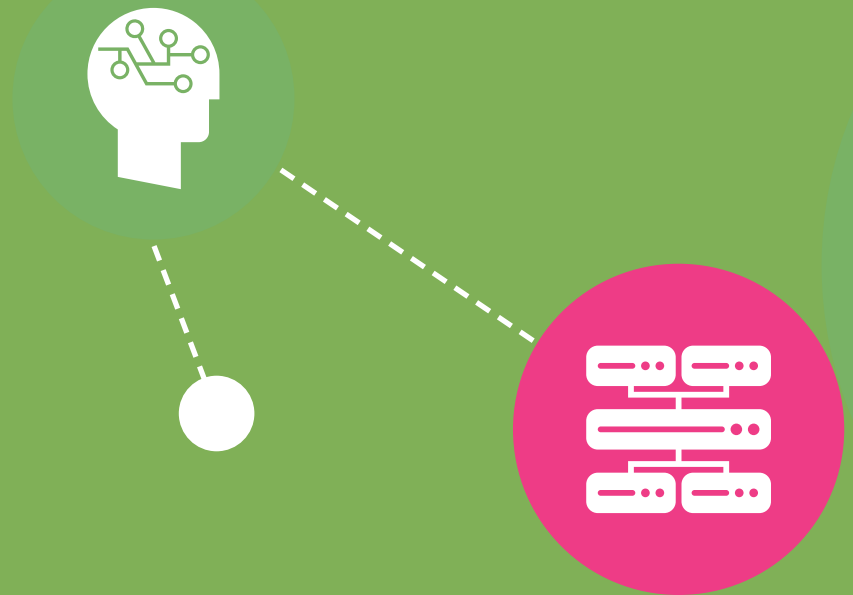
PETRAS

Industry Briefing

Cybersecurity for the Internet of Things and Artificial Intelligence in the Ambient Environment Sector

Zakiyya Adam



About PETRAS

The PETRAS National Centre of Excellence for IoT Systems Cybersecurity exists to ensure that technological advances in the Internet of Things (IoT) are developed and applied in consumer and business contexts, safely and securely. This is done by considering social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

The Centre is a consortium of 22 research institutions and the world's largest socio-technical research centre focused on the future implementation of the Internet of Things. The research institutions are: University College London, Imperial College London, University of Oxford, Lancaster University, University of Warwick, University of Southampton, Newcastle University, University of Nottingham, University of Bristol, Cardiff University, University of Edinburgh, University of Surrey, Coventry University, Northumbria University, Tate, University of Glasgow, Cranfield University, De Montfort University, Durham University, University of Manchester, Royal Holloway, University of London, and University of Strathclyde.

As part of UKRI's Security of Digital Technologies at the Periphery (SDTaP) programme, PETRAS runs open, national level funding calls which enable us to undertake cutting edge basic and applied research. We also support the early adoption of new technologies through close work with other members of the SDTaP programme, such as InnovateUK, supporting demonstrations of new technology and commercialisation processes.

In addition, we build the capacity of the UK to remain a world leader in IoT through our training and development programmes for early career researchers. Finally, we offer consultancy services to the public and private sectors to provide decision makers with insight and advice on a range of cybersecurity related issues.

The wider PETRAS community has played a role in creating this report - in particular Dr Charles Morisset, Sector Lead for Ambient Environment at PETRAS, at Newcastle University for his critical role in review, and Emilie Didier from the PETRAS Business Development Team for her editorial overview.

Design work by Dr Catherine Wheller is based on original work by Dr Michael Stead.

This report should be referenced as follows:

Adam, Z. 2021. *Industry Briefing: Cybersecurity for the Internet of Things and Artificial Intelligence in the Ambient Environment,* PETRAS National Centre of Excellence for IoT Systems Cybersecurity, London, UK

DOI:

From the Director

It is my pleasure to present this Industry Briefing on Cybersecurity for the Internet of Things and Artificial Intelligence in the Ambient Environment sector. This is the fourth in a series of Industry Briefings, intended to link with and inform the six PETRAS Sectors: Ambient Environment, Supply Chains and Control Systems, Infrastructure, AgriTech, Health and Wellbeing, and Transport and Mobility.

PETRAS has a large network of industry partners and expert academics, and works directly in collaboration with these and government partners to ensure that research can be directly applied to benefit society, business and the economy. I am delighted to see that as a Centre dedicated to identifying and addressing some of the needs within IoT, PETRAS has managed to connect industry with social and physical scientists to work towards some of the major challenges and questions around the cybersecurity of the Internet of Things. As IoT technology develops at speed and embraces AI and machine learning 'at the Edge', so do the challenges around cybersecurity and systems, and it is critical that these are addressed by industry, government and academia.

We hope that these Industry Briefings, which have highlighted insights into the challenges of deploying IoT systems, provide a fresh perspective on the existing and emerging opportunities for industry and those working within the Ambient Environment sector. With exciting innovative ideas, we are positive that PETRAS will be able to encourage collaboration between academia and industry, supporting the opportunities these challenges present, and we look forward to opening these discussions.

I hope this Industry Briefing will catalyse further debate and collaboration between researchers and users, making the use of the IoT safe and trustworthy, and maximising its social and economic value to the UK.

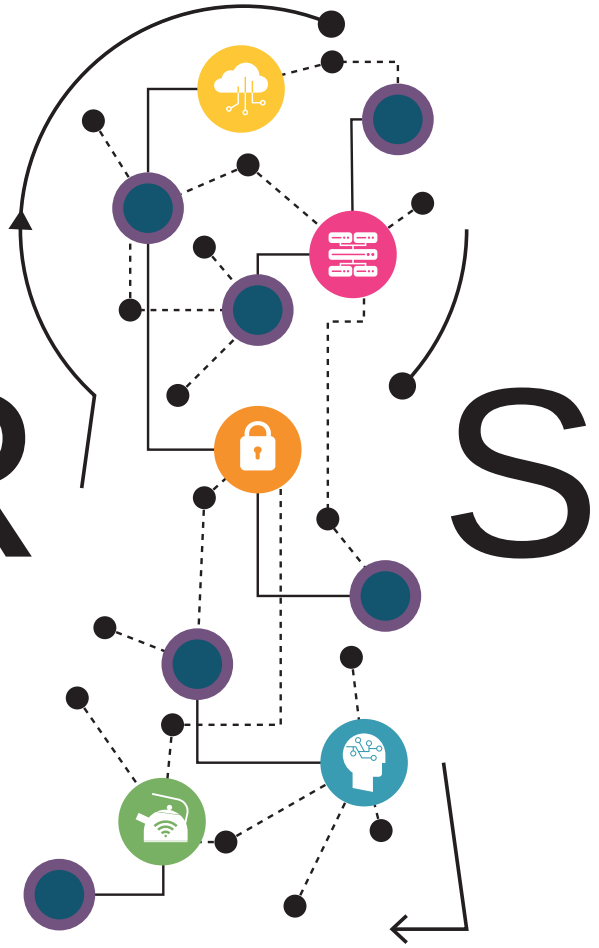
Professor Jeremy Watson CBE FREng
Director of the PETRAS National Centre of Excellence

UKRI Engineering and Physical Sciences Research Council

Contents

PETRAS

THE PETRAS NATIONAL
CENTRE OF EXCELLENCE
FOR IoT SYSTEMS
CYBERSECURITY



Executive Summary

The PETRAS National Centre of Excellence aims to ensure that technological advances in the Internet of Things (IoT) and Artificial Intelligence (AI) are developed and applied safely, and securely by considering social and technical issues in a variety of sectors.

