The Hague **Security Delta**

Enabling Big Data Applications for Security

Responsible by Design

Michel Rademaker MTL, Prof. Jaap vd Herik, Prof. Cees de Laat

HSD Café, 16 maart 2017

HSD
The Hague Security Delta

Participants

Dr. Bart Custers: Center for Law and Digital Technologies, Leiden University

Prof. dr. Jaap van den Herik: Centre for Law and Digital Technology (eLaw) and Director Leiden Centre of Data Science (LCDS), Leiden University

Prof. dr. ir. Cees T.A.M. de Laat: System and Network Engineering, University of Amsterdam

Michel Rademaker MTL: Deputy Director The Hague Centre for Strategic Studies, *Project leader*

Dr. Cor Veenman Senior Researcher Forensic Big Data Science, Leiden Institute of Advanced Computer Science (LIACS), Leiden University

Universiteit Leiden

UNIVERSITY OF AMSTERDAM

LCDS
LEIDEN CENTRE
OF DATA SCIENCE

The Hague Centre for Strategic Studies

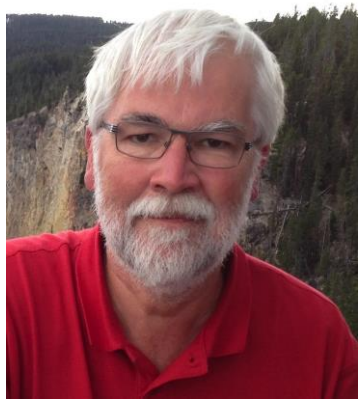
Authors

Bart Custers

Cor Veenman

Michel Rademaker

Jaap van den Herik



Cees de Laat

Acknowledgements

Graag bedanken wij HSD voor de uitnodiging. Onderzoek is teamwork over een lange periode, daarom is de lijst van samenwerkingsverbanden groot. Hieronder geven wij een selectie. Graag bedanken wij hen voor hun bijdrage en inspiratie:

Joost Kok, Arie van Bellen, Lissa Roberts, Bart Schermer, Monique Arntz, Erik Frinking.

Content of the report

1. Invariants
2. Technological opportunities
3. Information Strategies
4. How to organise?

Three aspects

We observe a decline of trust in Internet while dependency on Internet in daily life increases

- Ethical issues when dealing with big data.
- Re-enforce integrity of individual in digital world
- Understand Statistics behind AI & ML

Perfect case study

- Bank wants to lend money to entrepreneurs
- They published a psychological test:

  "How qualified am I to be an entrepreneur?"

- Aimed at unemployed people who had the intention to start their own business
- The advertisement reads: *"45,000 people have already taken this test"*
- Test is priced at € 10,-

Perfect case study

A clever student took the test and received a link (after submitting payment) to download the 30-page rapport with the test results. The link was as follows: <URL>?id=45420

- **First ethical problem:**

What would happen if I type 45419?

AND, if this works

- **Second ethical problem:**

What would happen if I type 3000 previous ID-numbers?

It became apparent that the bank had not taken any security measures and had not installed ‘rate limiters’.

Perfect case study

Panic ensued within:

- the Faculty
- the University
- the Bank
- the Society

1. What happened?
2. What measures had to be taken?

1: What happened?

1. Inappropriate ***ethical decision making***
2. Insufficient ***privacy***
3. Insufficient ***security***
4. Insufficient ***integrity***

These are four examples of **invariants**

1 (Future): what happened?

The fifth invariant is ***Safety***

Safety entails protecting a system with maximum efficiency (ideally perfection) against ***accidental*** damage.

Examples: damage caused by fire, water, nuclear explosion and earthquakes.

The meaning of security diverges from that of safety only very slightly as: protection against ***intended*** damage.

Examples: (computer)break-in, hacking, phishing, viruses.

2: What measures had to be taken?

How can we Observe and Measure these five invariants?

Five Invariants	Observation by	Measurements in 2017 using
➢ Ethical issues ➢ Privacy ➢ Security ➢ Safety ➢ Integrity	➢ Ethical Committee ➢ Privacy Barometer ➢ Intrusion Detection Systems ➢ Self Healing Systems ➢ Scrubbing	➢ Responsibility ➢ Reciprocity ➢ Adaptivity ➢ Autonomy ➢ Curation

