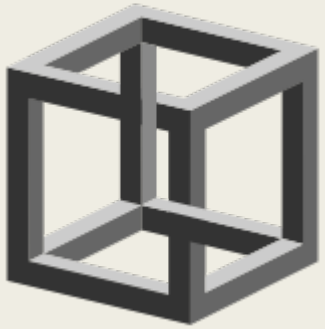


PRIVACY AS THE PROTECTION OF THE INCOMPUTABLE SELF

Mireille Hildebrandt

WHAT IF PRIVACY IS INCOMPUTABLE?

TIL Theoretical Inquiries in Law
THE CEGLA CENTER FOR INTERDISCIPLINARY RESEARCH OF THE LAW

Privacy as Protection of the Incomputable Self: From Agnostic to Agonistic Machine Learning

Mireille Hildebrandt

Abstract

This Article takes the perspective of law and philosophy, integrating insights from computer science. First, I will argue that in the era of big data analytics we need an understanding of privacy that is capable of protecting what is uncountable, incalculable or incomputable about individual persons. To instigate this new dimension of the right to privacy, I expand previous work on the relational nature of privacy, and the productive indeterminacy of human identity it implies, into an ecological understanding of privacy, taking into account the technological environment that mediates the constitution of human identity. Second, I will investigate how machine learning actually works, detecting a series of design choices that inform the accuracy of the outcome, each entailing trade-offs that determine the relevance, validity and reliability of the algorithm's accuracy for real life problems. I argue that incomputability does not call for a rejection of machine learning per se but calls for a research design that enables those who will be affected by the algorithms to become involved and to learn how machines learn — resulting in a better understanding of their potential and limitations. A better understanding of the limitations that are inherent in machine learning will deflate some of the eschatological expectations, and provide for better decision-making about whether and if so how to implement machine learning in specific domains or contexts. I will highlight how a reliable research design aligns with purpose limitation as core to its methodological integrity. This Article, then, advocates a practice of "agonistic machine learning" that will contribute to responsible decisions about the integration of data-driven applications into our environments while simultaneously bringing them under the Rule of Law. This should also provide the best means to achieve effective protection against overdetermination of individuals by machine inferences.

What's Next?

1. Differential privacy: the individual does not matter, makes no difference
2. Privacy as the protection of the incomputable self
3. Multistability of the self: the incompatible self
4. Agonistic machine learning
5. From text-driven to code- and data-driven normativity

Differential Privacy

- **What problems does it solve?**
  - *Reduces risk of detecting personal data in **aggregate data***
  - *Obtaining **statistical results** while protecting against (re)identification*
- **What problems are not solved?**
  - ***Manipulability** of individual persons based on ML or KDD inferences*
  - *Precisely because the individual does not make a difference*
- **What problems does it create?**
  - *Enables profiling & micro-targeting as it enables compliance*
  - *Creating the illusion that 'privacy' is solved by way of computation*

Differential Privacy

- Cp. homomorphic encryption, safe answers/open private data safe, polymorphic encryption and pseudonymisation, ABC
- DP protects personal data, but not necessarily a **person** or **privacy**
- **Privacy is not computable; it can be computed in different ways**
- The bigger challenge to the incomputability of the self is:
  - *Not in reidentification of personal data in aggregated data or models,*
  - *But in algorithmic decision-making, including nudging and pre-emption*

Differential Privacy

GDPR

- Advise: assume that data are **personal data** (pseudonymised, not anonymised)
- When **aggregating** behavioural data and **compressing to a target function**:
  - *Conduct a DPIA, assess risks to fundamental rights and freedoms*
  - *Apply DPbD, which may involve differential privacy and other design choices*
- Make sure you hav a **valid legal ground**, and a specific, explicit, legitimate **purpose** for each type of processing operations
- Check whether you are processing **art. 9 data (including inferred data)**, whether a relevant exception applies
- Check whether you make **automated decisions**, whether a relevant exception applies

Differential Privacy

GDPR

- Processing for scientific research, archiving and statistical purposes is subject to **broad exceptions, but still requires a propoer legal ground, and art. 9 exceptions**
- Differential privacy may result in 'the result of processing for statistical purposes' not being personal but 'aggregate data', **remaining outside scope, but** see Recital 126 – once the results are used to target individuals GDPR applies, possibly prohibition of automated decisions (unless an exception applies)
- Transparency requirements:
  - *Identity etc. of the controller (see further art. 13, 14, 15)*
  - ***Existence, meaningful explanation and envisaged consequences of automated decisions** (human intervention must be real to unqualify as such), see art. 13, 14, 15 and recital 71)*

Privacy as incomputability of the self

Incomputability in CS:

- *Undecidability*
- *Godel's incompleteness theorem*
- *Wolpert's NFT*
- *Humean scepticism (re inductive inferences)*
- *Gadamer & Popper:*
  - no perception & cognition without assumptions
  - no observation & knowledge without theoretical priors
- *ML: we cannot train on future data*
  - Saint-Exupery: the future, you must not foresee but enable

