1

Tracing the Path to Clever Computing

1.1 INTRODUCTION

Clever Computing, the convergence of physical sensing through the Internet of Things (IoT) with data-driven AI systems, is emerging within many settings of everyday life, like homes, workplaces, and public spaces. The IoT has long involved networked devices that sense and gather data about humans, things, and daily activities. But AI is increasingly being integrated into IoT systems to adapt the nature of user interactions, shift how data is used, and extend system autonomy. Clever Computing is often sold on the premise of increased convenience, safety, and efficiency. From a user perspective, the reality is often quite different, where systems may increase data surveillance and corporate control, erode citizen digital rights, and create a raft of new socio-technical and legal harms.

I argue that Clever Computing is not designed in a way that sufficiently accounts for social, ethical, and, most critically, *legal values*. Instead, to build Clever Computing systems that we want to live with now and in the future, technology design processes need to become human-centred *and* better account for the law. I propose *Accountable Design* as a novel, practically orientated approach to doing this. Laws often aim to protect humans, their rights, relationships, and environments by establishing responsibilities, requirements, and rules for those who can impact or harm those interests. Yet, situating what law means on the ground for technology design practices is often unclear. This book explores not only the implications of folding legal values into human-centred design processes but also how to move towards building more legally accountable Clever Computing systems.

Accountable Design is underpinned by extensive interdisciplinary research. It draws together methods, concepts, and frameworks from technology law, human–computer interaction (HCI), design research, applied ethics, and science and technology studies. Accountable Design shows how to integrate user needs and the legal obligations of designers in developing technologies that mitigate socio-technical and legal harms. As I will demonstrate, technology designers are already directly implicated and accountable for responding to a wide array of legal

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

requirements. Design is squarely at the centre of legislative endeavours to address risks stemming from Clever Computing systems. Measures aimed at protecting the societal values of privacy, security, trust, and safety – *by design* – exist within recent and upcoming legislation, particularly from the European Union (EU). Examples include:

- Privacy: EU General Data Protection Regulation 2016 (GDPR)[1] requires privacy by design through 'data protection by design and default' requirements and The EU Data Act 2023[2] mandates fair default data access.
- Security: The EU Amended Radio Equipment Directive 2014 (RED),[3] EU Cyber Resilience Act 2024 (CRA),[4] and the UK Product Security and Telecommunications Infrastructure Act 2023 (PSTI) Act[5] require increased security safeguards for the IoT by design.
- Trust and Safety: The EU Artificial Intelligence Act 2024 (AIA)[6] and EU Machinery Regulation 2023 (MAR)[7] set design and development requirements for high-risk AI systems and health and safety obligations when interacting with automated workplace systems.

Designers are charged with demonstrating how they are addressing the regulatory requirements within these frameworks. As a result, law itself is becoming a design brief, but what this means in practice for Clever Computing requires further

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) OJ L 119, https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

[2] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) PE/49/2023/REV/1 OJ L, 2023/2854, https://eur-lex.europa.eu/eli/reg/2023/2854/oj/eng.

[3] Consolidated text: Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Radio Equipment Directive), https://eur-lex.europa.eu/eli/dir/2014/53/2024-12-28.

[4] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No. 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act) PE/100/2023/REV/1 OJ L, 2024/2847, https://eur-lex.europa.eu/eli/reg/2024/2847/oj.

[5] Product Security and Telecommunications Infrastructure Act 2022, Chapter 46, www.legislation.gov.uk/ukpga/2022/46/introduction.

[6] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) No. 168/2013, (EU) 2018/858, (EU) 2018/1139, and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797, and (EU) 2020/1828 (Artificial Intelligence Act) PE/24/2024/REV/1 OJ L, 2024/1689, https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

[7] Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC (Machinery Regulation) PE/6/2023/REV/1, OJ L 165, https://eur-lex.europa.eu/eli/reg/2023/1230/oj.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

unpacking. I will show that Accountable Design is the much-needed response that bridges the gap between legal and technology design research and practitioner communities. To do this, I translate how law implicates design whilst charting how to build legally accountable Clever Computing systems by drawing on approaches and working practices from human-centred computing.

The book presents the socio-technical, design, organisational, and legal aspects of doing Accountable Design across different contexts of Clever Computing use through *three detailed case studies*. These show the need for an inherently interdisciplinary approach aligning conceptual, legal, design, and empirical analysis to ground and develop the concept. Through this analysis, I consider the necessity of reorientating technology design processes to integrate legal values to create more socially, ethically, and legally responsible Clever Computing systems. Ultimately, the book provides critical reflection on what it means to regulate *through* design whilst providing pathways to practical action for those designing systems on how to do it in a human-centred manner.

Each chapter has a detailed overview of its structure, outline, and conclusions, so I will only provide a brief roadmap here (summarised in Figure 1.1). The rest of this chapter develops the motivations behind the new term Clever Computing and outlines the history of similar technologies, showing that the increased integration of AI into IoT (and associated socio-technical and regulatory issues) is a long-standing trend. Chapter 2 examines the rationale behind the new concept of Accountable Design and provides an interdisciplinary analysis of the meanings of accountable, design, and the conceptual implications of regulating through technology design. Three case studies in Chapters 3–5 follow, which examine contexts of AI-enabled IoT use and apply the Accountable Design approach. Chapter 3 focuses on designing for privacy in Clever Urban Computing systems deployed in urban and city contexts. Chapter 4 examines how to design for security in Clever Domestic Computing in homes, whilst Chapter 5 explores design for trust and safety for Clever Biometric

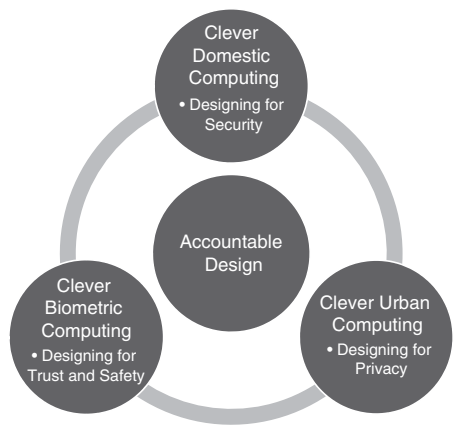


FIGURE 1.1 Book overview.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

Computing, particularly emotion and facial recognition technologies being deployed in public spaces and workplaces. Chapter 6 establishes a set of eleven principles and a six-step process for doing Accountable Design, coupled with a range of design tools to operationalise the approach. Through the development of decks of ideation cards, board games, speculative fictions, and technology impact assessments, I provide methodological reflections on how to fold law into technology design practices. Critically, through using and evaluating these tools, I offer insights about how to support researchers and practitioners who should be doing Accountable Design.