The Ambient Environment sector is growing rapidly within both the public and private domains. More of the spaces in which we live, work and move are becoming ambient, able to recognise our presence, identify our preferences and adapt to our needs. Such environments include smart homes, autonomous vehicles, hospitals, workplaces, the education sector, emergency services, and many others.

Based on research undertaken over the last few years, this brief offers insights into general trends and challenges in cybersecurity research and policy for IoT devices and AI within the Ambient Environment sector.

Challenges

Wide adoption of IoT technology in the sector poses numerous challenges, including:

- **Cybersecurity** risks need to be managed to ensure confidentiality, integrity and availability of data;
- **Privacy** considerations are necessary to prevent infringements on individuals' human rights;
- **Data reliability** is crucial for the effective operation of heavily data reliant ambient environments;
- Balancing human control and automation, and building **accessibility** into the systems at the design stage, is crucial;
- The pervasiveness of ambient environments makes **trust** in them essential for functional societies;
- **Ethical principles** should underpin design choices and guide implementation of ambient environments.

Policy

The UK ranked second in the Government AI Readiness Index 2020 and there are a range of frameworks and standards providing guidance on the implementation of IoT:

- The **UK Code of Practice for Consumer IoT Security** and **ETSI European Standard 303 645** provide 13 guidelines to ensure consumer IoT products are designed with security in mind;
- **Secure By Design Legislation** is planned in the UK;
- A new ISO standard - **ISO 31700 Consumer Protection - Privacy by**

Design for Consumer Goods and Services – is under development;
- **PAS 185:2017** provides a comprehensive framework to help smart cities adopt a security-minded approach to the use of information and data in the built environment;
- The proposed **Artificial Intelligence Act** will be the first ever legal framework on AI;
- **UK-GDPR** and **DPA 2018** set out and legalise principles that need to be adhered to in order to ensure data protection.

Opportunities

The challenges posed by ambient environments raise the opportunity for further research. Broad areas of interest include:

- Ensuring stable **connectivity** between devices;
- **Security** of the systems;
- **Compatibility and durability** of the technology and devices;
- Development of **standards**;
- Extraction of knowledge and insights to provide **smart analysis and actions**.

PETRAS has rich and expanding experience of working within the sector, and is well-placed to face the privacy, ethics, trust, reliability, acceptability, and security concerns that will emerge as IoT becomes increasingly more embedded within the spaces we occupy.

Introduction

Scope of this brief

This brief offers a summary of general trends and challenges in cybersecurity research and policy for IoT (Internet of Things) devices and AI (Artificial Intelligence) in the Ambient Environment sector. The geographic scope encompasses the UK, EU and the global level, based on research collected up to 2021. In addition, the document will offer insights into PETRAS activities that focus on ambient environments.

The intended audience is primarily external industry and government organisations, including small, medium and large companies working around IoT, AI, security and cybersecurity in the Ambient Environment sector, who would like to gain insights into PETRAS's work and collaboration offers.

Sector background

Ambient environments are able to recognise human presence, identify the preferences of those present, and adapt to their immediate needs [1].

Ambient environments may be identified by several characteristics[2]:

1. **Context Aware** – identifies and utilises contextual and situational information
2. **Personalised** – tailored to the needs of each individual
3. **Anticipatory** – anticipates the needs of an individual without the conscious intervention of the individual
4. **Adaptive** – adapts to the changing needs of individuals
5. **Ubiquitous** – embedded and is integrated into everyday environments
6. **Transparent** – recedes into the background of daily life in an unobtrusive way

Ambient environments rely on numerous technologies that individually do not make an environment ambient, but collectively create flexible and intelligent services for users in the space: pervasive computing, ubiquitous communication, human-computer interaction (HCI), artificial intelligence (AI), machine learning (ML), sensor networks, and the seamless connectivity of smart devices[1,4].

In order to function, ambient environments **perceive** the state of the environment using sensors, **reason** about the data obtained, and then **act** to create some change to the state of the environment.

Perception is achieved using sensors able to detect a wide range of parameters including: position, motion, chemicals, humidity, light, radiation, temperature, sound, strain, pressure, velocity, and direction[4].

Ambient environment algorithms require various forms of reasoning. *User modeling* involves creating a baseline model of user behaviour that allows the environment to be customised for the user and to detect anomalies or changes to usual patterns. *Activity prediction and recognition* is the ability to recognise different activities, such as driving behaviour to determine whether a driver is falling asleep. *Spatial-temporal reasoning* and *decision making* allow the system to make sensible decisions based on an awareness of where the users are and have been during some period of time; such reasoning can be used to analyse trajectories of people within a room and classify them as ‘having a clear goal’ or ‘being erratic’[4,5].

The system then acts on the reasoning, creating some change in the environment through the use of intelligent and assistive devices or robots, such as stopping and parking a vehicle automatically if it detects that the driver is falling asleep[4].

Ambient environments include smart homes, autonomous vehicles, hospitals, workplaces, the education sector, emergency services, and many others[1].

Internet of Things and AI Challenges

Numerous challenges arise regarding the use of IoT and AI technology within ambient environments. This section outlines some of the challenges concerning PETRAS's key areas of focus, namely Privacy, Ethics, Trust, Reliability, Accessibility and (Cyber)Security.

(Cyber)Security

Cybersecurity is concerned with the protection of networks, devices and data from attacks and unauthorised access. It is the practice of ensuring confidentiality, integrity and availability of data [6]. There are four classes of cybersecurity risk: actions of people; systems and technology failures; failed internal processes; and external events[7]. Cybersecurity should be at the core of design strategy[8].

The European Union Agency for Network and Information Security (ENISA) publish the ENISA Threat Landscape (ETL) report each year which includes an assessment of the top cyber threats in the world that have occurred during the reporting period. The most recent 2020 ETL report[9] noted the fifteen most pressing cybersecurity challenges, which included malware, phishing, DDOS, botnets and ransomware. ENISA also publish reports detailing the specific risks for various ambient environments.

Smart Homes

Specific cybersecurity risks to smart homes (Figure 1) were identified by ENISA to include[10,11]:

Physical Attacks	removal of/ddamage to the assets; degrade/ prevent functionality; disrupt communications between smart home components; uploading new software; adding hardware components; changing device settings; extracting encryption keys etc.
Unintentional Damage (Accidental)	information leakage/sharing; erroneous use/ administration of devices or systems; using information from an unreliable source; unintentional change of data in an information system; inadequate design/ planning; lack of adaptation etc.
Disasters and Outages	natural disasters; environmental disasters; lack of resources/electricity; internet outages; loss of support services; absennce of personnel; strike; network outage etc.
Damage/Loss (IT Assets)	damage caused by a third-party; loss from DRM conflicts; loss of (integrity of) sensitive information; loss or destruction of devices/ storage media/ documents; loss of information in the cloud; information leakage etc.
Failures/ Malfunctions	failures/malfunctions of parts of devices; failuers/malfunctions of devices or systems; failures of hardware; software bugs; failures/disruptions of communication linkns (communication networks); failures/disruptions of main supply; failures/ disruptions of the power supply; failures/disruptions of service providers (supply chain); configuration errors etc.
Eavesdropping/ Interception/ Hijacking and Nefarious Actvity/Abuse	man-in-the-middle/ session hijacking; interception of information; interfering radiation; interception of compromising emissions; war driving; replay of messages; network reconnaissance and information gathering; repudiation of actions; identity fraud; unsolicited and infected email; denial of service; malicious code/ software activity; abuse of information leakage; generation and use of rogue certificates; manipulation of hardware and software; manipulation of information; misuse of audit tools; falsification of records; unauthorised use or administration of devices and systems; unauthorised access to the information system/ network; unauthorised use of software; unauthorised installation of software; compromising confidential information; abuse of authorisations; abuse of personal data; hoax; badware; remote activity (execution); targeted attacks (including Advanced Persistent Threat) etc.
Legal	violation of laws or regulations/ breach of legislation; failure to meet contractual requirements; unauthorised use of copyrighted material etc.

