cyberwatching.eu

The European watch
on cybersecurity & privacy

Impact of AI on Privacy

Antonio Kung, Trialog
PDP4E H2020 Project

Funded by the European Commission
Horizon 2020 – Grant # 740129

PDP4E: Privacy and Data Protection 4 Engineering

PDP4E

- *3-Year project started in May 2018*
- *Model-driven engineering for privacy*
  - *Risk management*
  - *Engineering requirements*
  - *Privacy-aware design*
  - *Assurance management*
- *Two use cases*
  - *Connected vehicles*
  - *Big data for smart grid*

TRIALOG

list cea tech

POLITÉCNICA
UNIVERSIDAD POLITÉCNICA DE MADRID

beawre

UNIVERSITÄT DUISBURG ESSEN
Open-Minded

KU LEUVEN CiTiP
CENTRE FOR IT & IP LAW

ECLIPSE FOUNDATION

tecnalia Inspiring Business

Impact of AI on Privacy

- Study launched in October 2018 by ISO
  - Rapporteur: Antonio Kung + 6 co-rapporteurs
- Terms of reference:
  - Input
    - current privacy standards,
    - current work carried out in SC42,
    - study of domains where autonomous decision making systems are being developed including autonomous vehicles, robots, autonomous drones,
    - initiatives and projects on responsible approaches
    - Research work
    - …
  - Output
    - review the new generation of AI-based systems (autonomous systems) and identify their impact on privacy,
    - review the new threats to privacy which AI can create,
    - review how AI can be used by deploying improved privacy controls, and
    - provide recommendations for standardization work.
- Intermediate report provided in May 2019

List of references

- References studied
  - IEEE Ethically Aligned AI – 2018
  - Ethics guidelines for trustworthy AI (High level expert group on AI) – 2018
  - Privacy Commissioners declaration – 2018
  - CNIL contribution -2019
  - AI as a Disruptive Opportunity and Challenge for Security. ETSI workshop, 2018
  - PDP4E contribution to ITU-T SG17 workshop - 2019
  - Asilomar principles – 2017
  - French debate report – 2017
  - Australian human rights commission – Human rights and tech – 2019
  - Philippines contribution
  - Japan contribution

- References not studied
  - France IA (strategy for AI in France) – 2017 (in French) :
  - Towards useful demystified AI – March 2017 (in French) .
  - Report from Cédric Villani. March 2018 (in French) .
  - G7 declaration on AI. 2018 .
  - The Malicious Use of AI
  - European Group on Ethics in Science and New Technologies declaration - March 2018
  - UK House of Lords Select Committee on AI: AI in the UK: ready, willing and able? - March 2017
  - BS 8611:2016. Guide to the ethical design and application of robots and robotic systems- April 2016
  - Privacy and Freedom of Expression In the Age of Artificial Intelligence (Privacy International and Article 19) – April 2018

High Level Risks (CNIL)

- Impact on human lives (autonomous vehicles), originating from design or learning issues
- Errors that cannot be anticipated, due to deep learning based on unfounded abstractions
- Profiling, with or without automated individual decision-making, facilitated by deep learning
- Discrimination or unfair treatment, due to algorithm bias
- Undermining human dignity and free development of personality (people to change their behavior for fear of being considered unsuitable), due to algorithm bias
- No notification/control, in massive data operation
- Problem of enforcing principles such as minimization or retention limitation, in massive data operations
- Privacy measures insufficient, due to attack capacity increase (e.g. automated re-identification technologies)