In the remainder of this chapter, Section 1.2 explores the emergence of the IoT through the earlier 'ubiquitous computing' (Ubicomp) research agenda. This analysis helps situate the risks associated with engineering technologically driven visions of the future. These often neglect current social and human needs in favour of techno-led solutions, highlighting the need for systems design to better account for user needs and, by extension, legal values. I then define the IoT through key aspects such as reliance on physical sensors, pervasive data gathering, and ongoing connectivity with an ecosystem of actors. In Section 1.3, I present the reasoning behind Clever Computing. It captures the convergence of physical sensing through the IoT with data-driven AI in six ways: changing and improving interaction techniques with the IoT; making sense of IoT data and enabling distributed data analysis techniques; and augmenting existing functionality and increasing autonomy of IoT systems. Section 1.4 then provides a chapter summary.

1.2 FROM UBICOMP TO THE IOT

1.2.1 *Demonstrating the Need for Accountable Design: The Case of IoT Toys*

Toys *should* be items that children can always trust. However, the integration of data-gathering sensors into IoT teddy bears, dinosaurs, and walkie-talkies puts their young owners at unnecessary risk due to privacy and security being poorly accounted for in their design (Figure 1.2).[8] This is a long-standing issue, where a well-known example from 2017 was 'My Friend Cayla' – a doll with an onboard Bluetooth speaker and microphone. Security professionals found that it could easily be compromised, allowing hackers to remotely control the doll and speak to children.[9] In response, regulators around the world stepped in. Cayla was banned from sale in Germany,

[8] Gordon Chu, Noah Apthorpe, and Nick Feamster, 'Security and Privacy Analyses of Internet of Things Children's Toys' *IEEE Internet of Things Journal* (2018) 6(1) 978–985 DOI: 10.1109/JIOT.2018.2866423; Andrew Laughlin, 'Kids' karaoke machines and smart toys from Mattel and Vtech among those found to have security flaws' (*Which?*, 2 December 2019), www.which.co.uk/news/article/kids-karaoke-machines-and-smart-toys-from-mattel-and-vtech-among-those-found-to-have-security-flaws-in-a-which-investigation-aCZvy9z0N7R2.

[9] I can attest to this, having seen a live demo of this at a conference in 2023.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

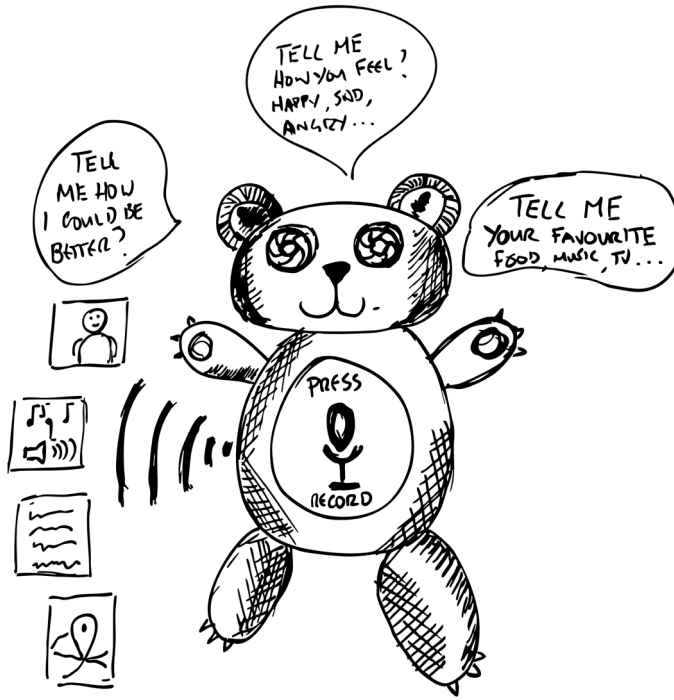


FIGURE 1.2 AI companion bear toy.

where the government even advised parents to destroy any Caylas in their homes.[10] A Norwegian Consumer Council investigation found Cayla and another IoT toy robot from the same manufacturer, i-Que, contravened consumer and data protection rules.[11] For example, contract terms for the devices could be changed without notice, data could be shared with third parties for targeted advertising, and commercial brands could be mentioned in conversations with children (posing manipulation risks). Whilst Cayla and i-Que are no longer on sale, they were not unusual in their risky design and associated business models. Other household toy names like the rebooted version of the 1990s classic toys, the Furby Connect and the Hello Barbie doll, faced similar security issues. The latter was hacked too, giving access to speakers, microphones, and account information from children. Barbie could select from 8,000 lines of dialogue during conversations to personalise its relationship with child users, a trend Val Steeves terms the 'dark side of customer relationship

[10] Philip Oltermann, 'German Parents Told to Destroy Doll That Can Spy on Children' (*The Guardian*, 17 February 2017), www.theguardian.com/world/2017/feb/17/german-parents-told-to-destroy-my-friend-cayla-doll-spy-on-children.

[11] Forbrukerrådet, *#Toyfail: An Analysis of Consumer and Privacy Issues in Three Internet-Connected Toys* (Forbrukerrådet: 2016, Oslo), www.forbrukerradet.no/siste-nytt/connected-toys-violate-consumer-laws.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

management', enabling deceptive and unfair marketing to children as a particularly vulnerable user group.[12]

AI is increasingly embedded in IoT toys too, posing new risks for children's data and wellbeing.[13] The market is awash with products using emotion recognition technology (ERT) in their interactions with children to infer their 'feelings' and respond appropriately.[14] For example, Casio's Moflin is a furry guinea pig esque companion pet robot that emotionally reassures, calms, and 'grows with you'.[15] Many toy firms, large and small, have started using generative AI. Start-up Curio created a soft plushie that integrates OpenAI's ChatGPT, providing children with a friendly face when conversing with the chatbot, and major toy manufacturer Mattel has partnered with OpenAI.[16] Embodied Inc.'s AI-powered Moxie robot fuses both AI approaches, positioning itself as a holistic 'learning robot with heart' that targets emotional and educational development of children using generative AI (again with ChatGPT), alongside face- and voice-based ERT.[17] The toy market mirrors wider shifts in educational technologies using AI to track the learning engagement of children,[18] which is prompting increased government concern in the UK.[19]

There are many legal issues around ERT (explored in depth in Chapter 5), but the use of generative AI in toys raises significant privacy issues.[20] The Italian government temporarily banned ChatGPT in 2023, citing concerns about the processing

[12] Valerie Steeves, 'A Dialogic Analysis of Hello Barbie's Conversations with Children' *Big Data and Society* (2020) 7(1) DOI: 10.1177/205395172091915.