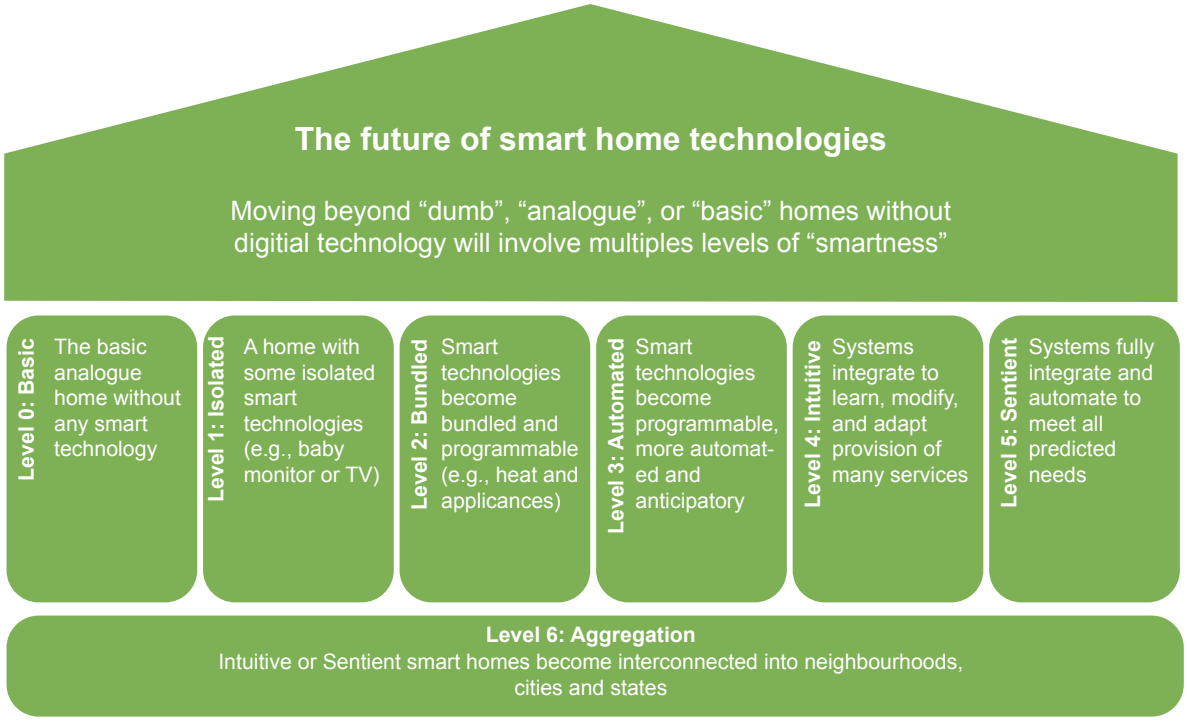


Figure 1.Levels of Smartness for Smart Home Technologies (adapted from Sovacool and Rio, 2020)[58]

Privacy

Informational Privacy

Informational privacy refers to the **ability to control the collection, storage, use, maintenance, dissemination/ disclosure, and disposition of one's personal information.** This extends beyond an individual's actions or status to include their thoughts, emotions, sensations and images[12,13]. In ambient environments, careful consideration needs to be given to the settings in which sensing data will be collected, the types of information that could be captured by the sensors, the inferences that might be drawn from that information, and what design measures might be needed to protect that information[14].

Studies have found that it is possible to re-identify individuals in anonymised datasets, rendering some current de-identification methods to be insufficient[15]. Linking together several sources of data enables inferences on individuals' habits and preferences to be drawn. Thus, even if an IoT device is not designed or expected to capture sensitive information, its data streams can indirectly enable serious invasions of user privacy [16]. Users may consent to the collection of various forms of sensor data without accounting for the effect of them being analysed collectively.

A user's desire for convenience and connectedness generally dictates their privacy-related behaviours, and their opinions about external entities collecting smart home data depend on the perceived benefit from these entities[19,21]]. In public spaces, people are usually not aware of being monitored, which data about them are collected and their context. In such situations, it is not possible for the individual to take control[19]. Privacy protection should be designed into IoT technologies.

Design of privacy measures needs to account for inferences that may be made despite efforts to protect data. Despite encryption, private in-home activities have been shown to be inferable by passive network observers - such as internet service providers - using encrypted metadata from commercially available smart home devices. For example, the Geeni lightbulb has only two states (on and off) and these

are reflected in the network send/receive rates. State changes are clearly observable as spikes in traffic rate, which could indicate when someone in a smart home turns the lights on and off. This information could in turn correlate with sleep patterns or home occupancy[20].

Decisional Privacy

Decisional privacy refers to an **individual's right against unwanted access, including unwanted interference in making decisions and taking actions.** It focuses on the individual's choice and their freedom to make important decisions on how they behave[24,25].

Ambient environments, such as smart homes, are equipped with numerous sensors. Regardless of whether these have been selected and purchased by the individual or exist within a public space, such technology raises concerns regarding constant surveillance[23]. When people suspect that they are being watched or recorded, their beliefs, movements, and association change[23]. The notion of peoples' actions and conversations being analysed within ambient environments affects the nature of those actions and conversations. Thus, ambient environments have the potential to interfere in an individual's decision making and actions.

More explicitly, ambient environments have the ability to directly impose certain behaviours on occupants within the space. For example, a paternalistic approach may result in obese citizens being denied access to public escalators and being forced to take the stairs[24]. Private conversations may identify an individual as being a potential political dissident or criminal; if their home was equipped with smart locks on the doors, it would be possible to effectively place them under house arrest[23]. During a global pandemic, a state could physically enforce lockdown on its citizens.

Reliability

The number of smart homes is expected to rise from over 221 million in 2020 to more than 482 million in 2025[25]. And the vast number of IoT devices - 12.6 billion in 2020 - is forecast to increase to 26.9 billion IoT connections by 2026, growth of 13% over the six year period[26].

The high volume of data generated by these devices raises numerous challenges regarding reliability. A systematic and comprehensive survey on IoT Big Data (IoTBD), published in December 2020, identified 13 V's of Big Data in IoT[27].

These 13 challenges are outlined below:

Volume: vast amounts of data
Variety: multi-source data generated in disparate formats
Velocity: real-time data generated at high velocity
Veracity: uncertainty regarding truthfulness of captured data (data inaccuracy)
Value: data-driven knowledge informing the actions and decisions
Variability: dynamicity associated with the data or data sources
Visualisation: graphics/ visuals to summarise knowledge to the end-user
Validity: uncertainty about data accuracy due to degradation after data has been acquired
Vulnerability: insecure data that is susceptible to security and privacy attacks
Volatility: short-term freshness of data and the temporal irrelevance of past data for analysis
Venue: varying access rights, ownership and non-interoperability of multiple venues used by data since its origin
Vocabulary: semantically representing data using ontologies, metadata, hashtags, data handles, dictionaries etc.
Vagueness: data ambiguity and incompleteness when combining data from multiple sources or diverse paradigms.

