive right (Westin 1967):
  - Right of individuals, groups, or institutions to **determine for themselves** when, how, and to what extent information about them is communicated to others
- Privacy as a positive right (Floridi 2014):
  - right of individuals, groups, or institutions **to control** the life cycle (especially the generation, access, recording, and usage) of their information and determine when, how, and to what extent their information is processed by others

Typology of privacy

		Goal incongruity	
		Low(er)	High(er)
Alice's ability to control	Low(er)	Cell (4) Alice – Government institution	Cell (3) Alice – Private corporation
	High(er)	Cell (1) Alice – Bob	Cell (2) Alice–(Bob–Carol–Dan-etc)

Control… the transformation process

Volunteered data *= created and explicitly shared by individuals, e.g. social network profiles.*

Observed data *= captured by recording the actions of individuals, e.g. location data when using cell phones.*

Inferred data *= data about individuals based on analysis of volunteered or observed information, e.g. credit scores.*

Typology of privacy

		Goal incongruity	
		Low(er)	High(er)
Alice's ability to control	Low(er)	Cell (4) Alice – Government institution Privacy strategy Compliance; lodge complaint to DPA; Resistance (overt/covert)	Cell (3) Alice – Private corporation Privacy strategy Control behavior via GDPR; lodge complaint to DPA
	High(er)	Cell (1) Alice – Bob Privacy strategy: Right and duty of partial display	Cell (2) Alice–(Bob–Carol–Dan-etc) Privacy strategy Geoprivacy by design

Typology of privacy

		Goal incongruity	
		Low(er)	High(er)
Alice's ability to control	Low(er)	Cell (4) Alice – Government institution Privacy strategy Compliance; lodge complaint to DPA; Resistance (overt/covert)	Cell (3) Alice – Private corporation Privacy strategy Control behavior via GDPR; lodge complaint to DPA
	High(er)	Cell (1) Alice – Bob Privacy strategy: Right and duty of partial display	Cell (2) Alice–(Bob–Carol–Dan-etc) Privacy strategy Geoprivacy by design

Examples: measures controlling the transformation process

	Measures controlling human/machine behaviour and outputs
Prior to campaign	**human behavior** (participation agreement, informed consent, institutional approval, assign privacy manager, train data collectors) **outputs** (define criteria of access to restricted data) **machine behavior** (ensure secure sensing devices, ensure secure IT system)
Processing and analysis	**outputs** (delete data from sensing devices, remove identifiers from data set)
After the campaign	**outputs** (reduce spatial and temporal precision, consider alternatives to point maps) **human behavior** (provide contact information, use disclaimers, avoid the release of multiple versions of anonymized data, avoid the disclosure of anonymization metadata, plan a mandatory licensing agreement, authenticate data requestors)

Typology of privacy

		Goal incongruity	
		Low(er)	High(er)
Alice's ability to control	Low(er)	Cell (4) Alice – Government institution Privacy strategy Compliance; lodge complaint to DPA; Resistance (overt/covert)	Cell (3) Alice – Private corporation Privacy strategy Control behavior via GDPR; lodge complaint to DPA
	High(er)	Cell (1) Alice – Bob Privacy strategy: Right and duty of partial display	Cell (2) Alice–(Bob–Carol–Dan-etc) Privacy strategy Geoprivacy by design

Typology of privacy

		Goal incongruity	
		Low(er)	High(er)
Alice's ability to control	Low(er)	Cell (4) Alice – Government institution Privacy strategy Compliance; lodge complaint to DPA; Resistance (overt/covert)	Cell (3) Alice – Private corporation Privacy strategy Control behavior via GDPR; lodge complaint to DPA
	High(er)	Cell (1) Alice – Bob Privacy strategy: Right and duty of partial display	Cell (2) Alice–(Bob–Carol–Dan-etc) Privacy strategy Geoprivacy by design

Covert resistance

"Boycott and sabotage the census"

"*The Federal President: DO NOT* boycott and sabotage the census".

Overt resistance

Don’t count us, count your days!

Based on Georgiadou, Y., Kounadi, O. and de By, R. (2018) **The Ethics of Where**.
In *The Manual of Digital Earth*, editors Huadong Guo, Michael Goodchild, Alessandro Annoni (invited contribution)

Typology of privacy

		Goal incongruity	
		Low(er)	High(er)
Alice's ability to control	Low(er)	Cell (4) Alice – Government institution Privacy strategy Compliance; lodge complaint to DPA; Resistance (overt/covert)	Cell (3) Alice – Private corporation Privacy strategy Control behavior via GDPR; lodge complaint to DPA
	High(er)	Cell (1) Alice – Bob Privacy strategy: Right and duty of partial display	Cell (2) Alice–(Bob–Carol–Dan-etc) Privacy strategy Geoprivacy by design

Variables	Values
Attacked	1. Any individual
Attacker	1. Government/ Institution 2. Corporation 3. Researcher 4. Any individual
Spatial data types	1. Discrete location data (Dd) 2. Discrete location data with co-variates (Dd+) 3. Space-time data (STd) 4. Space-time-attribute data (STd+)
Purpose of attack	1. Identify private attribute(s) of the attacked 2. Identify the attacked who has certain private attribute(s)
Attacker's strategy	1. Key-identifier exploitation 2. Combine to uniqueness 3. Re-engineering locations 4. Analysing locations 5. Homogeneity attack 6. Background attack 7. Composition attack
Privacy-preserving measures	1. Pseudoanonymity 2. K-anonymity 3. Spatial k-anonymity 4. l -diversity 5. Differential privacy

GROUP	GRID	
	LOW	HIGH
HIGH	Data distributivism (network) **Slogan**: We produce and manage our (personal) data **Privacy**: Personal data as unalienable, as constituting who I am	Data distributivism (hierarchy) **Slogan**: Data-for-all law **Privacy**: Personal data as a good that may be traded with a public good
LOW	Data distributivism (market) **Slogan**: My data are mine, but I can sell them for a fair price **Privacy**: Personal data as tradeable product	Data extractivism **Slogan**: You have zero privacy, get over it **Privacy**: Zero

PRIVACY

“Arguing that you don’t care about the right to privacy because you have nothing to hide is no different than saying you don’t care about free speech because you have nothing to say.”

Edward Snowden

Locating Information Privacy

Yola Georgiadou
University Twente
Lecture @ Department of Informatics, University of Olso
6 December 2018

Based on Georgiadou, Y., Kounadi, O. and de By, R. (2018) **The Ethics of Where**.
In *The Manual of Digital Earth*, editors Huadong Guo, Michael Goodchild, Alessandro Annoni (invited contribution)