
Faculty of Law, Economics and Finance
CRIM_AI
-
Country Roundtable – The UK
15 November 2023
UNIVERSITÉ DU
LUXEMBOURG

Tour de Table - Introducing the Project Team

UNIVERSITÉ DU LUXEMBOURG

Interdisciplinary Group of Experts

- Sabine Gless
- (*John Vervaele*)
- (*Paul De Hert*)
- (*Christoph Sorge*)
- Cornelia Kutterer
- Martin Sacleux
- Andre Klip
- Iain Walden

Country Rapporteurs

- DE: Dominik Browoski
- NL: Rick Robroek & (*Pieter Liefrink)*
- UK: Valsamis Mitsilegas & Clementine Salvi & Rudi Fortson
- US: Brandon Garett
- LU: Theo Antunes
- FR: Juliette Lelieur

Luxembourg Team

- Katalin Ligeti (PI)
- Charlotte Quaisser (RA UL)
- *(Pia Levicnik (PhD))*

Other Participants

- *Juraj Seifert (VUB/UL)*
- Lea Bachmann (PhD Uni Basel)
- Georgia Theodorakakou (PhD UL)

CRIM_AI Project Timeline

- Date of Final Conference & Book Launch 7-8 November 2024

Program and Objectives of the Country Roundtable

1. Brief Summery of the project objectives and methodology
2. Presentations on the UK Legal Framework and Practice

Introduction to the CRIM_AI Project

https://aiandcriminaljustice.uni.lu

FACULTY OF LAW, ECONOMICS AND FINANCE

UNIVERSITÉ DU LUXEMBOURG

CRIM/AI

HOME PROJECT NEWS TEAM RESOURCES

AI Evidence

New York Times Reports: In Connecticut Murder Case, a Fitbit Is a Silent Witness

By CHRISTINE HAUSER APRIL 27, 2017 The woman shot dead in the basement of her suburban Connecticut home had struggled with an intruder, her husband told the poli in 2015. But over time, the story fell apar to rely on a silent witness — a Fitbit exerc the woman's last movements and may be murder. The case that began at the hous Dabate in Ellington, a town of about 15,0 Hartford, and unfolded over the last yea example of how exercise devices have b investigators' tool kits. Fastened to the have a unique proximity as witnesses. T sleep schedules, locations and distance life events, from innocent mishaps to c factored into a Pennsylvania sexual ass personal injury case in Canada in 2014 recorded a young woman's struggle wi park in March.

CriminalDefenseLawyer Published by NOLO

LAWS BY CRIME ▾ LEGAL RIGHTS ▾ CRIMINAL PROCESS ▾

Home › Criminal Law › Criminal Process

Could Your "Smart House" be Called as a Trial Witness?

In-home devices that connect to the Internet, often with convenient features that allow off-site commands, alerts, and owner-preference settings, create what are colloquially called smart houses.

"Alexa, raise your right hand." The problem is, Alexa has no hands or any other human feature. You know Alexa—that's the name used by Amazon for its virtual personal assistant, most frequently invoked on its Echo in-home sm speaker. Alexa may not have a face, but the program is a potential witness to a murder in Arkansas.

What is a "Smart House?"

In-home devices that connect to the Internet, often with convenient features that allow off-site commands, alert owner-preference settings, create what are colloquially called smart houses. Smart TVs, thermostats, alarms, b monitors, and lighting systems are all available to home-owners. A recent addition is the "smart speaker," such Amazon's Echo device. Smart speakers are essentially voice-activated personal assistants that sit on your cou Echo, for example, comes with the Alexa smart assistant installed. With smart devices, the owner can issue a command (say, tell the Roomba to vacuum the hall) and the device carries it out. You can sit on your couch an "Alexa, get me a pepperoni pie," and the smart speaker will wake up and phone your favorite pizza joint to o delivery. Very sweet set up, no?

Murder solved by Alexa: Domestic abuser who killed his wife is jailed for life with 20-year minimum term - after voice recordings on Amazon device helped bring him to justice

- **Daniel White, 36, murdered Angie White, 45, at her home in Swansea, Wales**
- **Amazon's Alexa saved audio recordings of White at the time of the murder**

By ALEXANDER BUTLER
PUBLISHED: 16:51 BST, 24 March 2023 | **UPDATED:** 16:58 BST, 24 March 2023

Share 48 shares 123 View comments

An Amazon Alexa device helped bring a murderer to justice after it captured incriminating voice recordings of him at the time he strangled his wife.