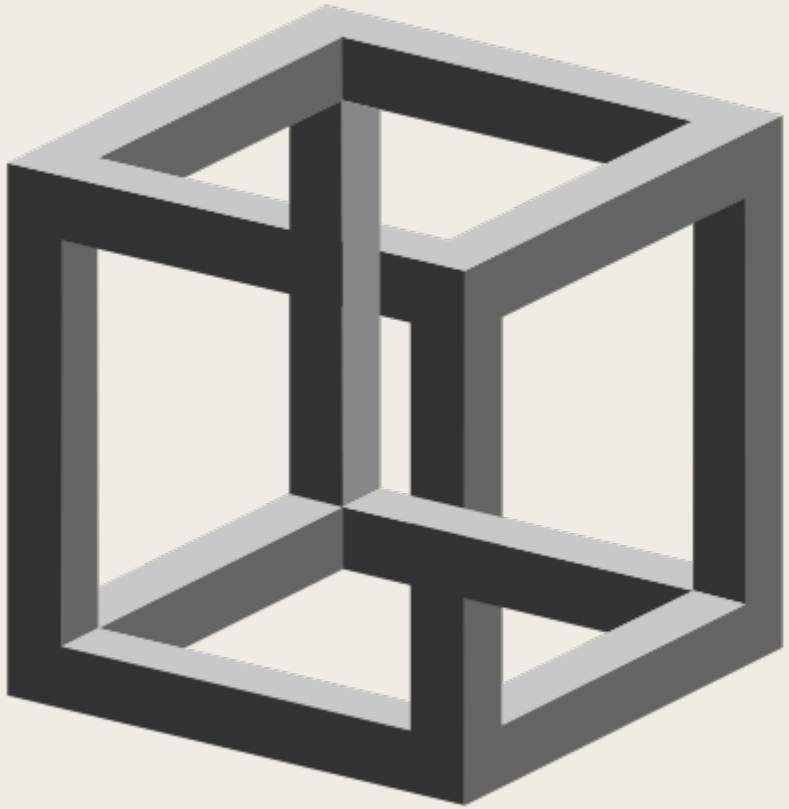
Privacy as incomputability of the self

- Incomputability of the self
  - *G.H. Mead (American pragmatism): 'generalised other'*
  - *Parsons/Luhmann: 'double contingency'*
  - *Plessner: 'ex-centric positionality'*
  - *Ricoeur: 'oneself as another'*
  - *Arendt: 'natality'*

The multistability of the self

- The self is *under*determined
- The self is relational and ecological
- **Different ICIs shape different selves**
- Don Ihde: multistability of technologies (and thus of the self)

The multistability of the self



The multistability of the self

- Necker cube: different ways of computing, different outcomes
- Protecting the self = protecting incomputability & incompatibility of the self
- Incomputability: different ways of computing the same self
- **Incomputability is protected by ensuring multi-computability**
- Scott Fitzgerald in 'On Booze':
  - *"The test of a first-rate intelligence is the ability to hold two opposed ideas in mind at the same time and still retain the ability to function."*

Agonistic ML

ML research design choices:

- *Selection, curation of data (low hanging fruit?)*
- *Feature space (confirmation bias, survival bias, etc.)*
- *Task (what are you optimising for, who gets to decide?)*
- *Hypothesis space (complex, linear)*
- *Performance metrics (how many, tweaked to raise outcome?)*
- *Out-of-sample testing (data dredging, assumptions of similar distribution)*

Agonistic ML

ML research design choices:

- *Trade-offs between* (e.g.):
  - Speed and accuracy
  - Overfitting risks and generalisation risks
- *Bugs* (e.g.):
  - Accuracy on the data, nonsense in real life
  - Spurious correlations
  - Patterns that are artefacts of translation

Agonistic ML

ML research design choices:

- Bring in those who will suffer the consequences
- Will make output more robust and acceptable
- Agile assessment (iterant)

Agonistic ML

- Rip: **constructive technology assessment** (agonism increases robustness)
- Mouffe: **participatory democratic theory** (assuming consensus is hazardous)
- Dewey: **participatory democratic theory** (formation of publics around issues)
- Latour: from ***matters of fact*** to ***matters of concern***

