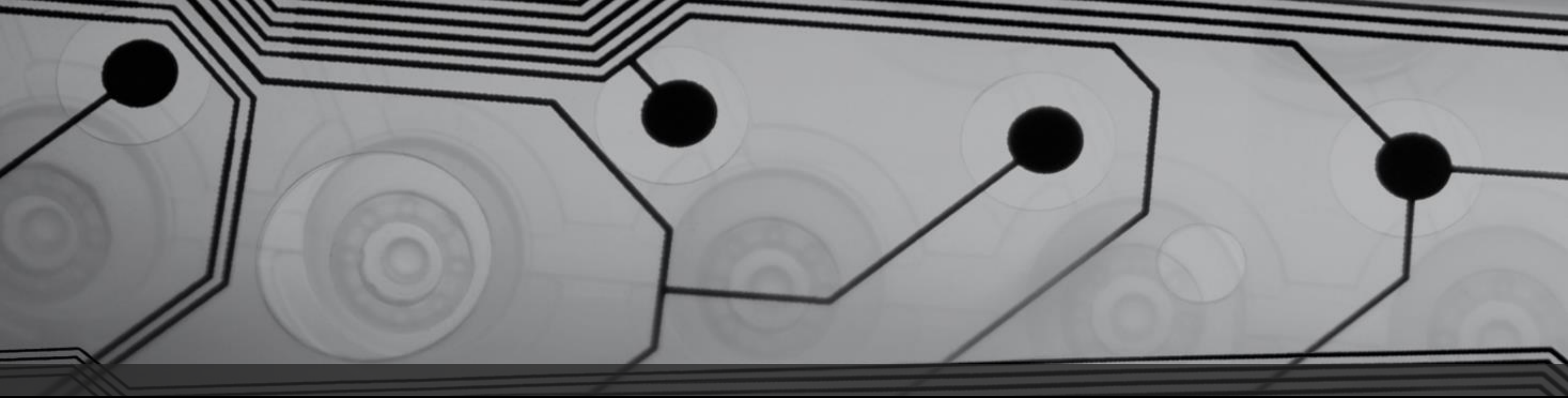


From Privacy Impact Assessment to Social Impact Assessment

Preserving trust in the Internet of Things

Lilian Edwards, Derek McAuley, and Laurence Diver
Universities of Strathclyde, Nottingham, and Edinburgh

horizon
DIGITAL ECONOMY RESEARCH

CREATe

University of
Strathclyde
Glasgow

THE UNIVERSITY OF EDINBURGH

The problem space : trust in the IoT

- Consumer trust in the Internet of Things is at vulnerable place
  - e.g. Samsung smart TV "listening" to conversations
  - Hackable baby alarms (Houston "wake up you little slut!"); 9 models tested in 2015 still had major flaws)
  - Search engine for IoT devices, inc. private webcam streams (shodan.io)
- Hypothesis: SMEs creating IoT chips and systems are not privacy aware
- Why?
  - Not traditionally customer facing;
  - Privacy a bug not a feature;
  - Little awareness of legal DP regulation;
  - May be regarded as responsibility of retail chain;
  - Engineers don't see themselves as responsible for ethical values
- Baseline questionnaire going out, via Digital Catapult , via IoTUK
- Also fits into general miasma of consumer distrust post-Snowden

The problem space: law

- IoT involving processing personal data (PD) is challenging for European DP law (DPD/GDPR)
- Is the law enough to reassure consumers?
- Consent (free, informed, signified, unambiguous) is problematic given "pervasive" environment ambition of ubicomp; esp for public systems eg smart transport, roads
  - In private systems , consent can be given by contract – but quality of consent?
- DP allows other grounds for collecting/processingPD eg "legitimate interests" of data controller if not harming fundamental rts of data subject
- BUT ePrivacy Directive ONLY accepts prior, informed consent (opt in) where location or traffic data collected (much confusion, and reform underway)
- Also increasingly hard to argue IoT systems only processing "anonymous" data (i.e. non-PD
  - NB under GDPR "pseudonymous" data expressly considered to be PD