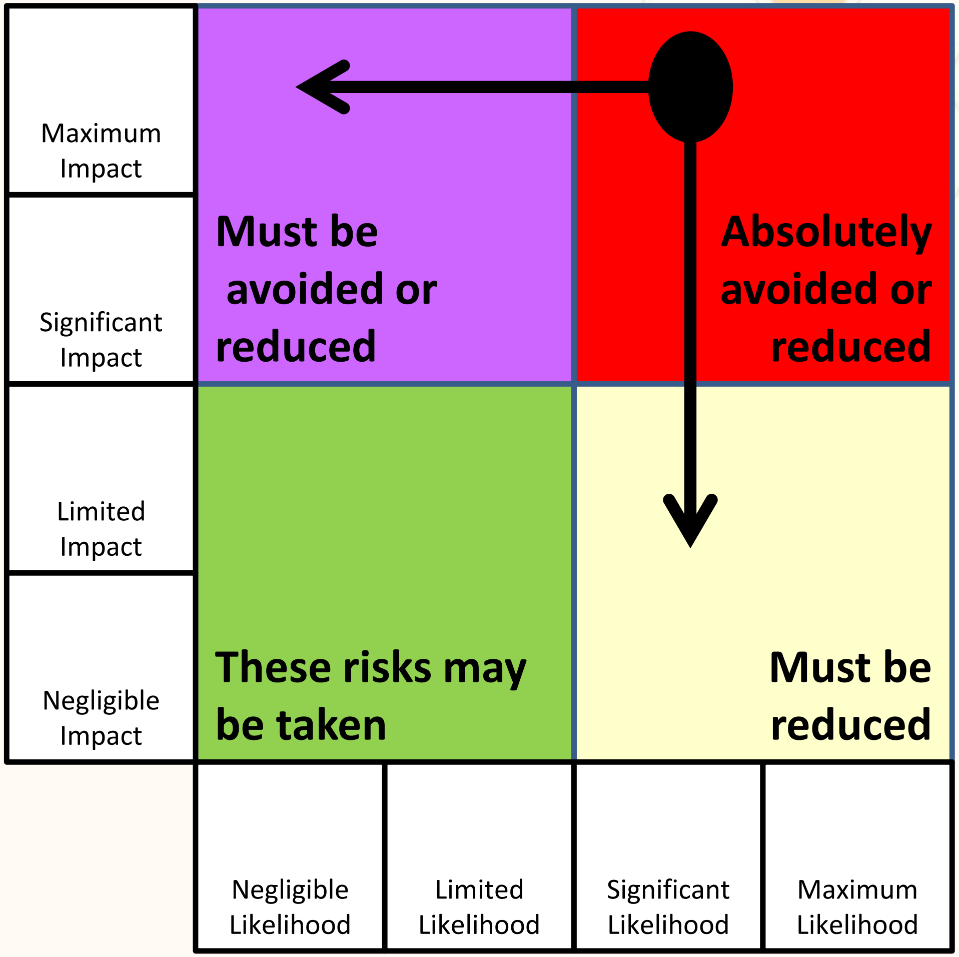
Benevolent AI

- Assistance to avoid attacks (reduce likelihood of threats)

←

- Assistance to breaches (reduce severity of impact)