Accessibility

Within ambient environments, there is a shift towards greater automation of previously human operator-controlled activities. Smart devices and their underlying algorithms are increasingly controlling processes, services and devices, such as heating and lighting. This raises questions regarding **how much control humans should retain** over smart services. Whether humans should be able to intervene, take control and even stop a smart service, or if automatic systems will have no option for human intervention [22,33].

The importance of balancing human control and automation is pertinent to three distinct concerns:

1. **Error-prone behaviour of AI.** High quality data are essential for high quality algorithms. Two algorithms designed to carry out the same task but developed using different training data and algorithmic constraints may result in very different results/ predictions. AI systems based on incomplete or biased training data can lead to inaccurate outcomes [22,34].
2. **Rigidity.** Small deviations from standard routines or processes may render the system unable to handle the request.
3. **Missing transparency and traceability.** Lack of traceability results in unreproducible outcomes and a lack of accountability[19].

Ambient environments should be used as a tool for people to make more informed and mature decisions. The design goal should be that “smart spaces make people smarter” [19]. People should not only be in control of the systems, they should “own the loop”. People should be in control of the degree of human intervention and decision making and the configuration of system automation. In order for these trade-off decisions to be available to individuals, the options and types of balance must be anticipated and carefully built into the system at the design phase.

Trust

AI systems should be introduced in ways that build trust and understanding, follow fundamental human principles and values, and safeguard the well-being of people and the planet. Trust in AI can only be attained by fairness, transparency, accountability and regulation[35,36].

The pervasiveness of digital technologies makes trusting them essential for societies to operate effectively. Constant supervision of a machine learning algorithm used to make a decision is unfeasible. Conversely, a complete lack of supervision may lead to serious risks. Therefore, it is crucial to identify an effective way of trusting digital technologies so that we can harness their value, while protecting fundamental rights and fostering the development of open, tolerant and just information societies. This is especially important in hybrid systems involving human and artificial agents [36,37].

Fairness. Fairness and impartiality are crucial for developing trust in AI. We must ensure that decisions are free from bias and discrimination, and do not deepen already entrenched social inequalities. This is challenging as it is impossible to know what algorithms that are based on neural networks are actually learning when you train them with data[31].

Transparency. There are two main challenges pertaining to transparency. Firstly, understanding why an autonomous system made a particular decision. Transparency may be very difficult with modern AI systems, especially those based on deep learning systems, often referred to as ‘black boxes’. To ensure that a program does what you intend it to, and that there are no biases or unintended consequences, thorough validation, investigation and evaluation of the program during development is required. In many cases, disclosure of source code or data may be unnecessary. Transparency is about the external behaviour of algorithms. In

regulating human behaviour, we do not look into the brain's neural circuitry, but rather observe behaviour and judge it against certain standards of conduct[31]. Secondly, the proprietary nature of software and data. Many companies view their software and algorithms as valuable trade secrets and may not be willing to divulge how they address a particular problem. When using third-party software, public bodies sacrifice their ability to exercise meaningful oversight of algorithm operation and functioning as well as their ability to comply with their own mandated obligations of transparency and reason-giving. Algorithm setup often remains undisclosed to the purchasing public body, to those adversely affected by it, and/or to citizens at large[33].

Ethics

It is widely accepted that there are five foundational principles of ethics: **beneficence** (do good), **nonmaleficence** (do no harm), **autonomy** (respect for independence; self-determination), **justice** (fairness; bias; discrimination), and **fidelity** (trust)[34]. Challenges pertaining to some of these – such as privacy, fairness and transparency - have been discussed in previous sections.

In 2019, the IEEE published their report, **Ethically Aligned Design**, providing a vision for human-centric design of autonomous and intelligent systems[35].

The IEEE propose the following General Principles:

1. **Human Rights:** created and operated to respect, promote, and protect internationally recognised human rights;
2. **Well-Being:** adopt increased human well-being as a primary success criterion for development;
3. **Data Agency:** empower individuals with the ability to access and securely share their data, and to maintain people's capacity to have control over their identity;
4. **Effectiveness:** creators and operators shall provide evidence of the effectiveness and fitness for purpose;
5. **Transparency:** the basis of a particular decision should always be discoverable;
6. **Accountability:** created and operated to provide an unambiguous rationale for all decisions made;
7. **Awareness of Misuse:** creators shall guard against all potential misuses and risks of operation; and
8. **Competence:** creators shall specify and operators shall adhere to the knowledge and skill required for safe and effective operation.

Policy and Legislation

UK

Consumer Devices

UK Code of Practice for Consumer IoT Security. Published in 2018, the standard outlines 13 guidelines to ensure consumer IoT products are secure by design. They are outcome-focused, rather than prescriptive, giving organisations the flexibility to innovate and implement solutions appropriate for their products. Top 3 recommendations: no default passwords, implement a vulnerability disclosure policy, and keep software updated[36].

ETSI European Standard 303 645 (ETSI EN 303 645). Published in June 2020, developed by the European Standards Organisation. Based on the first globally applicable standard for consumer IoT - ETSI TS 103 645 - released in February 2019. Designed to prevent large-scale, prevalent attacks against smart devices by establishing a security baseline for connected consumer products and provides a basis for future IoT certification schemes. The standard sets out the same 13 recommendations as the UK Code of Practice[37-39].

Secure By Design legislation. Planned in the UK to enforce internationally accepted standards. Legislation will enforce the top three security recommendations of the UK Code of Practice for Consumer IoT Security, also included in ETSI EN 303 645: (1) customers must be informed at the point of sale the duration of time for which a smart device will receive security software updates; (2) ban on manufacturers using universal default passwords, often pre-set in a device's factory settings; and (3) manufacturers will be required to provide a public point of contact to make it simpler for anyone to report a vulnerability. The announcement, made on 21 April 2021, noted that government will legislate when parliamentary time allows[40,41].

ISO 31700 Consumer Protection - Privacy by Design for Consumer Goods and Services. A new ISO standard currently under development. The standard will address the design process to ensure consumer goods and services meet consumers' domestic processing privacy needs as well as the personal privacy requirements of Data Protection[42,43].

The UK Code of Practice for Consumer IoT Security - Where We Are and What Next. In April 2021, DCMS published the PETRAS report assessing the impact of the code of practice and suggested areas for further consideration. Three issues are identified requiring urgent consideration: (1) use of IoT devices by perpetrators of domestic abuse; (2) fitness devices have proven easy to compromise and reveal deeply personal information about people's bodies, their homes and their movements, and (3) children's IoT

connected toys due to the implications of embedded cameras and microphones for a child's (or parent's) protection and right to privacy[44].

