Privacy Protection, Ethics and Regulations in Autonomous Cars summary

S. Altini, Prof. Ioannis Pitas,
Aristotle University of Thessaloniki
pitas@csd.auth.gr
www.aiia.csd.auth.gr

Version 1.0

Artificial Intelligence & Information Analysis Lab

Levels of Autonomy

The 6 Levels of Vehicle Autonomy

- **Level 0** (No Driving Automation)
- **Level 1** (Driver Assistance
- **Level 2** (Partial Driving Automation)
- **Level 3** (Conditional Driving Automation)
- **Level 4** (High Driving Automation)
- **Level 5** (Full Driving Automation)

SOCIETY OF AUTOMOTIVE ENGINEERS (SAE) AUTOMATION LEVELS

Full Automation

0	1	2	3	4	5
No Automation	**Driver Assistance**	**Partial Automation**	**Conditional Automation**	**High Automation**	**Full Automation**
Zero autonomy; the driver performs all driving tasks.	Vehicle is controlled by the driver, but some driving assist features may be included in the vehicle design.	Vehicle has combined automated functions, like acceleration and steering, but the driver must remain engaged with the driving task and monitor the environment at all times.	Driver is a necessity, but is not required to monitor the environment. The driver must be ready to take control of the vehicle at all times with notice.	The vehicle is capable of performing all driving functions under certain conditions. The driver may have the option to control the vehicle.	The vehicle is capable of performing all driving functions under all conditions. The driver may have the option to control the vehicle.

Safety, Security and ethical issues

- **Misuse avoidance & Data Security**
- Data Protection
- Privacy protection
- Moral Machine

Safety, Security and ethical issues

Misuse avoidance & Data Security

- **There is no existing legislation referring to safety precautions and preventive measures against misuses, and vulnerabilities exploited by attackers**
- **Data security**: Footage data collected by vehicles raise privacy concerns.
- **Types of Cyber Security attacks on ACs:**
  - **Attacks on authentication**: Sybil attack; GPS spoofing attack; Wormhole attack; Timing attack; Information tampering attack; Replication attack;
  - **Attacks on routing**: Eavesdropping attack; DoS attack; Misrouting attack; Flooding; Jamming attack;
  - **Attacks on accountability**: Auditing attack; Non-repudiation attack;
  - **Miscellaneous attacks**: Replay attack; Data interception attack; Malware attack; Greedy behavior attacks.

Safety, security and ethical issues

Misuse avoidance

- **Attacker's objectives:**
  - Communication disruption;
  - Jamming on components;
  - Manipulation on software
  - Vehicle hacking.

Safety, Security and ethical issues

Misuse avoidance

Potential vulnerable components and behavior:

- **Camera**: lane detection, obstacles, traffic sign, other AVs, reducing the security like false object detection;
- **Sensors**: hamper functioning of GPS, LiDAR, RADAR sensors, that perceive the state of the surroundings for AVs smooth functioning;
- **Vehicle platooning**: affecting the process of the industry in whole;
- **Trajectories**: jam/falsify GPS signals via hacking the GPS sensor;
- **Vehicle access**: misguide other AVs, leading to collisions/road accidents;
- **Communication**: depending on the specific target communication type (V2V, V2I, V2X;
- **Software**: AV is being misled by its software update in random and unintentional way.

Autonomous Cars Data Security

Blockchain secures AVs control and data through:

- facilitation of decentralized data sharing and security management;
- facilitation, verification, enforcement, and negotiation;
- performance of smart contracts, allowing credible transactions without third parties;
- achievement of 5-way trade-off in P2P network;

Blockchain-based IoT system stores data by transactions via nodes, guaranteeing data security/cost reduction.;

Deep reinforcement learning in combination with **decentralized approach** used to address this problem.

Safety, Security and ethical issues

- Misuse avoidance & Data Security
- **Data Protection**
- Privacy Protection
- Moral Machine

Data Protection issues in Autonomous Cars

- **Location/trajectory data**: collected/used data for navigation purposes.
    - **Risks**: private information disclosure, e.g. location, travel patterns.
- **Car sensor data**: collected data about outside ACs environment.
    - **Risks**: use of captured imagery, including ownership disputes/potential invasion of confidential treatment.
- **Driver performance data:** driving habits, destinations.
    - **Risks**: disclosing information about other drivers without their consent.