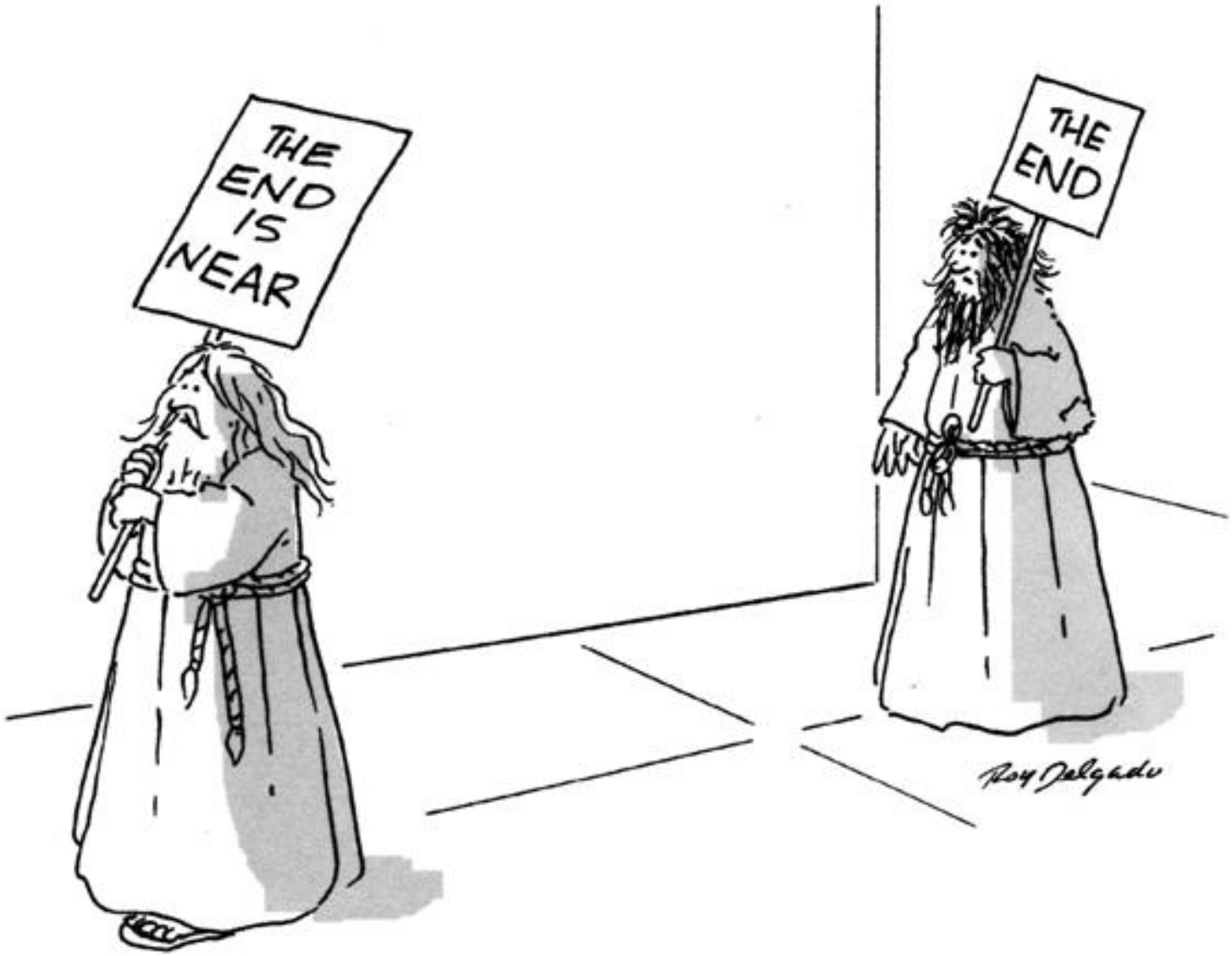
From text-driven normativity to code- and data-driven normativity

- **Text-driven ICIs afford:**
  - *Fixiation and externalisation of norms*
  - *Issues of interpretation due to distantiation norm, issuer, addressee*
  - *Contestability of the norm, due to its explicit nature and interpretability*
  - *Rule of Law: issuance, execution and decision on interpretation separated*
- **Code- and data-driven ICIs afford:**
  - *To regulate behaviour by way of pre-emption (data-driven nudging)*
  - *To regulate behaviour by way of self-execution (code-driven compliance)*
  - *Hiding norms by way of invisible defaults & incomprehensible code*

From text-driven normativity to code- and data-driven normativity

- **Computational law:**
  - *Not law but public administration*
  - *Must be brought under democratic scrutiny and under the rule of law*
  - *E.g. by way of agonistic ML*


COUNTING AS A HUMAN BEING
IN THE ERA OF COMPUTATIONAL LAW
COHUBICOL
SAY CUBICLE · THINK WITTGENSTEIN'S CUBE
ON THE PROJECT
COMPUTATIONAL LAW
LEGAL PROTECTION
EVENTS
PRESS
RESEARCH OUTCOME
Tweet
INNOVATION OF LEGAL METHOD
'It would be nice if all of the data which sociologists require could be enumerated because then we could run them through IBM machines and draw charts as the economists do. However, not everything that can be counted counts, and not everything that counts can be counted'.
William Cameron, Informal Sociology, 1963, p. 13


THE END IS NEAR
THE END
Roy Delgado