Smart Cities

PAS 185:2017 - Smart Cities Specification for Establishing and Implementing a Security-Minded Approach - provides a comprehensive framework for the use of information and data in the built environment (BSI, 2017). The smart city security management plan needs to account for people, physical, data and information, and technology:

- **People:** Security competence of staff fulfilling specific roles; security screening and vetting; induction requirements; general security training and awareness; role-specific security training; demobilisation of personnel and organisations
- **Physical:** Physical security measures at locations processing sensitive data or information; protective measures for equipment handling city data and/or information; protective measures for infrastructure supporting data and information sharing and access by citizens
- **Data and Information:** Security features required for the city's data and information architecture; managing the accuracy, authenticity and long-term utility of city data and information; managing the security of data and information that could be used to cause harm to assets, services and/or the city's citizens; data and information sharing and publication
- **Technology:** Cyber security of systems and the interconnections and interactions between them; interoperability of systems; configuration management and change control for systems processing city data and/or information; level of software trustworthiness; secure retention, deletion, destruction and/or removal of access to city data and information

Artificial Intelligence

In April 2021, the European Commission proposed the first ever legal framework on AI, the **Artificial Intelligence Act**. The framework addresses the risks of AI and aims to ensure the protection of fundamental rights and user safety, as well as trust in the development and uptake of AI. The legal framework will apply to both public and private actors inside and outside the EU as long as the AI system is placed on the Union market or its use affects people located in the EU[43,44].

The **2018 Coordinated Plan** laid the foundation for policy coordination on AI and encouraged Member States to develop national strategies. Since then, the technological, economic and policy context on AI has considerably evolved. To remain agile and fit for the purpose, in 2021 the Coordinated Plan will be reviewed[45].

The European Parliament and the Member States will need to adopt the Commission's proposals on a European approach for Artificial Intelligence in the ordinary legislative procedure. Once adopted, the final Regulations will be directly applicable across the EU. In parallel, the European Commission will continue to collaborate with Member States to implement the actions announced in the Coordinated Plan[45].

Data Protection

UK-GDPR. The UK General Data Protection Regulation (UK-GDPR) transcribes into UK law the EU General Data Protection Regulation (EU-GDPR) following Brexit. The key principles, rights and obligations remain the same. However, there are implications for the rules on transfers of personal data between the UK and the EEA. The UK-GDPR sets out seven principles: (1) lawfulness, fairness and transparency; (2) purpose limitation;
(3) data minimisation; (4) accuracy;

(5) storage limitation; (6) integrity and confidentiality (security); and (7) accountability[48,49]. UK-GDPR requires the integration of data protection into processing activities and business practices, from the design stage right through the lifecycle. This concept is not new; it was previously known as 'privacy by design' and has always been part of data protection law. The key change with the UK-GDPR is that it is now a legal requirement [49].

Data Protection Act. The Data Protection Act (DPA) 1998 was updated in 2018 to account for additional stipulations introduced in line with GDPR. The DPA 2018 is the UK's legal implementation of the GDPR[51,52].

Personal Data. Understanding what constitutes as *personal data* is fundamental to legal discussions around ambient environments. Pseudonymised data can help reduce privacy risks by making it more difficult to identify individuals, but it is still personal data. If personal data can be truly anonymised, then the anonymised data is not subject to the UK-GDPR[52]. Ambient environments collect data on a wide range of parameters, and determining which data may be considered to be personal data is both important and complicated. For example, governments, companies, and other entities are either using or planning to rely on thermal imaging as an integral part of their strategy to reopen economies post COVID-19. A person's body temperature is personal data concerning their health and therefore constitutes "special category" personal data under Article 9 of the GDPR. The ICO warns organisations that want to deploy temperature checks or thermal cameras on site that *"any monitoring of employees needs to be necessary and proportionate, and in keeping with their reasonable expectations."* However, it does seem to allow such practices in principle after a Data Protection Impact Assessment is conducted. The stance on thermal cameras differs in other European countries. In France, for example, *"the mere verification of temperature through a manual thermometer (such as, for example, the contactless thermometers using infrared) at the entrance of a place, without any trace being recorded, and without any other operation being effectuated (such as taking notes of the temperature, adding other information etc.), does not fall under data protection law"*. However, things fundamentally change when thermal scanning through cameras is involved; the French Data Protection Agency, CNIL, issued a prohibition: *"According to the law (in particular Article 9 [of the General Data Protection Regulation] GDPR), and in the absence of a law that expressly provides this possibility, it is forbidden for employers to: (1) collect the temperature of employees or visitors as soon as it is recorded through an automated process or in a paper file; and (2) collect temperature in an automated manner or to use tools such as thermal cameras"* [53].

Comparative Global Standing

The Government AI Readiness Index 2020 developed by Oxford Insights and the International Research Development Centre (IDRC) draws on 33 indicators across 10 dimensions to rank Governments across the world on their position to take advantage of AI enabled technologies[54]. The index is based on three fundamental pillars of government AI readiness: (1) the Government needs to be willing to adopt AI, and able to adapt and innovate to do so; (2) the Government needs a good supply of AI tools from the technology sector; and (3) these tools need to be built and trained on high quality and representative data, and need the appropriate infrastructure to be delivered to and used by citizens. The US ranked the highest, with the UK in second place. Finland, Germany and Sweden ranked third, fourth and fifth respectively.

Opportunities

A systematic review of IoT-based applications in smart environments, published in February 2021, identified five broad areas that need to be addressed: connectivity; security; compatibility and durability; standards; and smart analysis and actions[55].

Connectivity. Stable connections between devices are a critical component of ambient environments. Existing communication models – in which a centralised server/client paradigm is used for authenticating, authorising, and connecting several nodes across a network – will not suffice.

Security. The large numbers of new hubs being added to the networks and connected to the internet provide attackers with innumerable attack vectors to invade the system. A problem that is exacerbated by the security deficiencies present within many of these devices.

Compatibility and Durability. Rapid expansion of the IoT has led to various technologies vying to become a standard. This may cause future problems regarding compatibility, requiring the development and deployment of additional hardware and software to ensure that devices from different manufacturers and industries can be interconnected. Additionally, some of these technologies will ultimately become obsolete within a few years. IoT devices, however, tend to last for many years so they should be able to function even when their producer goes out of service.

Standards. Comprised of network protocols, data aggregation, and communication protocols, standards are necessary to build an IoT infrastructure. Two main issues face the adoption of standards in IoT: (1) standards for managing unstructured data, and (2) technical skills required for leveraging new tools for data collection.

Smart Analysis and Actions. Extraction of knowledge and insights for analysis. Challenges facing the adoption of smart operations in IoT include:

- The security and privacy of information
- The influence of machines on human behaviour
- Unpredictable conditions of machines operations
- The interoperability of machines
- The moderate adoption of recent technologies
- The inaccurate analysis because of the uncertainty in the data and/or models
- The inability of traditional systems to analyse unstructured data
- The inability of traditional systems to manage streaming data

Additional opportunities for future research within the Ambient Environment sector include assessment of how to:

- Compute the **value of information** considering accuracy, uncertainty, cost and multiple data sources
- Establish a **link between a sensor and decisions** made at higher-level based on data from that sensor
- Decide **information ownership, stakeholders and legal responsibility** from multiparty sensor systems
- Integrate **demand side response mechanisms**, to nudge user behaviour to optimise overall performance
- Design **visualisations** to convey dynamic constructs such as risk and trust that are meaningful to users
- Measure the impact of increasing ambient technology on **user perception of security and privacy issues**
- Design edge systems to address **sustainability** and not increase the volume of **e-waste** produced
- Reduce **ambient sensing costs** with dynamic transmission rates or self-generating/ healing networks
- Create incentives for **diverse actors** in the deployment, monitoring and maintenance of sensor IoT systems
- Build **effective training methods/exercises** to help users/stakeholders handle security and safety incidents
- **Augment information from sensors** with rich real-time, crowdsourced information from users, and deliver value/insights back to users in return.