Safety, Security and ethical issues

- Misuse avoidance & Data Security
- Data Protection
- **Privacy protection**
- Moral Machine

Autonomous Cars Data Security requirements

Types of data must be protected:

- **Data stored** on AC and/or external locations;
- **On AVs data encryption**, access allowed to authenticated actors only;
- **Data stored in clouds;**
- **Data transmitted:**
  - Data controller transmit personal data to commercial partner (recipient), based legal basis, compliant to Art. 6 GDPR.
  - Data owner's consent required before data transmission to commercial partner (data controller).
- **Data publicly distributed** (e.g., AVs datasets).

Privacy and Data Protection

Cyber security and data protection in AVs: Implementing GDPR in EU and other countries.

- Legal provisions integrated with others related to data protection/cyber security;
- Directive (EU) 2016/1148, Network Information Security and NIS;
- Regulation (EU) 2016/679, General Data Protection Regulation (GDPR);
- Directive (EU) 2016/680;
- Directive (EU) 2016/681;
- EU Regulation 2018/1807, concerning to free/non free flow of personal data, that took effect on May 29, 2019.

Privacy and Data Protection

- **Data protection regulations and policies:**
  - Non EU Countries adopted regulations similar to GDPR;
  - Some EU countries incorporated GDPR in national legislation in 2019-2020;
  - Data management and protection of AVs collected data is still at a nascent stage;
  - Anonymization is a key factor for the protection of personal collected data.
- **Unanswered issues:**
  - Inherent difficulty consists the distinction between personal/non-personal data;
  - Capability of “re-identification” originally anonymous data through AI/ Big Data integration with those available publicly;
  - Challenge of current methods for strengthening privacy protection: k-anonymity, randomness on a certain threshold of statistical population, "pseudo-anonymization” comply with article 4(5), 25 and 32 of GDPR.

Privacy and Data Protection

• **GDPR:** data protection legislation within EU, replaces Directive 95/46/EC, complementing accountability requirement (article 5, paragraph 2).

• **Special data:** “accessibility, exchange, re-use” of data related to static road data (article 4), dynamic road data (article 5), traffic data (article 6), according to EU Delegated Regulation 2015/962, have to be granted.

•**Technological standard for data transmission** on naturally road safety, compliant to DATEX II, an EU regulation, constitutes primary objective nationally (e.g., Sweden, UK) or internationally (e.g., EU).

• **Protection of individuals** from processing and free flow of personal data, pursuant to Directive 95/46/EC of European Parliament and Council of October 24, 1995;

• **Anonymization**: data could be anonymized, ensuring that cannot be re-identified;

Privacy and Data Protection

Privacy Concerns in AVs: measures to protect personal collected/stored data.

- **Legislation**: EDR data downloaded only with owner's consent are granted to certain exceptions (vehicle safety research, service/repair of vehicle, court orders);
- **Privacy by Design**: privacy/security risk assessment; minimization of collected/retained data; security measures before launching;
- **Industry guidance**: utilizing innovative technologies as to protect customers' privacy relating to AVs features' development;
- **Notice and Consent**: key principles for privacy laws and frameworks poses challenges.

Privacy Protection, ethics and regulatory issues

Ethical Impacts: Safety and prevention

- Moral algorithms;
- Autonomy;
- Responsibility;
- Rights: most of the countries are still require level 3 automation, following non-autonomous driving policies in relation to driving capacity;
- Insurance and discrimination;
- Privacy.

Typical AVs regulations in EU

Automated Driving System (ADS) "refers to the hardware and software, collectively capable of performing the DDT [dynamic driving task] on sustained basis, regardless of whether it is limited to a specific operational design domain" (SAE International, 2018: 3).

The above definition refers to levels 3-5 driving automation systems:

- **Discussions of driving automation systems** "refer to six levels of automation" (SAE International, 2018).
- **SAE levels 3-5**: need of new regulations/laws related to safety controversies for non human-controlled driving;
- **SAE level 5**: driving without limitations of operational design and the need of driver fallback;
- **SAE International**: "driving automation systems for any level 1-5 system/feature that performs part/all DDT on a sustained basis" (SAE International, 2018: 4).

Typical AVs international regulations

International Regulation: by jurisdiction

- Rules for licensing, testing, operating on public roads with/without driver;
- Rules for V2V communications;
- Data privacy and cybersecurity rules.