↓

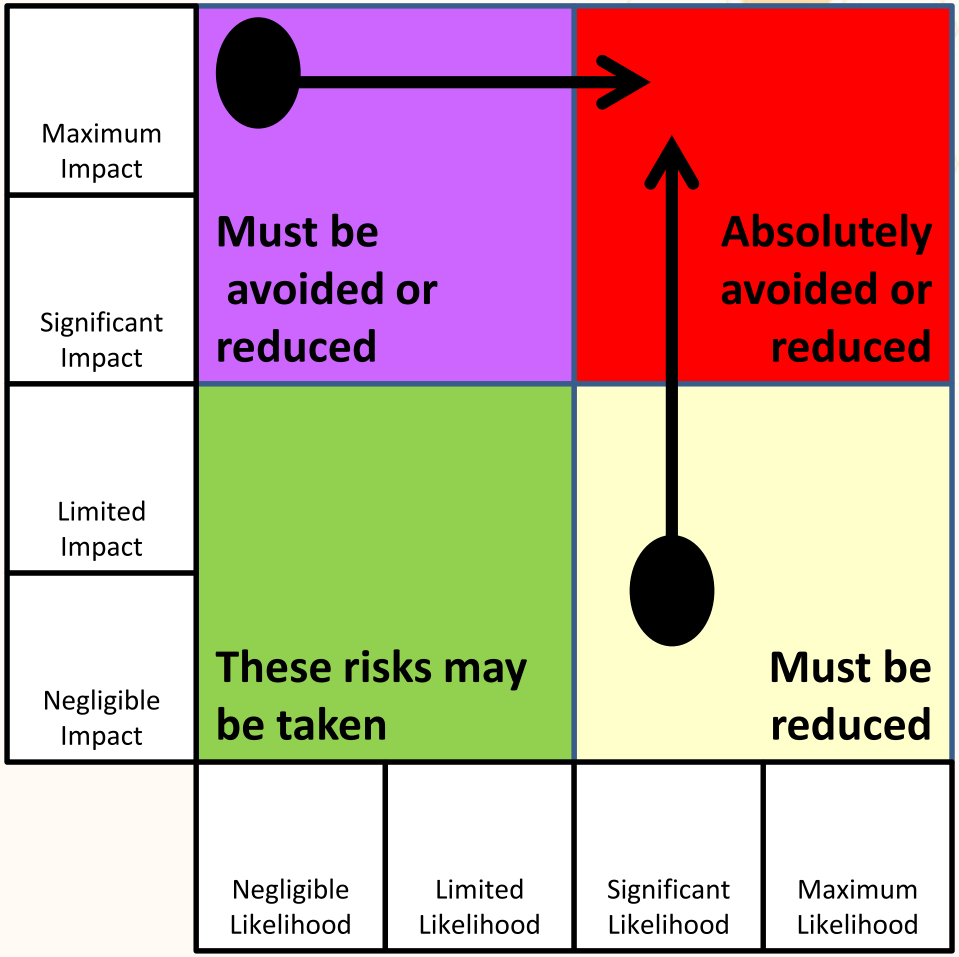


Maximum Impact				
Significant Impact	Must be avoided or reduced		Absolutely avoided or reduced	
Limited Impact				
Negligible Impact	These risks may be taken		Must be reduced	
	Negligible Likelihood	Limited Likelihood	Significant Likelihood	Maximum Likelihood