PETRAS in the UK Research Landscape

There are numerous research centres focused on IoT and cybersecurity related issues in the Ambient Environment sector. A few notable ones include:

The BRE **Centre for Smart Homes and Buildings** (CSHB) which launched in September 2017 and is a collaborative hub for industry, academia and government. CSHB works to ensure that smart technologies and services meet the needs of end users, to provide clarity on the performance of devices and systems, and to address emerging risks;
The **Connected Places Catapult** which is the UK's innovation accelerator for cities, transport, and places. It is human-centred and solution-led, advocates for standards which enable interoperability, replicability and scale, and it looks to connect people in terms of physical connectivity, social connectivity and digital connectivity;
The **Centre for Digital Built Britain** (CDBB) which is a partnership between the Department for Business, Energy & Industrial Strategy (BEIS) and the University of Cambridge, established by HM Government in the 2017 Autumn Budget as the home of the UK BIM and Digital Built Britain Programmes. Security for digital construction - growth in the use of digital technologies, and the increasing sophistication and connectivity of cyber-physical systems working in real-time to influence outcomes - is a key area of focus for CDBB.

PETRAS has a strong, and expanding, research focus in Ambient Environments. There are over 25 projects within the sector, either completed or ongoing, some of which are detailed in Tables 1 and 2. Further details on all of the projects can be found at: https://petras-iot.org/projects/?_sft_sector=ambient

PETRAS has a dedicated Business Development team who connect the public and private sectors with a network of transdisciplinary academic experts, to enable research collaborations that address social and technical issues relating to the cybersecurity of IoT devices, systems and networks.

If you are a research institution, private or public sector organisation interested in collaborating with PETRAS, please contact petras@ucl.ac.uk.

Table 1. A selection of completed PETRAS projects in cybersecurity in the Ambient Environment sector

Project	Partners	Description
House Training the Internet of Things (HTIoT)	• BBC; • BRE; • V&A; • Tate Modern; • DCMS; • Pinsent Masons	• Considered acceptability and adoption of IoT products in the home setting through the creation of a series of speculative designs of plausible future products and services that explore aspects of privacy, security, and trust within the domestic context. The project sought to make recommendations for the design of Internet of Things devices that negate negative perceptions which may affect acceptability and adoption.
Displays and Sensors on Smart Campuses (DiSSC)	• O2 Telefonica; • Teoco	• Explored the issue of IoT trust in the context of a campus network. The project sought to start a smart campus IoT testbed, in Lancaster, that incorporates two important IoT elements - sensor units and displays - and to produce the world's first research insights into the use of displays portals for trusted access to proximate IoT devices. It explored security and privacy related issues such as ownership of personal data when collected in public spaces, data ownership of information collected on personal devices, data provenance, and the right of being forgotten while contributing to the generation of crowd-knowledge.
User-centric Design for Adoption of IoT (UDAIoT)	• The Financial Conduct Authority; • Which?	• Looked to provide a baseline of consumer and citizen understanding of ethics, privacy, and trust in IoT by uncovering psychological representations of the concepts. The project focused on: (1) developing psychological representations based on machine learning; (2) engagement with consumer groups; (3) mapping of representations of beliefs pertaining to ethics, privacy and trust from a managerial and organisational cognition perspective; and (4) developing a portfolio of IoT scenarios illustrating the breadth of ethics, privacy, and trust issues.
Resolving Conflicts in Public Spaces (ReCoPS)	• SSB (Rail Standards and Safety Board); • Stagecoach South	• Analysed the tensions between the benefits offered by IoT enabled services in public spaces (e.g. using in situ displays to guide users through rail interchanges or an airport) and issues arising regarding prioritisation of displays and actuators. The project identified potential threats caused by malicious actuation/ misinformation.
Making the Invisible Visible - Secure, Trustworthy IoT Displays and Sensors for Urban Environments in CityVerve (IDice)	• Lancaster City Council; • CityVerve	• Sought to: (1) explore the use of IoT sensors and displays to provide users with trusted visibility of local IoT devices in urban environments; (2) demonstrate the potential of such an approach using IoT air quality sensors and displays deployed at three locations within the CityVerve region; (3) report on user attitudes to IoT visibility and produce guidelines for future deployments; (4) conduct an initial study of how display-based sensor and data visibility can be used in conjunction with maps of IoT sensors to further user awareness and trust in an otherwise invisible IoT infrastructure

Table 2. A selection of ongoing PETRAS projects in cybersecurity in the Ambient Environment sector

Project	Partners	Description
The Reappearing Computer: Foregrounding Privacy in IoT (REAPPEAR)	• Mozilla Foundation; • ThingsCon; • Simply Secure	• Explores how it might be possible, as computers have 'disappeared' into common objects, to cause the computer to 'reappear'. The project works with end-users and industry to understand the anxieties caused by the hidden activities of consumer devices and demonstrates new design patterns for more trusted products. This might mean devices that show their connections to the wider world and help people to understand the hidden complexities behind them, or that better expose the distinction between tasks carried out on devices and those relying on a greater intelligence somewhere on the internet.
Markets for Connected Space Sharing (MaCs)	• Creative Space Management	• Connects technological and legal aspects to make better use of shared workspaces. MaCs is developing a novel shared space data management platform which integrates data anonymisation processes. MaCs also investigates the legal aspects, starting with a Data Protection Impact Assessment and producing a set of legal guidelines for smart building data collection.
Intelligible Cloud and Edge AI (ICE-AI)	• BBC R&D	• Addresses how AI systems can support human trust and ethically-sensitive design. This is done by exploring the development of robust user behaviours and perception of AI in the cloud and AI at the edge. ICE-AI considers social and conceptual understandings with user experience of algorithmic systems in the cloud and at the edge. The team aim to develop and evaluate at least one prototype interface
Responding to Attacks and Compromise at the Edge (RACE)	• Thales	• Develops methods to enable IoT systems to respond to attacks and to continue to operate even after being partially compromised. RACE is articulated into four broad themes of work: understanding attacks and mitigation strategies, maintaining an adequate representation of risk to the other parts of the system by understanding how attacks can evolve and propagate, understanding the impact of the compromise upon the functionality of the system and selecting countermeasure strategies taking into account trade-offs between minimising disruption to the system operation and functionality provided and minimising the risk to the other parts of the system.

Glossary

AI (Artificial Intelligence) is “the theory and development of computer systems able to perform tasks normally requiring human intelligence, such as visual perception, speech recognition, decision-making, and translation between languages” [56]

ML (Machine Learning) is “the use and development of computer systems that are able to learn and adapt without following explicit instructions, by using algorithms and statistical models to analyse and draw inferences from patterns in data” [57]

End Notes

[1] Z. Mahmood, Ed., Guide to Ambient Intelligence in the IoT Environment: Principles, Technologies and Applications. Springer, 2019.

[2] G. Acampora, D. J. Cook, P. Rashidi, and A. V. Vasilakos, “A Survey on Ambient Intelligence in Health Care,” Proc IEEE Inst Electr Electron Eng, vol. 101, no. 12, pp. 2470–2494, Dec. 2013, doi: 10.1109/JPROC.2013.2262913.