Safety, Security and ethical issues

- Misuse avoidance & Data Security
- Data Protection
- Privacy Protection
- **Moral Machine**

Privacy Protection, ethics and regulatory issues

- **Ethical Valence Theory (EVT)** - AVs decision-making as a type of claim mitigation

Differences between humans and AVs:

- Humans have the ethical common sense to deal with new driving situations;
- AVs need to test this ethical sense.

- **AVs**, not fully automated, are legal compliant to Vienna Agreement (UNECE WP1, 2017)
- **AVs in the law area**: product liability law/tort law/warranty/traffic law/criminal law/insurance law/data privacy act/ legal implications vary among countries, including EU.

Privacy protection, ethics and regulatory issues

Ethical norms and moral values

Question: How “fully autonomous” vehicles are or whether they should be morally autonomous?

AVs as different agents than humans,

need to be adjusted to **a human oriented “original” virtue ethics**

Privacy Protection, ethics and regulatory issues

A GAN-based approach to protect Vehicular Camera Data

Auto-Driving GAN (ADGAN): generate privacy-preserving camera images for protecting location privacy in auto-driving:

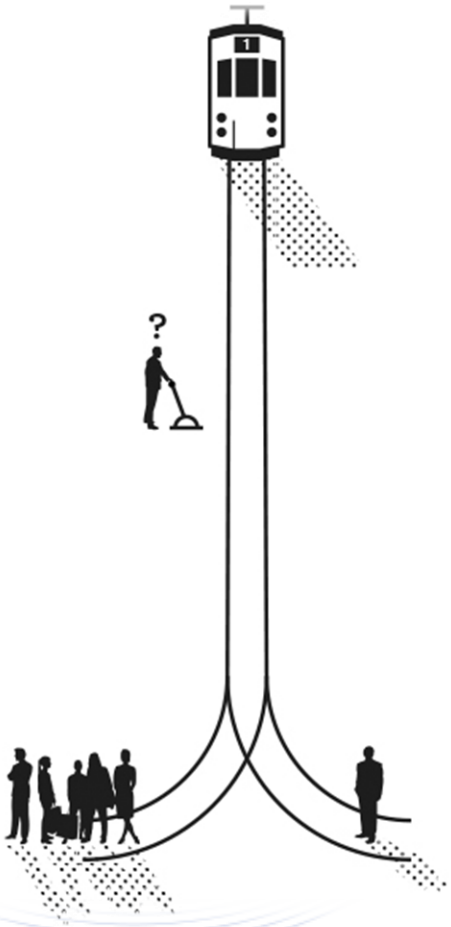
- **Prevents camera data** from being attacked by location inference;
- **Offers an effective tradeoff** between recognition utility and privacy protection for camera data in comparison with the state-of-the-art.

(f) ground truth (g) pix2pix (h) pix2pix+pri (i) UNIT+pri (j) ADGAN

Fig. 1: Visual quality comparison of generated images for Google Street View. Left to right: ground truth of input, pix2pix result, pix2pix+pri result, UNIT+pri result and ADGAN result.