[13] Ayca Atabey, Cara Wilson, Lachlan Urquhart, and Burkhard Schafer, 'Fairness by Design: Cross-Cultural Perspectives from Children on AI and Fair Data Processing in their Education Futures' *CHI '25: Proceedings of the 2025 CHI Conference on Human Factors in Computing Systems, Yokohama, Japan* (ACM Press: New York, 2025) DOI: 10.1145/3706598.3714402; Eric Berger, 'After a Teddy Bear Talked about Kink, AI Watchdogs Are Warning Parents against Smart Toys' (*The Guardian*, 28 Nov 2025) www.theguardian.com/technology/2025/nov/28/artificial-intelligence-smart-toys.

[14] Andrew McStay and Gilad Rosner, 'Emotional Artificial Intelligence in Children's Toys and Devices: Ethics, Governance and Practical Remedies' *Big Data and Society* (2021) 8(1) DOI: 10.1177/2053951721994877.

[15] Casio Moflin Website: www.casio.com/uk/moflin/.

[16] Andrew McStay, 'Mattel and OpenAI Have Partnered Up – Here's Why Parents Should Be Concerned about AI in Toys' (*The Conversation*, 25 June 2025), https://theconversation.com/mattel-and-openai-have-partnered-up-heres-why-parents-should-be-concerned-about-ai-in-toys-259500.

[17] Moxie Robot Website, https://moxierobot.com.

[18] Deborah Lupton and Ben Williamson, 'The Datafied Child: The Dataveillance of Children and Implications for Their Rights' *New Media and Society* (2017) 19(5) 780–794 DOI: 10.1177/1461444816686632.

[19] UK Parliament Education Committee Inquiry 'The Use of Artificial Intelligence and EdTech in Education' (UK Parliament, 26 February 2026) https://committees.parliament.uk/work/9642/the-use-of-artificial-intelligence-and-edtech-in-education/.

[20] Recital 14 of the amended EU Toy Safety Regulation 2025 does not establish new obligations security, privacy or other hazards from use of AI in toys, instead reiterating the need for compliance with other instruments analysed in this book, namely AIA, GDPR, RED and the CRA. Regulation (EU) 2025/2509 of the European Parliament and of the Council of 26 November 2025 on the safety of toys and repealing Directive 2009/48/EC https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L_202502509.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

of children's data.[21] The European Data Protection Board (EDPB) ChatGPT Taskforce foregrounds the technology's impact on the GDPR fairness principle in Article 5(1)(a), which requires data not to be processed in a manner that is detrimental to the subject. The EDPB state that, as a public-facing platform, data subjects are offering personal data to ChatGPT, and OpenAI, as the data controller, should not shift responsibility to data subjects for screening their own chat inputs. They are using chat data to further train their model, so they remain responsible for GDPR compliance.[22] However, in practice, toy companies are shifting responsibility *precisely* in this way. The Mozilla Foundation's consumer protection initiative '*Privacy not Included', which reviews privacy risks around new consumer products, examined the Moxie AI robot. They found that the privacy policy instructs parents to tell children not to share private information with the toy.[23] In late 2024, Moxie closed down, switching off their cloud reliant robots. Parents were left with an expensive piece of e-Waste and a difficult conversation with their child about where their artificial emotional support companion had gone.

Design of next-generation AI-enabled toys needs significantly stricter regulation, given the target audience of children, alongside critical reflection on to what extent designing fair and safe child-AI interactions is even possible. Remedial steps can and have been taken, including enforcement actions, regulator investigations, bans, and litigation against manufacturers.[24] Pre-emptive action to mitigate harm in the first place is needed. A *turn to design* can be a way of embedding measures that respond to legal responsibilities within the fabric of the technology itself. In the UK, the Information Commissioner's Office (ICO) has already sought to improve the design of digital services for children more broadly. Their *Age-Appropriate Design Code of Conduct* mandates design steps that build from the UN Convention on the Rights of the Child,[25] including acting in the best interests of the child or conducting a data protection impact assessment (DPIA) to address risks for children at different ages

[21] Shiona McCallum, 'Chat GPT Banned in Italy over Privacy Concerns' (*BBC News*, 1 April 2023), www.bbc.co.uk/news/technology-65139406.

[22] European Data Protection Board, *Report of the Work Undertaken by the ChatGPT Taskforce* (EDPB: Brussels, 2024), www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf. See Clause 24.

[23] Mozilla *Privacy Not Included Website. www.mozillafoundation.org/en/privacynotincluded/.

[24] Federal Trade Commission, 'Electronic Toy Maker Vtech Settles FTC Allegations That It Violated Children's Privacy Law and the FTC Act' (*FTC.gov*, 8 January 2018), www.ftc.gov/news-events/news/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated-childrens-privacy-law-ftc-act; Relatedly, Ofcom opened an inquiry into coverage of the UK Online Safety Act 2023 for 'AI character companion chatbot services' (triggered by Grok / X chatbot creating harmful, sexualised deepfakes of real individuals). Ofcom 'Investigation into X, and scope of the Online Safety Act' (*Ofcom*, 3 February 2026) www.ofcom.org.uk/online-safety/illegal-and-harmful-content/investigation-into-x-and-scope-of-the-online-safety-act.