[3] J. C. Augusto, H. Nakashima, and H. Aghajan, “Ambient Intelligence and Smart Environments: A State of the Art,” in Handbook of Ambient Intelligence and Smart Environments, H. Nakashima, H. Aghajan, and J. C. Augusto, Eds. Boston, MA: Springer US, 2010, pp. 3–31. doi: 10.1007/978-0-387-93808-0_1.

[4] D. J. Cook, J. C. Augusto, and V. R. Jakkula, “Ambient intelligence: Technologies, applications, and opportunities,” Pervasive and Mobile Computing, vol. 5, no. 4, pp. 277–298, 2009, doi: https://doi.org/10.1016/j.pmcj.2009.04.001.

[5] BrainAble, D.5.1: Ambient Intelligence in Assistive Technologies. Barcelona Digital Centre Tecnològic, 2010. Accessed: Mar. 18, 2021. [Online]. Available: https://cordis.europa.eu/docs/projects/cnect/7/247447/080/deliverables/D5-1-Ambient-Intelligence-in-Assistive-Technologies-v1-1.pdf

[6] CISA, “What is Cybersecurity? | CISA,” Cybersecurity & Infrastructure Security Agency, 2019. https://us-cert.cisa.gov/ncas/tips/ST04-001 (accessed Apr. 17, 2021).

[7] J. J. Cebula and L. R. Young, “A Taxonomy of Operational Cyber Security Risks,” Software Engineering Institute, CMU/SEI-2010-TN-028, Dec. 2010. Accessed: Apr. 18, 2021. [Online]. Available: https://apps.dtic.mil/sti/pdfs/ADA537111.pdf

[8] P. Siddhanti, P. M. Asprion, and B. Schneider, “Cybersecurity by Design for Smart Home Environments,” 2019.

[9] ENISA, The Year in Review: ENISA Threat Landscape. ENISA, 2020. Accessed: May 14, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/year-in-review

[10] ENISA, “Security and Resilience of Smart Home Environments,” ENISA, Report/Study, 2015. Accessed: Apr. 22, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/security-resilience-good-practices

[11] ENISA, “Threat Landscape for Smart Home and Media Convergence,” ENISA, Report/Study, 2015. Accessed: Apr. 22, 2021. [Online]. Available: https://www.enisa.europa.eu/publications/threat-landscape-for-smart-home-and-media-convergence

[12] S. A. Alpert, “Protecting Medical Privacy: Challenges in the Age of Genetic Information,” Journal of Social Issues, vol. 59, no. 2, pp. 301–322, 2003, doi: https://doi.org/10.1111/1540-4560.00066.

[13] R. J. R. Levesque, “Informational Privacy,” in Adolescence, Privacy, and the Law, New York: Oxford University Press, 2016. doi: 10.1093/acprof:oso/9780190460792.003.0004.

[14] N. Martinez-Martin et al., “Ethical issues in using ambient intelligence in health-care settings,” The Lancet Digital Health, vol. 3, no. 2, pp. e115–e123, 2021, doi: https://doi.org/10.1016/S2589-7500(20)30275-2.

[15] L. Rocher, J. M. Hendrickx, and Y.-A. de Montjoye, “Estimating the success of re-identifications in incomplete datasets using generative models,” Nature Communications, vol. 10, no. 1, p. 3069, Jul. 2019, doi: 10.1038/s41467-019-10933-3.

[16] J. Kröger, “Unexpected Inferences from Sensor Data: A Hidden Privacy Threat in the Internet of Things,” in Internet of Things. Information Processing in an Increasingly Connected World, Cham, 2019, pp. 147–159.

[17] M. Friedewald, E. Vildjiounaite, Y. Punie, and D. Wright, “Privacy, identity and security in ambient intelligence: A scenario analysis,” Telematics and Informatics, vol. 24, no. 1, pp. 15–29, Feb. 2007, doi: 10.1016/j.tele.2005.12.005.

[18] S. Zheng, N. Apthorpe, M. Chetty, and N. Feamster, “User Perceptions of Smart Home IoT Privacy,” Proc. ACM Hum.-Comput. Interact., vol. 2, no. CSCW, Nov. 2018, doi: 10.1145/3274469.

[19] N. Streitz, D. Charitos, M. Kaptein, and M. Böhlen, “Grand challenges for ambient intelligence and implications for design contexts and smart societies,” Journal of Ambient Intelligence and Smart Environments, vol. 11, no. 1, pp. 87–107, Jan. 2019, doi: 10.3233/AIS-180507.

[20] N. Apthorpe, D. Y. Huang, D. Reisman, A. Narayanan, and N. Feamster, “Keeping the Smart Home Private with Smart(er) IoT Traffic Shaping,” Proceedings on Privacy Enhancing Technologies, vol. 2019, no. 3, pp. 128–148, Jul. 2019, doi: 10.2478/popets-2019-0040.

[21] R. J. R. Levesque, “Decisional Privacy,” in Adolescence, Privacy, and the Law, New York: Oxford University Press, 2016. doi: 10.1093/acprof:oso/9780190460792.003.0002.

[22] M. Lanzing, “‘Strongly Recommended’ Revisiting Decisional Privacy to Judge Hypernudging in Self-Tracking Technologies,” Philos. Technol., vol. 32, no. 3, pp. 549–568, Sep. 2019, doi: 10.1007/s13347-018-0316-4.

[23] A. Henschke, “Privacy, the Internet of Things and State Surveillance: Handling Personal Information within an Inhuman System,” Moral Philosophy and Politics, vol. 7, no. 1, pp. 123–149, Apr. 2020, doi: 10.1515/mopp-2019-0056.

[24] K. Finch and O. Tene, “Welcome to the Metropticon: Protecting Privacy in a Hyperconnected Town,” Fordham Urban Law Journal, vol. 41, no. 5, p. 1581, Mar. 2016.

[25] Statista, “Smart Home - number of households in the segment Smart Home worldwide 2025,” Statista, 2021. https://www.statista.com/forecasts/887613/number-of-smart-homes-in-the-smart-home-market-worldwide (accessed Apr. 22, 2021).

[26] Ericsson, “Ericsson Mobility Report,” Ericsson, Sweden, Nov. 2020. Accessed: Apr. 21, 2021. [Online]. Available: https://www.ericsson.com/en/mobility-report/reports

[27] M. Bansal, I. Chana, and S. Clarke, “A Survey on IoT Big Data: Current Status, 13 V’s Challenges, and Future Directions,” ACM Comput. Surv., vol. 53, no. 6, p. 131:1-131:59, Dec. 2020, doi: 10.1145/3419634.

[28] N. Streitz, “Beyond ‘smart-only’ cities: redefining the ‘smart-everything’ paradigm,” J Ambient Intell Human Comput, vol. 10, no. 2, pp. 791–812, Feb. 2019, doi: 10.1007/s12652-018-0824-1.

[29] FRA, “Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights,” EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2019. Accessed: Apr. 21, 2021. [Online]. Available: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf

[30] V. Dignum, “Ethics in artificial intelligence: introduction to the special issue,” Ethics Inf Technol, vol. 20, no. 1, pp. 1–3, Mar. 2018, doi: 10.1007/s10676-018-9450-z.

[31] EPRS, “The ethics of artificial intelligence: issues and initiatives.,” European Parliamentary Research Service, 2020. Accessed: Apr. 23, 2021. [Online]. Available: https://data.europa.eu/doi/10.2861/6644

[32] L. Floridi and M. Taddeo, “What is data ethics?,” Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences, Dec. 2016, doi: 10.1098/rsta.2016.0360.