Privacy Protection, ethics and regulatory issues

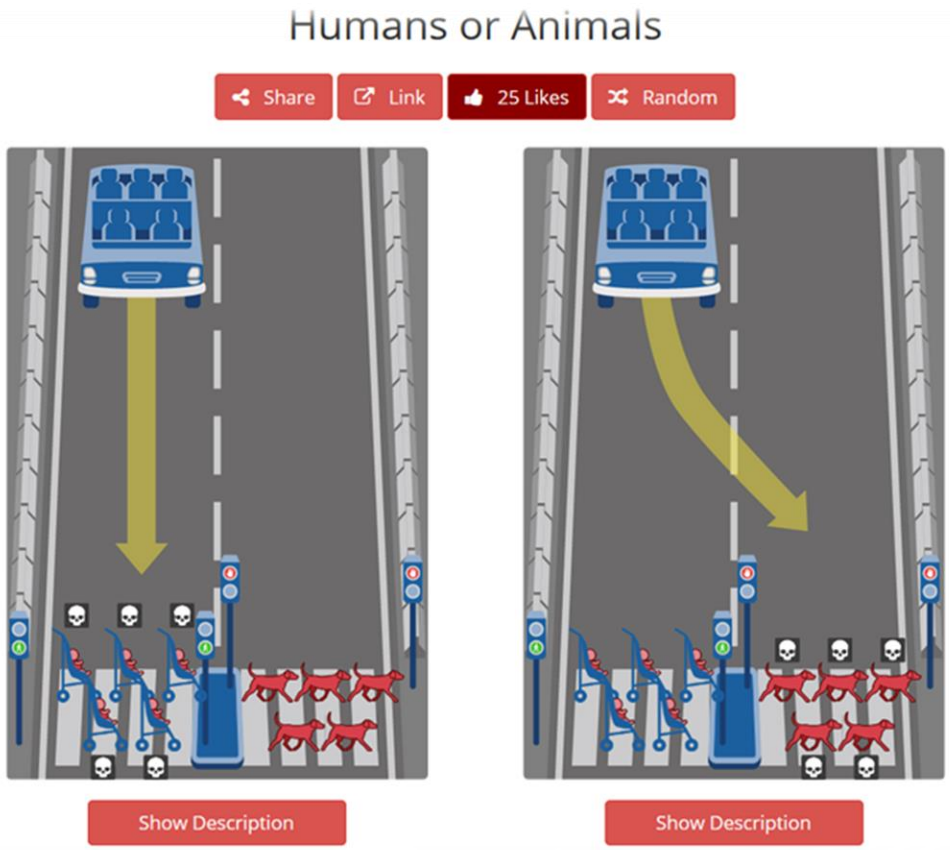
- **Trolley problem** describes “a moral dilemma that either way, harm to persons is unavoidable and there are good ethical reasons for one or the other behaviour”.
- **Trolley cases** are “dramatic, stylised, black-and-white situations that have little resemblance to real-life extreme traffic situations”.