[25] Information Commissioner's Office, *Age Appropriate Design: A Code of Practice for Online Services* (ICO: Wilmslow, 2020), https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/code-standards/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

and developmental stages. The Code suggests design responses to create more age-appropriate systems, including minimising the data collected in the first place, using high privacy-protecting defaults, and being transparent about what data is used (and presenting this information in accessible formats). Alongside design, it is crucial to change business models to avoid harmful commercial practices like sharing children's data or profiling and nudging them to change their settings to be less restrictive. A combination of strict regulatory and design-led efforts is necessary to shift current practices, which are worryingly showing no sign of slowing. A 2025 US Public Interest Group showed developers continued integration of AI chatbots into many toys on the market, despite parent AI companies having policies against it on age grounds.[26]

AI-enabled IoT toys are just one example of Clever Computing within this book that highlights the growing need to properly account for legal rights and responsibilities in design processes. I will now look backwards at the historical trajectory of Clever Computing to examine the emergence of embedded, data-driven, connected, and now AI-driven IoT systems in everyday life.

1.2.2 *Learning from the History of Ubicomp*

Early innovations in the networking of physical devices did not start with a grand vision of building a connected future. Instead, it was driven by computer science researchers' need for caffeine. The first IoT device in 1982 was a vending machine at Carnegie Mellon University in the US. It was networked by David Nicols and fellow graduate students to the Advanced Research Projects Agency Network (ARPANET – i.e. the early Internet) to check on real-time stocks of Coca-Cola. This helped the students decide if it was worth taking a stroll downstairs to retrieve a cold can or not.[27] Similarly, in 1991, the Trojan Room Coffee Machine at Cambridge University's Computer Lab in the UK set up the world's first webcam. Instead of being used for making endless conference calls, as they are today, it took periodic photos of the coffee machine. These were then uploaded to a server which allowed creator Quentin Stafford-Fraser and his colleagues in the Systems Research Group to remotely check if there was still coffee left in the pot.[28]

Around the same time, Mark Weiser proposed an ambitious future vision of 'post-desktop computing'.[29] Pioneered at Xerox PARC in the US in the early 1990s, Ubiquitous Computing (Ubicomp) was the label for a programme of work to

[26] Including Claude, Grok, Llama and Gemini. See R.J. Cross and Rory Erlich, *Kids Aren't Allowed to Use A.I. Chatbots—But Developers Are Still Putting Them in Toys* (PIRG: Mountain View, 2026) https://publicinterestnetwork.org/wp-content/uploads/2026/03/PIRG-NOT-FOR-KIDS-FOUND-IN-TOYS-March-2026.pdf.

[27] Jordan Teicher, 'The Little-Known Story of the First IoT Device' (*IBM Blog*, 7 February 2018), www.ibm.com/blog/little-known-story-first-iot-device.

[28] Quentin Stafford-Fraser, 'The Life and Times of the First Web Cam: When Convenience Was the Mother of Invention' *Communications of the ACM* (2001) 44(7) 25–26, www.cl.cam.ac.uk/coffee/qsf/cacm200107.html.

[29] Mark Weiser, 'The Computer for the 21st Century' *Scientific American* (1991) 265(3) 94–105.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

develop computers that 'weave themselves into the fabric of everyday life until they are indistinguishable from it'.[30] It aimed to make embedded computing 'invisible in use' in the workplace and at home. Ubicomp would shift how users interacted with computers by going beyond conventional desktop-based peripherals such as a mouse and keyboard and instead move towards interactive 'tabs, pads, and boards'. In contemporary terms, these are wearables, handheld mobile devices, and large interactive displays. Existing preconceptions around how humans interact with computers would be challenged, as interactions would no longer just be a one-to-one relationship with a device.[31] Instead, shared boards could enable interactions with multiple users in a room whilst ambiently sensing and supporting different tasks, for example, working collaboratively in an office or cooking at home in a Ubicomp kitchen. Many of the advances in Ubicomp were supported by concurrent shifts in 'mobile computing'.[32] The 'tabs and pads' of Weiser's vision were coming to life through portable phones and tablets with sophisticated on-device processing, screen-based graphical user interfaces, mobile networking, and global positioning system (GPS) that provided scope for new user interactions 'in the wild', from location-based games to map navigation apps.[33]

Ubicomp was not the only 'post-desktop' vision in town. Similar trends emerged with slightly different labels like Pervasive Computing,[34] Calm Computing,[35] and Ambient Intelligence,[36] latterly followed by Everyware,[37] Cyber-Physical Systems,[38] and Smart Technologies.[39] Some emerged from different starting points, and others tweaked, refined, or extended Ubicomp. For example, calm computing recognised

[30] Weiser, 'Computer for 21st Century' p. 94.

[31] Jonathan Grudin, 'The Computer Reaches Out: The Historical Continuity of Interface Design' *CHI '90: Proceedings of the 1990 SIGCHI Conference on Human Factors in Computing Systems, Seattle, USA* (ACM Press: New York, 1990) 261–268. DOI: 10.1145/97243.97284.

[32] Mark Dunlop and Stephen Brewster. 'Mobile Computing: The Challenge of Mobile Devices for Human Computer Interaction' *Personal and Ubiquitous Computing* (2002) 6(4) 235–236. DOI: 10.1007/s007790200022.

[33] Steve Benford, Andy Crabtree, Martin Flintham, Adam Drozd, Robanastasi, Mark Paxton, Nick Tandavanitj, Matt Adams, and Ju Row-Farr 'Can You See My Now?' *Transactions on Computer Human Interaction* (2006) 13(1) 100–133. DOI: 10.1145/1143518.1143522.

[34] Mahadev Satyanarayanan, 'Pervasive Computing: Vision and Challenges' *IEEE Personal Communications* (2001) 8(4) 10–17. DOI: 10.1109/98.943998.

[35] Mark Weiser and John Seely Brown, 'The Coming Age of Calm Technology', *Beyond Calculation: The Next Fifty Years of Computing* (Springer: New York, 1997). DOI: 10.1007/978-1-4612-0685-9_6. p1-2.

[36] Emile Aarts and Stefano Marzano (eds), *The New Everyday: Views on Ambient Intelligence* (Uitgeverij 010: Rotterdam, 2003).

[37] Adam Greenfield, *Everyware: The Dawning Age of Ubiquitous Computing* (New Riders: Berkeley, 2006).

[38] Christopher Greer, Martin Burns, David Wallman, and Edward Griffor. *Cyber-Physical Systems and Internet of Things* (National Institute of Standards and Technology: Gaithersburg, 2019). DOI: 10.6028/NIST.SP.1900-202.

[39] Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar Publishing: Cheltenham, 2016).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

the value of calmness as a Ubicomp design principle because 'if computers are everywhere they better stay out of the way, and that means designing them so that the people being shared by the computers remain serene and in control'.[40] The constant beeping, buzzing, and notifications of contemporary IoT systems suggest that calmness was not been the guiding principle in our current 'attention capture'-driven economy.