Daniel White, 36, kicked open his wife Angie White's locked bedroom door and strangled her before cutting her throat with a Stanley knife in October last year.

He then fled the house in Swansea, Wales, in his wife's car and hours later phoned police to confess to killing her.

Detectives discovered White's voice commands recorded by Alexa at the time of the murder which aided his prosecution.

He was recorded as sounding 'out of breath' when saying 'Turn on - Alexa' during the early hours of the morning he killed Mrs White.

- Focus of CRIM_AI is **AI Evidence**, i.e. AI directed towards providing evidence against criminal defendants
  - no attention to AI informed predictive policing (helps to prioritize deployment of police, but it is not introduced in court as evidence of guilt)
  - no attention to AI informed judicial decision on regarding pretrial detention, sentencing, corrections, and re-entry (AI is used for risk assessment).

- Types of AI Evidence studied by the project are

Forensic AI Evidence
- filtering AI (e.g. used by SFO);
- data mining AI;
- FRT (e.g. NeoFace Watch; Clearview)
- voiceprint;
- ANPR
- probabilistic genotyping AI e.g. TrueAllelle , STRMix)

Consumer Product AI.
- Google Earth
- Find My iPhone
- Alexa
- Etc.

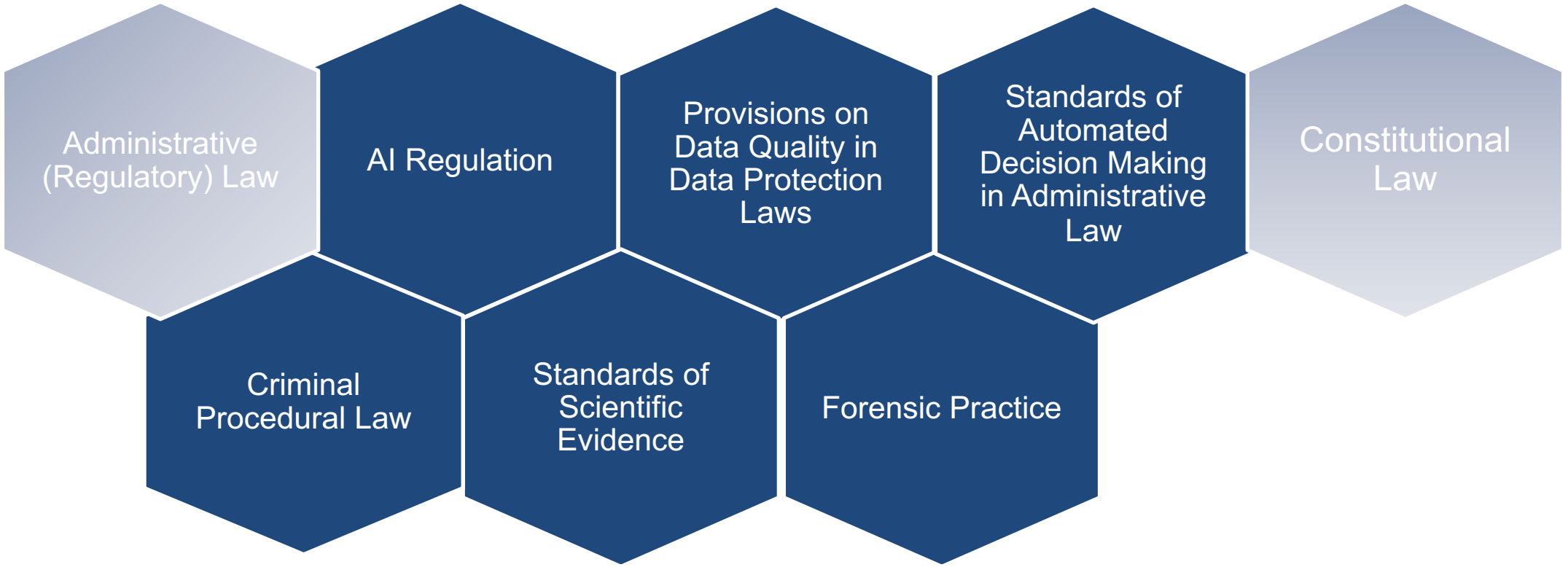
1. Main points of the national policy discussion
2. Legal definition and legal framework for AI Evidence
    - Existing categories of evidence and AI Evidence
    - Rules of scientific evidence and criminal forensics
    - Admissibility of AI Evidence
    - Right of the defence and AI Evidence
    - Requirements of AI Developers