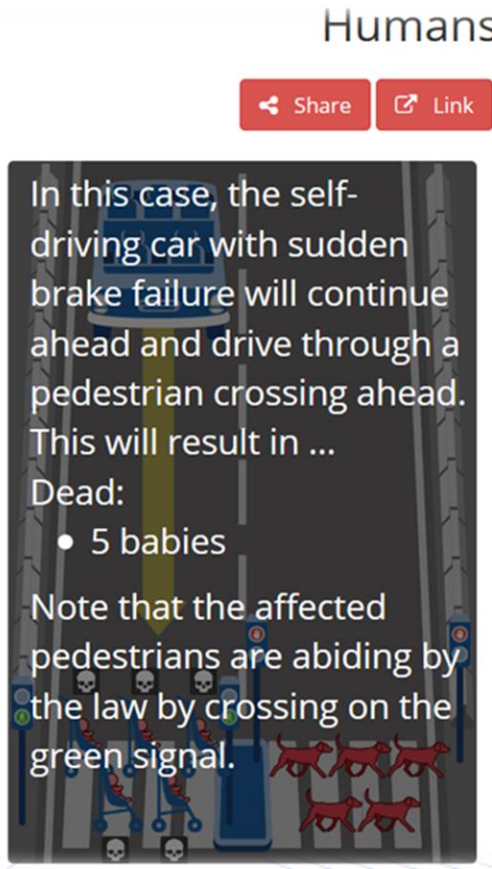


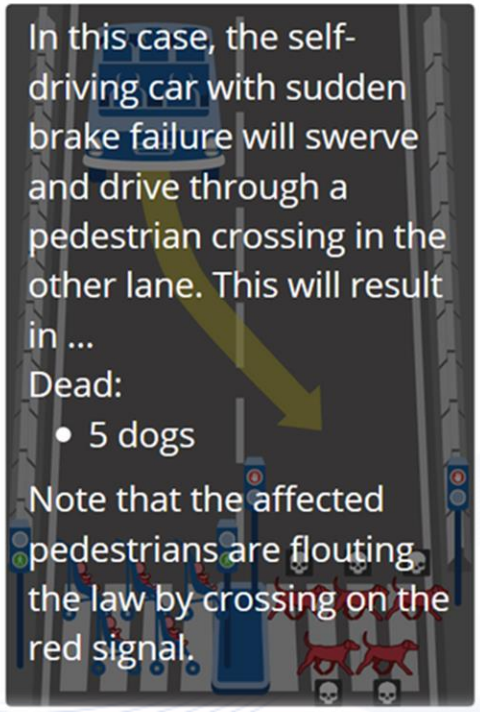
https://fs.blog/trolley-experiment/

Privacy Protection, ethics and regulatory issues

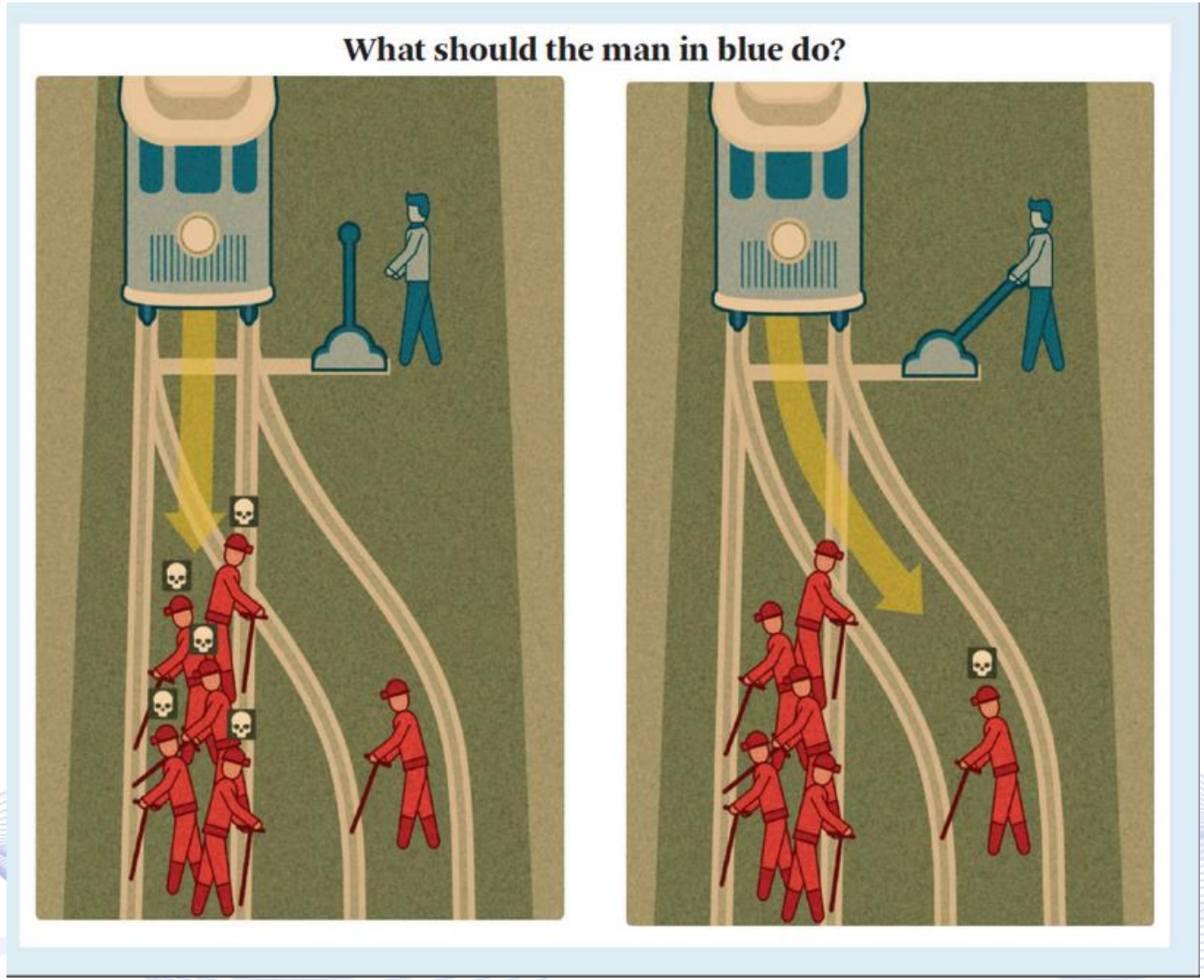
“Moral Machine” - an online experimental platform: moral preferences in AVs moral dilemmas







https://www.moralmachine.net



Awad, E. Dsouza, D., Bonnefon, J.-F., Shariff, A., Rahwan, I. (2020). Crowdsourcing moral machines. *Communications of the ACM*, vol. 63 (3), pp. 48-55.

Q & A

Thank you very much for your attention!

More material in
http://icarus.csd.auth.gr/cvml-web-lecture-series/

Contact: Prof. I. Pitas
pitas@csd.auth.gr