Nevertheless, collaborative academic, industry, and government investment in the 1990s and 2000s underpinned the growth of many research programmes into physical, mobile, and embedded computer systems. This included Philips and Eindhoven University's collaboration on Ambient Intelligence,[41] IBM and Carnegie Mellon's concurrent research into Pervasive Computing,[42] the European Commission's Disappearing Computer programme,[43] Intel's work on Proactive Computing,[44] and numerous university projects like the University of Nottingham Equator Consortium,[45] MIT's Project Oxygen,[46] and Georgia Tech's Aware Home.[47] This led to a long period of research and development tackling difficult technical questions like:[48]

- How to design invisible interfaces that can ambiently collect data from users without constantly asking them for permission or being obvious?
- What is necessary to build a networking infrastructure that can seamlessly follow devices and users moving between different contexts like their home and work, whilst avoiding any drop in quality of service?
- How can ambient sensors that constantly watch and gather data from their environment be sustained, for example, with battery life or environmental resilience?

[40] Mark Weiser and John-Seely Brown, 'The Coming Age of Calm Technology', in Peter Denning and Robert Metcalfe (eds.), *Beyond Calculation* (Copernicus: New York, 1997), p. 78.

[41] Caroline Hummels, Emile Aarts, and Kees Overbeeke. 'The Shared Worlds of Industrial Design TU/e and Philips Research'. *CHI '09: Extended Abstracts on Human Factors in Computing Systems, Boston, USA* (ACM Press: New York, 2009) 2639–2642. DOI: 10.1145/1520340.1520371.

[42] Wendy S. Ark and Ted Selker, 'A Look at Human Interaction with Pervasive Computers' *IBM Systems Journal* (1999) 38(4) 504–507. DOI: 10.1147/sj.384.0504. IBM also worked on 'autonomic computing', see Mireille Hildebrandt and Antoinette Rouvroy, *Law, Human Agency and Autonomic Computing: The Philosophy of Law Meets the Philosophy of Technology* (Taylor & Francis: London, 2011).

[43] Disappearing Computer Website, www.disappearing-computer.eu/resources.html.

[44] David Tennenhouse, 'Proactive Computing' *Communications of the ACM* (2000) 43(5) 43–50. DOI: https://dl.acm.org/doi/pdf/10.1145/332833.332837.

[45] University of Nottingham Equator Project Website, web.archive.org/web/20120702141940/ www.equator.ac.uk/.

[46] MIT Project Oxygen Website, http://oxygen.lcs.mit.edu.

[47] Georgia Tech's Aware Home Research Initiative Website, www.cc.gatech.edu/fce/house/house.html.

[48] Yong Liu, Jorge Goncalves, Denzil Ferreira, Simo Hosio, and Vassilis Kostakos, 'Identity Crisis of Ubicomp? Mapping 15 Years of the Field's Development and Paradigm Change' *Ubicomp '14: Proceedings of the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing, Seattle, USA* (ACM Press: New York, 2014), 75–86. DOI: 10.1145/2632048.2632086.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

Alongside this active technical agenda, Computer Supported Cooperative Work (CSCW) and HCI researchers increasingly foregrounded the need to avoid neglecting the social messiness of the myriad contexts computing would now be used in. Reflecting on this point remains pertinent today, as developments in AI increasingly risk overlooking human interests again. One useful example from the time was designing 'invisible interfaces'. In part, this required examining suitable materials, sensors, or where to place devices in a space. However, Peter Tolmie and others found designing for invisibility was not just a technical challenge. Understanding the social context of human interactions with a system was key, particularly the everyday routines of users' daily lives and what makes these activities routine in the first place.[49] Lucy Suchman's earlier work similarly centred the need to account for social practices of users in technology design, rather than assumptions of designers and categorical logics imposed by machines.[50] The research agendas in CSCW and HCI became central in establishing the importance of human centricity in Ubicomp system design. The fields provide (often qualitative) research methods necessary to develop vital insights around deployment contexts, system requirements, and evaluation with human interests at the forefront. For example, ethnomethodology and ethnographic approaches were invaluable because design ethnography provided understanding of the social order where technologies would be deployed, and this could inform system design.[51] The future-orientated nature of Ubicomp provided another way human needs could be forgotten. Scholars like Stuart Reeves and Paul Dourish and Genevieve Bell warn that user practices and concerns are often displaced or ignored in favour of ever-aspirational technologically driven futures that can never be achieved.[52]

This provides a cautionary tale for contemporary IoT and AI trends in the latter chapters, where user interests are still secondary to technological solutionism.[53]

[49] Peter Tolmie, James Pycock, Tim Diggins, Allan MacLean, and Alain Karsenty, 'Unremarkable Computing' *CHI '02: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, Minneapolis, USA* (ACM Press: New York, 2002), 399–406. DOI: 10.1145/503376.503448. *'Put simply, we need to embed computation within life not just cups'*.

[50] Lucy Suchman, *Plans and Situated Actions: The Problem of Human-Machine Communication* (Cambridge University Press: New York, 1987), and *Human Machine Reconfigurations* (Cambridge University Press: New York, 2007).

[51] Paul Dourish and Graham Button, 'On "Technomethodology": Foundational Relationships between Ethnomethodology and System Design' *Human–Computer Interaction* (1998) 13(4) 395–432. DOI: 10.1207/s15327051hci1304_2; Andy Crabtree, Mark Rouncefield, and Peter Tolmie, *Doing Design Ethnography* (Springer: London, 2012).

[52] Stuart Reeves, 'Envisioning Ubiquitous Computing' *CHI '12: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2012, Austin, USA* (ACM Press: New York, 2012), 1573–1582. DOI: 10.1145/2207676.2208278; Genevieve Bell and Paul Dourish, 'Yesterday's Tomorrows: Notes on Ubiquitous Computing's Dominant Vision' *Personal and Ubiquitous Computing* (2007) 11, 133–143. DOI: 10.1007/s00779-006-0071-xp140.