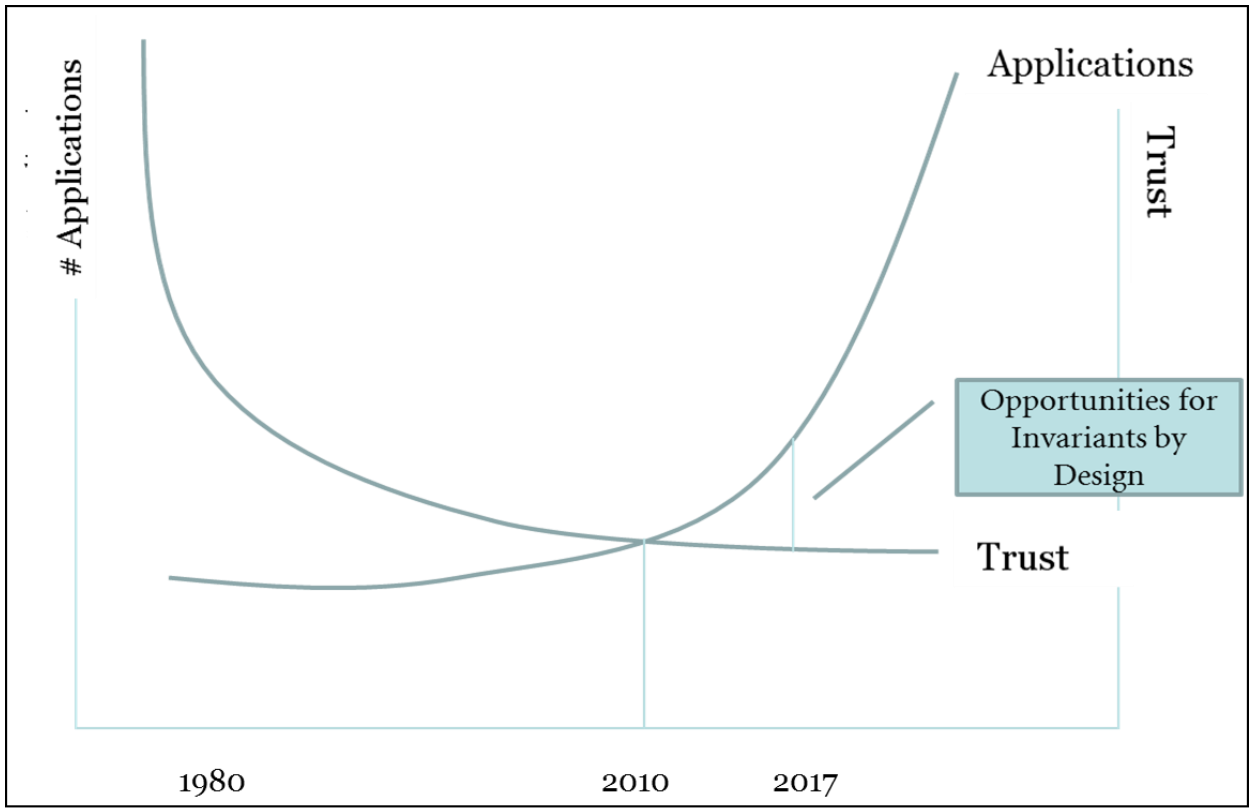
Note: this is limited to time

2: What measures had to be taken?

For 2037 we expect:

Five Invariants	Measurements in 2017 using	Measurements in 2037 using
➢ Ethical issues ➢ Privacy ➢ Security ➢ Safety ➢ Integrity	➢ Responsibility ➢ Reciprocity ➢ Adaptivity ➢ Autonomy ➢ Curation	➢ Deep Learning ➢ Deep Networks ➢ Quantum Computing ➢ Independency ➢ Transparency