[33] M. Busuioc, “Accountable Artificial Intelligence: Holding Algorithms to Account,” Public Administration Review, vol. n/a, no. n/a, Aug. 2020, doi: https://doi.org/10.1111/puar.13293.

[34] K. S. Kitchener and R. F. Kitchener, “Social Science Research Ethics: Historical and Philosophical Issues,” in The Handbook of Social Research Ethics, 2455 Teller Road, Thousand Oaks California 91320 United States: SAGE Publications, Inc., 2009, pp. 5–22. doi: 10.4135/9781483348971.n1.

[35] IEEE, Ethically Alligned Design. IEEE, 2019. Accessed: May 09, 2021. [Online]. Available: https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf?utm_medium=undefined&utm_source=undefined&utm_campaign=undefined&utm_content=undefined&utm_term=undefined

[36] DCMS, “Code of Practice for Consumer IoT Security,” GOV.UK, Oct. 2018. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security (accessed Apr. 26, 2021).

[37] DCMS, “ETSI industry standard based on the Code of Practice,” GOV.UK, 2020. https://www.gov.uk/government/publications/etsi-industry-standard-based-on-the-code-of-practice (accessed Apr. 26, 2021).

[38] ETSI, “ETSI EN 303 645 V2.1.1 (2020-06),” REN/CYBER-0048, 2020. Accessed: Apr. 26, 2021. [Online]. Available: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[39] ETSI, “ETSI - Consumer IoT security,” ETSI. https://www.etsi.org/technologies/consumer-iot-security (accessed Apr. 26, 2021).

[40] DCMS and M. Warman, “New cyber security laws to protect smart devices amid pandemic sales surge,” GOV.UK, Apr. 21, 2021. https://www.gov.uk/government/news/new-cyber-security-laws-to-protect-smart-devices-amid-pandemic-sales-surge (accessed Apr. 26, 2021).

[41] DCMS and M. Warman, “Government response to the call for views on consumer connected product cyber security legislation,” GOV.UK, Apr. 21, 2021. https://www.gov.uk/government/publications/regulating-consumer-smart-product-cyber-security-government-response/government-response-to-the-call-for-views-on-consumer-connected-product-cyber-security-legislation (accessed Apr. 26, 2021).

[42] ISO/COPOLCO, Form 4: New Work Item Proposal. ISO, 2017. [Online]. Available: https://iapp.org/media/pdf/resource_center/ISO%20NWIP%20(Privacy%20by%20design%20for%20consumer%20goods%20and%20services).pdf

[43] ISO, “ISO/CD 31700,” ISO, n.d. https://www.iso.org/standard/76772.html?browse=tc (accessed Jun. 07, 2021).

[44] S. D. Burton, L. M. Tanczer, S. Vasudevan, S. Hailes, and M. Carr, “The UK Code of Practice for Consumer IoT Security - Where We Are and What Next,” PETRAS, Mar. 2021. Accessed: Apr. 26, 2021. [Online]. Available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/978692/The_UK_code_of_practice_for_consumer_IoT_security_-_PETRAS_UCL_research_report.pdf

[45] European Commission, “New rules for Artificial Intelligence – Q&As,” European Commission, Apr. 21, 2021. https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683 (accessed Jun. 07, 2021).

[46] European Commission, “Proposal for a Regulation laying down harmonised rules on artificial intelligence | Shaping Europe’s digital future,” Jun. 03, 2021. https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence (accessed Jun. 07, 2021).

[47] GDPR, “General Data Protection Regulation (GDPR) – Official Legal Text,” General Data Protection Regulation (GDPR), 2018. https://gdpr-info.eu/ (accessed May 09, 2021).

[48] ICO, “The principles,” ICO, Mar. 21, 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/ (accessed May 10, 2021).

[49] ICO, “Data protection by design and default,” ICO, Feb. 09, 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/ (accessed May 10, 2021).

[50] Data Protection Act, “Data Protection Act 2018,” 2018. https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted (accessed May 09, 2021).

[51] GOV.UK, “Data protection,” GOV.UK, n.d. https://www.gov.uk/data-protection (accessed May 09, 2021).

[52] ICO, “What is personal data?,” ICO, Jan. 01, 2021. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/ (accessed May 10, 2021).

[53] H. Schaller, G. Zanfir-Fortuna, and R. Hendricks-Sturrup, “THERMAL IMAGING AS PANDEMIC EXIT STRATEGY: LIMITATIONS, USE CASES AND PRIVACY IMPLICATIONS,” Future of Privacy Forum, 2020. https://fpf.org/blog/thermal-imaging-as-pandemic-exit-strategy-limitations-use-cases-and-privacy-implications/ (accessed May 10, 2021).

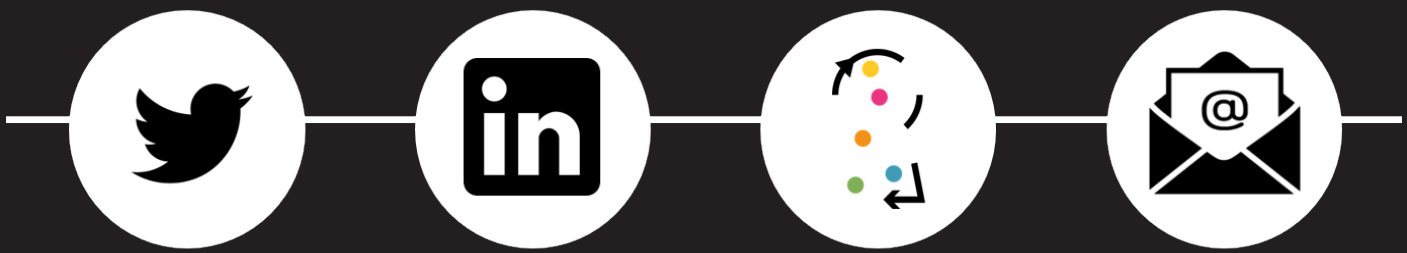
[54] Oxford Insights, “Government AI Readiness Index 2020,” Oxford Insights, 2020. https://static1.squarespace.com/static/58b2e92c1e5b6c828058484e/t/5f7747f29ca3c20ecb598f7c/1601653137399/AI+Readiness+Report.pdf (accessed May 10, 2021).

[55] Y. Hajjaji, W. Boulila, I. R. Farah, I. Romdhani, and A. Hussain, “Big data and IoT-based applications in smart environments: A systematic review,” Computer Science Review, vol. 39, p. 100318, Feb. 2021, doi: 10.1016/j.cosrev.2020.100318.

[56] Lexico, “Artificial Intelligence,” Lexico, n.d. https://www.lexico.com/definition/artificial_intelligence (accessed Feb. 14, 2021).

[57] Lexico, “Machine Learning,” Lexico, n.d. https://www.lexico.com/definition/machine_learning (accessed Feb. 14, 2021).

[58] Sovacool, B. K. and Rio, D. D. F. D. (2020) ‘Smart home technologies in Europe: A critical review of concepts, benefits, risks and policies’, Renewable and Sustainable Energy Reviews, 120, p. 109663. doi: https://doi.org/10.1016/j.rser.2019.109663.



TWITTER
@PETRASiot

LINKEDIN
linkedin.com/
school/petrasiot

WEBSITE
petras-iot.org

EMAIL
petras@ucl.ac.uk