[53] Dave Randall, 'Living Inside a Smart Home: A Case Study' in Richard Harper (ed.), *Inside the Smart Home* (Springer: London, 2003).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

For example, in smart home research examined in Chapter 4, Charlie Wilson and others found that the goals of efficiency, comfort, or convenience are often favoured over human interests and understanding the processes by which technologies come to have meaning and utility in homes. As they argue, 'Use and meaning of technologies will be socially constructed and iteratively negotiated, rather than being the inevitable outcome of assumed functional benefits'.[54] This echoes earlier work by Sanna Leppënen and Marika Jokinen, who stated 'inhabitants themselves make a home and little everyday practices make the known life go on … a smart home should not be smarter than its inhabitants'.[55] AI deployments similarly often disregard or actively work against human values, interests, users, and non-users who are subject to these systems, particularly with large-scale technology-driven projects. For example, Virginia Eubanks showed that access to *public welfare* based on automated decision-making disproportionally impacts poorer socio-economic groups;[56] Petra Molnar found that *biometric and mobility* AI security systems trialled on vulnerable refugees negatively impacted their human rights;[57] and Danielle Citron and Frank Pasquale observed *automated credit scoring* results in a range of intersectional harms.[58]

Returning to the history of Ubicomp, despite decades of research and funding, scholars contested if it truly emerged in its planned form. Ramon Caceres and Adrian Friday posited it remained aspirational,[59] whilst for Yvonne Rogers its original goals shifted over time.[60] For Dourish and Bell, it did arrive but in a different guise, where Ubicomp emerged through real-world practice of appropriation and domestication of technologies into users' daily lives.[61] As they state, 'the lesson

[54] Charlie Wilson, Tom Hargreaves and Richard Hauxwell-Baldwin, 'Smart Homes and Their Users: A Systematic Analysis and Key Challenges' *Personal and Ubiquitous Computing* (2015), 19. 463. DOI: 10.1007/s00779-014-0813-0. p. 466.

[55] Sanna Leppänen and Marika Jokinen, 'Daily Routines and Means of Communication in a Smart Home' in Richard Harper (ed.), *Inside the Smart Home* (Springer: London, 2003), p. 223.

[56] Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (St Martin's Publishing Group: New York, 2018).

[57] Petra Molnar, 'Territorial and Digital Borders and Migrant Vulnerability under a Pandemic Crisis' in Anna Triandafyllidou (ed.), *Migration and Pandemics: Spaces of Solidarity and Spaces of Exception* (Springer International Publishing: London, 2022).

[58] Danielle Keats Citron and Frank Pasquale, 'The Scored Society: Due Process for Automated Predictions' *Washington Law Review* (2014) 89(1), https://digitalcommons.law.uw.edu/wlr/vol89/iss1/2.

[59] Ramon Caceres and Adrian Friday, 'Ubicomp Systems at 20: Progress, Opportunities, and Challenges' *IEEE Pervasive Computing* (2012) 11(1) 14. DOI: 10.1109/MPRV.2011.85 p. 15.

[60] Yvonne Rogers, 'Moving on from Weiser's Vision of Calm Computing: Engaging Ubicomp Experiences' *Ubicomp '06: Proceedings of the 8th International Conference on Ubiquitous Computing, Orange County, USA* (ACM Press, New York, 2006), 404–421 DOI: 10.1007/11853565_24 p. 406.

[61] Roger Silverstone and Leslie Haddon, 'Design and the Domestication of Information and Communication Technologies: Technical Change and Everyday Life' in Robin Mansell and Roger Silverstone (eds.), *Communication By Design* (Oxford University Press: Oxford, 1996).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

of the real world of ubicomp is that we will always be assembling heterogeneous technologies to achieve individual and collective effects, and they will almost always be messy'.[62] The current levels of adoption of mobile phones, tablets, IoT, and now AI, suggest that they were right.[63] The Ubicomp experience showed that understanding the social is a key part of technology design; a point that needs to be reiterated for current visions of AI-enabled IoT. Issues still arise because systems are still not built in a human-centred way, but this book extends this point further. Accounting for human needs also requires accounting for legal values, protections, rights, and responsibilities in Clever Computing design processes too.

1.2.3 *IoT beyond RFID*

Kevin Ashton coined the term the IoT in 1999 to describe an approach to tracking items within globally fragmented business supply chains using radio-frequency identification (RFID).[64] RFID can include battery-powered RFID tags that actively broadcast their ID to receivers or passive RFID tags that require a human to scan with a reader. RFID is now often combined with short-range near-field communications (NFC) and barcode like QR codes too. Critically, RFID provides unique digital IDs to physical things, making them documentable and traceable, where diverse applications have emerged over the years such as:

- Monitoring the origin and quality of food through tracing packaging, for example, where fish is caught, packaged, transported, and sold (Figure 1.3).[65]
- Tracking high-value items like whisky on supermarket shelves to prevent shoplifting.
- RFID wristbands at theme parks, such as Disneyland's MagicBand+, to track visitors and support payments during their visit.[66]

[62] Paul Dourish and Genevieve Bell, *Divining a Digital Future: Mess and Mythology in Ubiquitous Computing* (MIT Press: Cambridge, 2011) '…by looking outside of the research laboratory, we are looking at ubiquitous computing as it is currently developing rather than it might be imagined to look in the future'. p. 26.

[63] Ofcom *Online Nation Report* (Ofcom: London, 2024), www.ofcom.org.uk/siteassets/resources/documents/research-and-data/online-research/online-nation/2024/online-nation-2024-report.pdf?v=386238.

[64] Kevin Ashton, 'That "Internet of Things" Thing' (*RFID Journal*, 22 *June 2009*), www.itrco.jp/libraries/RFIDjournal-That%20Internet%20of%20Things%20Thing.pdf.

[65] Chris Graham, 'Fish Traceability Technology Examined' *(Gov.uk*, 28 June 2023), https://marinedevelopments.blog.gov.uk/2023/06/28/fish-traceability-technology-examined/; Estefania Abad, Francisco Palacio, Maider Nuin, Alberto Gonzalez De Zarate, A Juarros, Jose Maria Gómez, and Santiago Marco, 'RFID Smart Tag for Traceability and Cold Chain Monitoring of Foods: Demonstration in an Intercontinental Fresh Fish Logistic Chain' *Journal of Food Engineering* (2009) 93(4) 394–399. DOI: 10.1016/j.jfoodeng.2009.02.004.