Legal Framework for the Design and Deployment of AI in Criminal Proceedings

- Policy and regulatory devide (EU – CoE – US)
  - curbing innovation, maintaining efficiency?
  - risk based approach or rather innovation friendly?
  - transversal or sector specific?
  - principles or hard law? And how to operationalise principles?
  - exceptions for national defence? national security? law enforcement?
  - prohibited technologies (FRT?, predicitive policing?, ethnic profiling?)

- From general regulatory framework to criminal justice
  - human overseight, safe AI..
  - trustworthiness (linked to the debate on transparency *v* accountability and recommendation of the UK Justice and Home Affairs Committee for mandatory registers for AI used by the police and in the criminal justice system)
  - discrimination bias and profiling.

Legal Frameworks Applicable to AI Evidence



No specific legal framework for AI Evidence, but a patchwork of frameworks that reveal **tensions** between different bodies of law (see e.g. the proposed reform of the NL Code of Criminal Procedure)

Applying exisiting categories of evidence to AI Evidence

- AI Evidence is not considered as a special form of evidence (neither is computer evidence).
- AI Evidence can be introduced via
  - witness testimony;
  - expert testimony;
  - documentary evidence
  - inspection report (?)
  - measurement of raw data (?).
- Divergent national rules on admissibility and exlcusion of evidence.

Admissibility of AI Evidence

- Evidentiary AI must be reliable, valid and credible to be be admitted in trial.
- General tendecy to admit Evidentiary AI without too-detailed scrutiny as to validity, reliability, or credibility (assumptions in national practice that computers – and hence AI –, is reliable).
- Litigation in the reporting countries tends to apply the rules of scientific evidence to Evidentiary AI.
- Are exisiting rules sufficient for the judge to assess the admissibility of evidence?
  - Technology is black box AI developed by US Big Tech – is validation by national forensic practitioners enough?
  - How do violations of privacy and data protection can be established and how would such violations affect the lawfulness of the evidence?
  - How to test the reliability and veracity of AI Evidence especially in case of opaque black box AI ?

Defence rights and AI Evidence

- No duty to inform in advance the defence of the use of AI Evidence, BUT
- Whether the court orders the disclosure of the AI Evidence's specifications, source code, and training data relevant to the reliability and admissibility of the AI Evidence very much depends on the case.
- How can the defence scrutinise and critically assess (incriminating) AI Evidence (black box AI)? Do we need to accommodate disclosure and discovery rules?
- Defence might not have the financial means to challenge it.
- Do we need new defence rights such as access to the dataset or access to the AI tool?
- When assessing the fairness of the proceedings as a whole, ECtHR reviews the domestic courts' evaluation of evidence to determine whether the domestic courts' assessment of the weight of the evidence could be considered unacceptable or arbitrary.

AI Developers

- We see both public and private development of Evidentiary AI
  - so far states shy away from imposing obligations on AI Developers;
  - few voluntary initiatives of private sector to disclose how their AI works.

- Areas of tension
  - claims of proprietary or trade secrets protection by AI Developers;
  - right to information and the needs and efficiency of law enforcement.

- Approaches to address the tensions
  - National approaches
    - IT if automated decision affects individuals all information has to be given to the court)
    - NL Algorithm Register
    - US Justice in Forensic Algorithms Act
  - EU approach
    - Draft EU AI Act stipulates transparency obligations (need to be detailed at national level for AI Evidence).
    - Data protection law
      - Article 15(1)(h) GDPR right to “meaningful information about the logic involved as well as the significance and envisaged consequences of automated processing operations for the data subject”
      - Recital 63 GDPR “that right should not adversely affect the rights or freedoms of others, including trade secrets or intellectual property”
      - Opinion of Advocate General Pikamäe in SCHUFA Holding (C-634/21).

Thank you very much for your attention!