Malicious AI

- Security incident / privacy breach is more likely to occur

- Security incident / privacy breach has more impact



Maximum Impact

Significant Impact

Limited Impact

Negligible Impact

Must be avoided or reduced

Absolutely avoided or reduced

These risks may be taken

Must be reduced

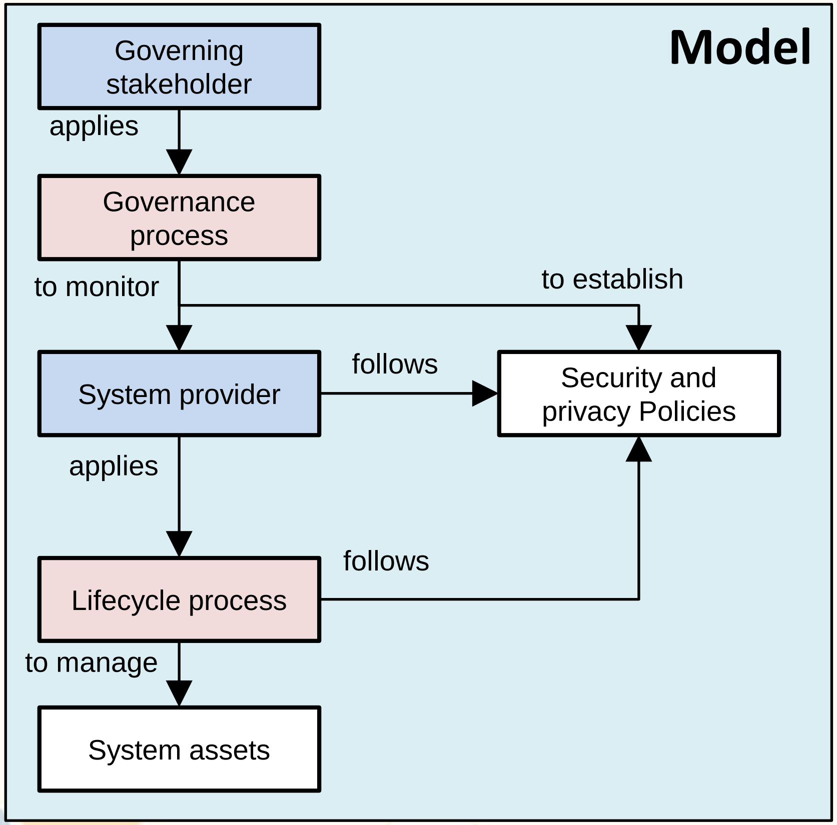
Negligible Likelihood

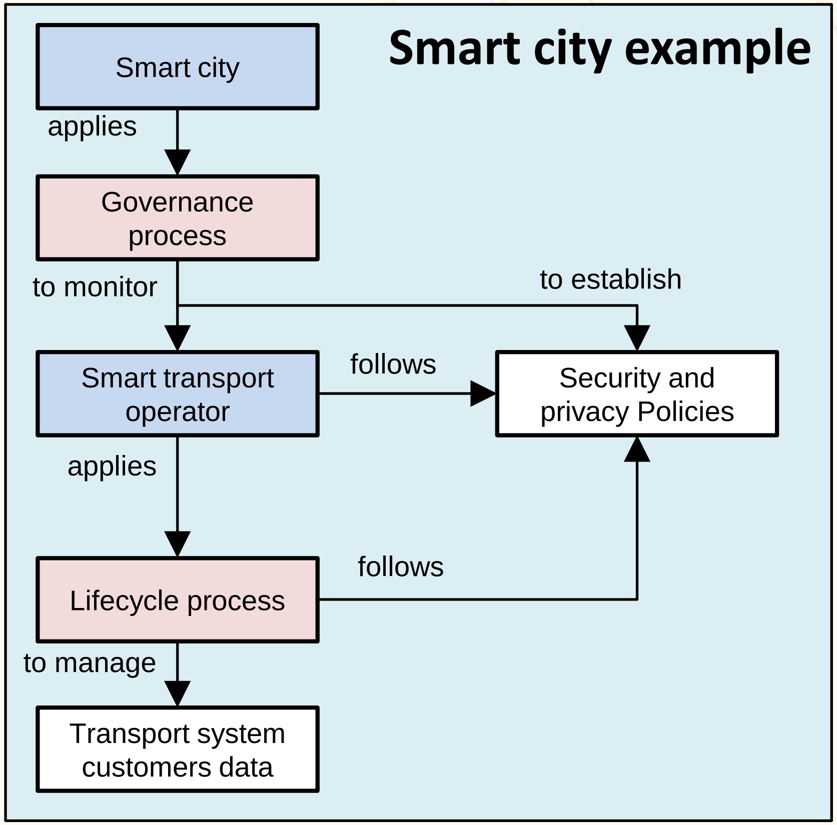
Limited Likelihood

Significant Likelihood

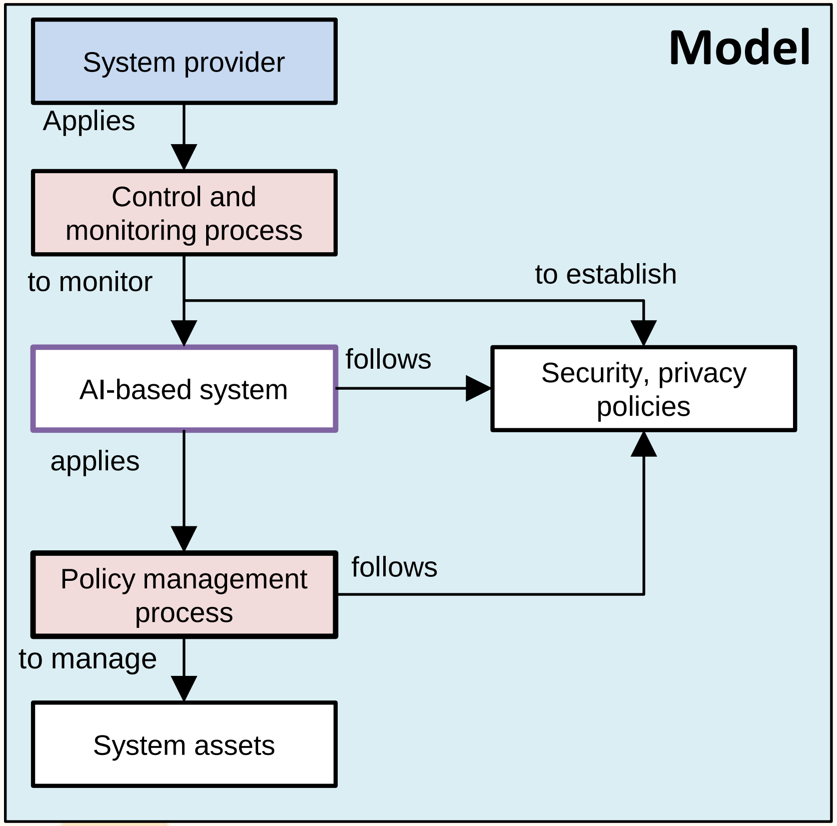
Maximum Likelihood

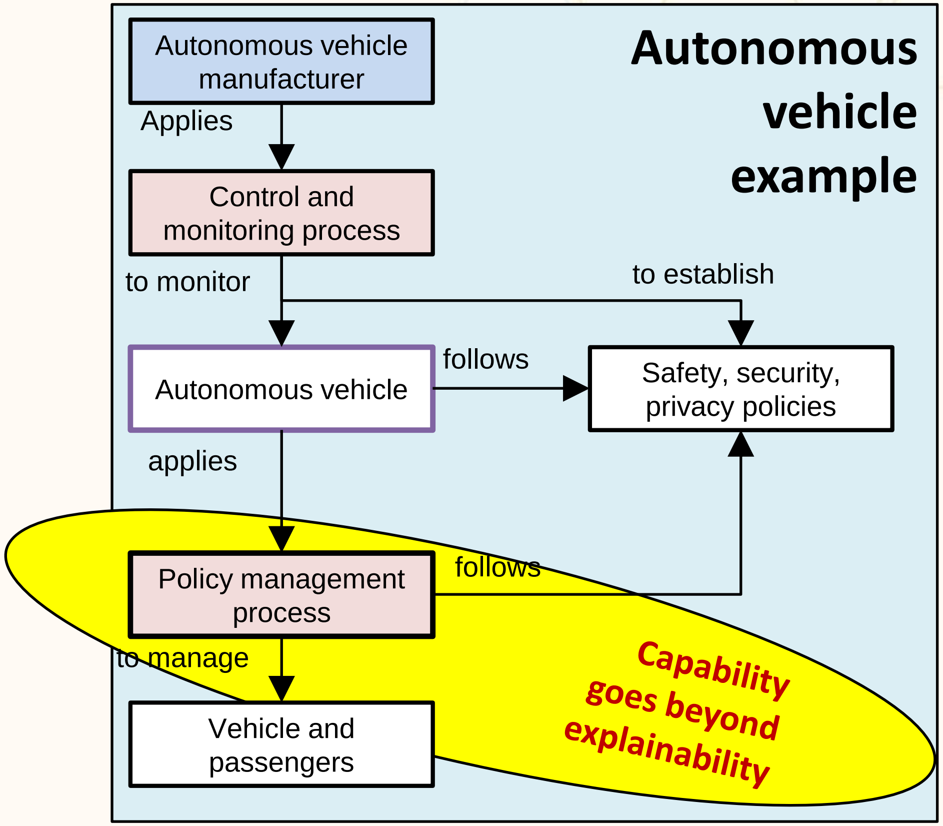
Governance for systems





Governance for AI-based systems





Autonomous vehicle example
Autonomous vehicle manufacturer
Applies
Control and monitoring process
to monitor
to establish
Autonomous vehicle
follows
Safety, security, privacy policies
applies
Policy management process
follows
to manage
Vehicle and passengers
Capability goes beyond explainability

cyberwatching.eu

The European watch
on cybersecurity & privacy

Thanks

PDP4E

Antonio Kung, Trialog
PDP4E H2020 Project

Funded by the European Commission
Horizon 2020 – Grant # 740129