[66] Disneyland MagicBand Website, www.disneyworld.co.uk/guest-services/disney-bands/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

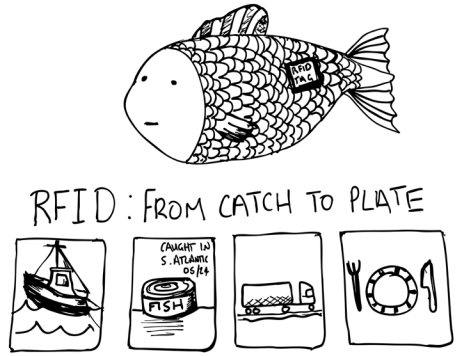


FIGURE 1.3 RFID use case: food supply chain.

- Developing intelligent fitting rooms like Ralph Lauren's New York store, where RFID and a smart mirror would identify clothes and then tailor the lighting/ambience for the customer.[67]
- Tracking the histories and stories of objects for creative and cultural value, such as RFID storing and logging the battle stories of Warhammer 40K figurines.[68]

Despite its practical utility, Jordan Firth cautions that RFID created 'infrastructures of identification' for sorting, tracking, and surveillance of objects.[69] This extends to tracking humans too, through the digital proxy of RFID. For example, whilst contactless bankcards or mobile device apps like Apple Pay now dominate the market, originally Oyster RFID travel cards were the primary means for ticketing on the London Underground (with similar RFID cards for travel systems around the world).[70] This capability allowed both its parent organisation, Transport for London, and the police, to monitor passenger movements, positioning it as a significant data resource in criminal investigations.[71]

[67] It eventually shut down due to cut costs. Anna Hensel, 'After Years of Hype, RFID Is Still Struggling to Catch on in Retail' (*ModernRetail.com*, *14 January* 2020), www.modernretail.co/retailers/after-years-of-hype-rfid-is-still-slowly-catching-on-in-retail/.

[68] Dimitrios Paris Darzentas, Michael Brown, Martin Flintham, and Steve Benford, 'The Data Driven Lives of Wargaming Miniatures', *CHI '15: Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems, Seoul, South Korea* (ACM Press: New York, 2015). DOI: 10.1145/2702123.2702377.

[69] Jordan Frith, *A Billion Little Pieces: RFID and Infrastructures of Identification* (MIT Press: Cambridge, 2019).

[70] Transport for London, 'New Analysis Shows That Pay as You Go with Mobile on the Tube Now More Popular Than before the Pandemic' (*Transport for London*, 28 October 2022), https://tfl.gov.uk/info-for/media/press-releases/2022/october/new-analysis-shows-that-pay-as-you-go-with-mobile-on-the-tube-now-more-popular-than-before-the-pandemic

[71] BBC News, 'Oyster Data Is "New Police Tool"' (*BBC News*, 13 March 2006), http://news.bbc.co.uk/1/hi/england/london/4800490.stm

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

BOX 1.1 Working definition of Internet of Things

The IoT is *networked* physical devices and sensors combining hardware and software to conduct *data gathering and sharing* within an *ecosystem* of human and non-human actors.

The term IoT is no longer constrained to the limited technical capabilities of RFID. Instead, it is now synonymous with the physical sensing and data-gathering 'tabs, pads, and boards' of Weiser's Ubicomp. The IoT exists in domestic settings with smart homes, in public and semi-public spaces with smart buildings and cities, and in workplaces too with industrial IoT and Industry 4.0. Current estimates state that there will be thirty-eight billion IoT devices online by 2030, and the sheer number of consumer products that have become networked is vast, from vacuum cleaners and children's toys to thermostats and wearable devices.[72] Nevertheless, the IoT is a difficult term to define. Given its centrality to Clever Computing, I suggest the following working definition of IoT in Box 1.1.

This consolidates elements of definitions from internet standards bodies, advocacy groups, and government agencies, and builds on my own fieldwork on defining the IoT.[73] The international Internet standards organisation, the Internet Engineering Task Force, defines the IoT as embedded devices with internet connectivity and an ability to communicate on a machine-to-machine basis without direct human control and oversight.[74] The international non-profit group, the Internet Society, focuses on the use of cloud computing for ongoing data gathering/storage, and miniaturisation of physical devices.[75] The former EU Article 29 Working Party (which preceded the EDPB) emphasises data sharing and remote control of devices by manufacturers.[76] In my expert interview study with thirteen lawyers and technologists on

[72] Matthew Iji and Rohit Gurung, 'IoT Connections Forecast to 2030' (*GSMA Intelligence, Dec* 2023), https://data.gsmaintelligence.com/research/research/research-2023/iot-connections-forecast-to-2030.

[73] Lachlan D. Urquhart, 'White Noise from the White Goods? Privacy by Design for Ambient Domestic Computing' in Burkhard Schafer, Edina Harbinja, and Lilian Edwards (eds.), *Future Law* (Edinburgh University Press: Edinburgh, 2020).

[74] Hannes Tschofenig, Jari Arkko, Dave Thaler, and Danny R. McPherson, 'IETF RC 7452: Architectural Considerations in Smart Object Networking' (*Internet Engineering Task Force DataTracker*, March 2015), https://datatracker.ietf.org/doc/rfc7452/. The IETF states that the IoT is a 'Network of physical objects or "things" embedded with electronics, software, sensors, actuators, and connectivity to enable objects to exchange data with the manufacturer, operator, and/or other connected devices'.

[75] Scott Eldridge Karen Rose and Lyman Chapin, *Internet of Things: An Overview* (Internet Society: Geneva, 2015), www.internetsociety.org/resources/doc/2015/iot-overview/.

[76] Article 29 Data Protection Working Party, *Opinion 8/2014 on the Recent Developments in the Internet of Things* (European Union: Brussels, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf. *Section 1.3 – the IoT is* 'Devices that can be controlled remotely over the internet … most home automation devices are constantly connected and may transmit data back to the manufacturer'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

the nature of the IoT and regulatory challenges, I found neither group advanced a canonical vision that strictly demarcates what makes a system IoT or not (unlike with Ubicomp).[77] Instead, participants generally discussed the IoT as encompassing a wide variety of networked sensors and devices, where the smartphone is a key mediating control device. The lawyers' foregrounded the importance of IoT applications domains like wearables. In contrast, the technologists highlighted the technical attributes of the IoT, such as the partiality of user interfaces, need for pervasive networking, and ubiquitous data collection. To develop a richer IoT definition that underpins Clever Computing, I focus on three key features (and associated risks), namely impacts of IoT sensing the physical world, ongoing control through the IoT, and the ecosystem of data gathering and sharing the IoT creates.