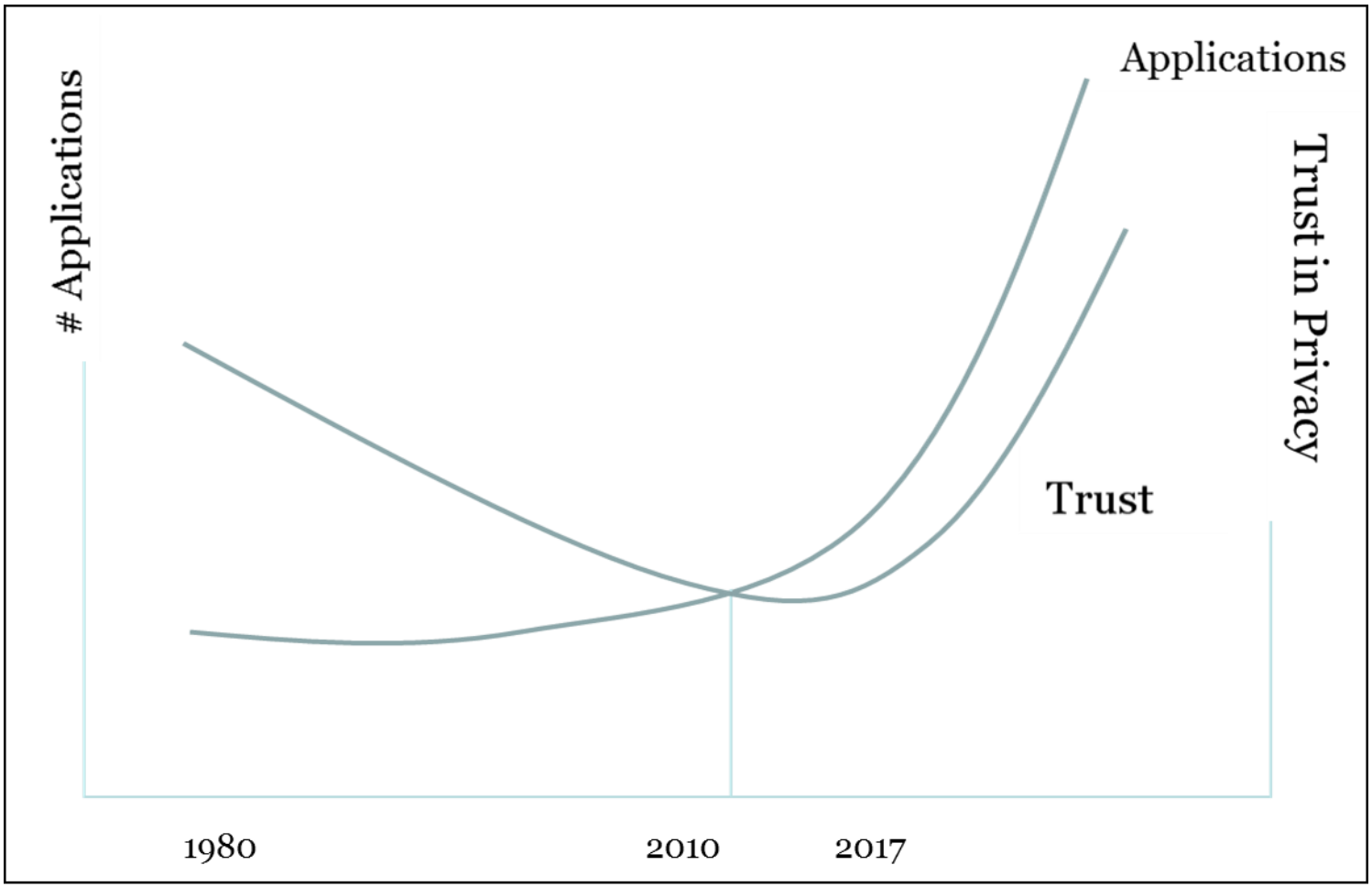
Current situation



Techniques for:

- Statistics
- Machine learning
- Computer science

Future situation



Which gap is ethically defendable??

HSD
The Hague Security Delta

Observations

After the implementation of these recommendations we may conclude that within two waves of disruptive developments (each taking, say, 25 years) computers will be at a par with, or even better at taking ethical decisions than human beings.

Big Data supplements rather than replaces human intuition.

Three aspects

We observe a decline of trust in Internet while dependency on Internet in daily life increases

- Ethical issues when dealing with big data.
- Re-enforce integrity of individual in digital world
- Understand Statistics behind AI & ML

What has this to do with the National Science quiz 2013?

- Q13: For an illness that 1 out of 1000 people suffer, a 99% accurate test is developed. You are tested with that method and found bearer of the illness. What is the probability that you really have the specific illness?
- Choose: [A: 99%, B: 50%, C: 9%]
- Answer C: because you are in the set of true and false positives!
- Suppose the accuracy of PRISM, Tempora, Xkeyscore, etc. is 99% and 1 out of 100000 of the subjects are indeed terrorists
- False positives among 100k … ~1000 !
- Send in the drones: http://www.businessinsider.com/nsa-cia-drone-program-2013-10?international=true&r=US&IR=T

Alternate Titles

- Enabling Big Data Applications for Security.
- Enabling Security for Big Data Applications.
- Enabling Applications for Big Data Security.
- Enabling Big Data for Security Applications.
- …

Final result 1:

Dependency vs. Trust

remains a challenge

Final result 2:

Statistics

is heavily involved in new developments

Final result 3:

Ethical governance

will be reflected in

National Data Authorities

And National Ethical Committees

HSD
The Hague Security Delta