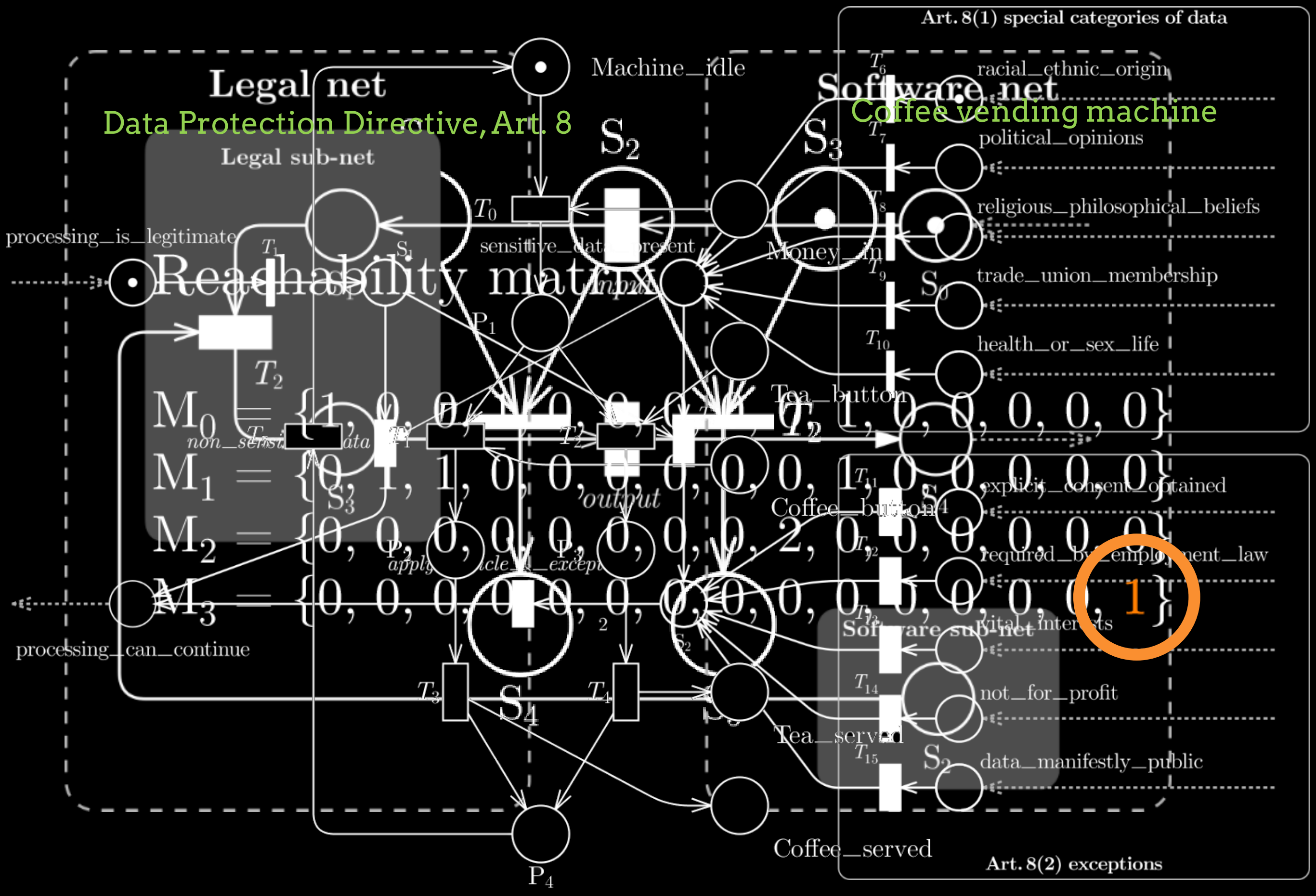
From *post factum* legal compliance to *a priori* privacy by design

- GDPR mandates "privacy by design" by 2018
- Also requires Data Protection Impact Assessments (DPIAs) where "high risk" processing
- DP by design to be embedded "from the very early stage", "within entire life cycle of technology"
- How c/should DPIAs be used in IoT? By SMEs? To be useful for entire design process, and consumer trust - not box ticking exercise too late on?
  - e.g. a system to detect bus seat occupancy using anonymous sensors not CCTV
- One key idea: a wider Social Impact Assessment to cover impacts of data processing which are not confined to classic privacy intrusions (Responsible Innovation)
  - e.g. discrimination from profiling systems (Sweeney)
  - Other values we might want to embed from start – data minimisation, interoperability, sustainability, transparency of algorithmic processing
  - Ethical impact assessment prior work exists (SATORI, PULSE, PRIPARE, EDPS) – but not so far aimed at private sector, IoT, and SMEs

SIA: bridging the law–technology gap

- GDPR
- SMEs – awareness, fears, resources
- Opening the “black box”
- Different legal regimes

- **Petri Net visual model**
- Easily understood & technically robust
- Both technical and legal processes
- Formally provable
- Portable models; IDE integration
- Evidential basis for SIA?


Art. 8(1) special categories of data
Legal net
Data Protection Directive, Art. 8
Machine_idle
Software net
Coffee vending machine
racial_ethnic_origin
political_opinions
religious_philosophical_beliefs
trade_union_membership
health_or_sex_life
Legal sub-net
processing_is_legitimate
sensitive_data_present
Money_in
Reachability matrix
Tea_button
Coffee_button
explicit_consent_obtained
required_by_employment_law
vital_interests
Software sub-net
not_for_profit
data_manifestly_public
Tea_served
Coffee_served
processing_can_continue
Art. 8(2) exceptions
M_0
M_1
M_2
M_3
1
S_2
S_3
S_4
P_1
P_4
T_0
T_1
T_2
T_3
T_4