1.2.4 *IoT All around Us: Interconnected Devices Sensing the Physical World*

IoT devices are networked through techniques like short-range Bluetooth and IoT-specific networking protocols such as Zigbee or z-Wave. Devices can also be connected across cities and entire regions through Long-Range Wide Area Network (LoRaWAN), as exists in Edinburgh and Scotland's Central Belt.[78] Such interconnectivity means that IoT devices are not sitting in isolation but can instead share data gathered from the physical world through sensors like accelerometers, cameras, motion sensors, and microphones. Many home IoT products, explored in more detail in Chapter 4, capitalise on this ability to share context-sensitive information, for example, with a front door lock being opened, then triggering a home CCTV camera to stop (or start) recording. A lack of interoperability has meant that cross-device communications have often been fragmented, although the landscape is shifting. For example, the Connectivity Standards Alliance Matter open-source standard has support of IoT manufacturers like Amazon, Alexa, Apple, LG, and Samsung. It creates an ecosystem with a common wireless protocol, Thread, that makes it easier for these devices to interact and break down proprietary standards.

Whilst the growth of networked connected devices allows manufacturers and deployers to use IoT devices in novel ways, it also surfaces socially problematic consequences. Apple AirTags highlight the need to account for human-centred, socio-technical, and legal considerations in both design and operation. Apple AirTags are coin-sized Bluetooth devices that users purchase to attach to their keys or luggage

[77] See Section 3.5 for further details of this study.

[78] Long-Range Wide Area Network – low power networking protocol for long-range data sharing. For example, Edinburgh has a LORAWAN network with 'multi-sensor IoT devices at scale across 7,700 km², totalling some 10,000 devices and 100,000 sensing elements, including for the capture of a unique real-time environmental dataset that will be used for schools' education, academic research, public services, and to spawn future innovation and entrepreneurship'. IoT Research and Innovation Service Overview (The University of Edinburgh, 24 November 2023), https://edinburgh-international-data-facility.ed.ac.uk/updates-events/iot-research-and-innovation-service.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

to keep track of them. The AirTags become part of a large peer-to-peer network of Apple phones, tablets, and laptops, which can help pinpoint where an AirTag, and any attached property, is. Whilst this ability to digitally search the physical world has convenience for those who often lose things, AirTags have also been appropriated for significant harm. Stalkers have secretly attached them to their victim's rucksack or clothing. In a Welsh case, a court served an offender a restraining order and prison sentence for attaching an AirTag to their ex-partner's car to follow and harass them.[79] Tragically, in the United States (US), there have been cases where stalkers have used information from AirTags to track and ultimately kill their victims.[80] Current-generation AirTags do take some privacy measures at the architectural level. This includes avoiding storing location data on tags, not sharing the identity of the device that discovered it, encrypting communications data, and providing phone notifications about unidentified AirTags.[81] A class action suit in the US argues that these measures are insufficient; for example, when phones are not on the Apple network, users will not be notified about unknown tags, unless they have a specific third-party app.[82]

Accounting for human values in design, particularly privacy and safety, is central to addressing risks that can arise during use when devices are appropriated beyond the intentions of manufacturers. Finding mechanisms to surface and address risks effectively is necessary. For example, Diana Freed and others research on the relationship between intimate partner violence and technology suggests the need to conduct safety reviews on interface design to reduce, or degrade, usability of devices for abusers and to anticipate potential abuse, much like the process of security penetration testing.[83] I will return to this topic in Chapter 3.

1.2.5 *IoT Bricking: Ongoing Control over Devices and Lack of User Agency*

As with many digital products, the IoT is underpinned by an ongoing service relationship between manufacturers and users. Whilst once manufacturers had

[79] Jason Evans, 'Jealous Man Used Apple AirTag to Track Ex-Partner's Car' (*Wales Online*, 10 August 2022), www.walesonline.co.uk/news/wales-news/stalking-apple-airtag-tracker-partner-24719143.

[80] Amelia Neath, 'Apple AirTag Killer Jailed for Repeatedly Running over Boyfriend' (*The Independent*, 25 September 2023), www.independent.co.uk/news/world/americas/crime/apple-airtag-killer-gaylyn-morris-b2417957.html.

[81] Apple AirTag Website, www.apple.com/uk/airtag/.

[82] Ashley Belanger, 'Apple AirTags Stalking Led to Ruin and Murders, Lawsuit Says' (*Ars Technica*, 12 October 2023), https://arstechnica.com/tech-policy/2023/10/apple-airtags-triggered-explosion-of-stalking-reports-nationwide-lawsuit-says/.

[83] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell, '"A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology', *CHI '18: Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, Montreal, Canada*. DOI: https://dl.acm.org/doi/10.1145/3173574.3174241; Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer, 'Internet of Things': How Abuse Is Getting Smarter' *Safe – The Domestic Abuse Quarterly* (2019) 63 22–26. https://discovery.ucl.ac.uk/id/eprint/10070024/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

limited control after software was developed and delivered[84] the shift towards more iterative, flexible software development methodologies, like agile[85] and now DevOps, provide more ongoing control.[86] Here, manufacturers can tweak user interfaces, adjust what data is harvested into their cloud servers, push over-the-air software updates, or remotely disable or enable functionality of onboard hardware.[87] As the development and operation of the IoT are more closely coupled, greater feedback on use is possible, allowing manufacturers continued abilities to oversee their software and data processing across the whole lifecycle of an IoT system.

Importantly, users often have limited agency to shape or change manufacturer decisions, which can lead to backlash. The Revolv IoT hub, which controlled different smart home devices, was remotely bricked after Nest acquired the company. Like the Moxie robot, the hub was rendered obsolete when support was removed, consigning an otherwise fully functioning device to e-waste.[88] In 2022, BMW offered customers a subscription to unlock and use their heated seats (which are already installed), a move they later dropped in 2023 due to criticism.[89] Whilst 'planned obsolescence' is a business decision to limit support periods or design lifespan for components, intellectual property laws also provide a route to IoT device redundancy through enforcing ongoing control. Technical protection measures and digital rights management have underpinned the denial of users 'right to repair' to fix, upgrade, or change their technologies, famously in the US with John Deere tractors.[90] An extreme example from 2023 shows how much power is retained where Polish train manufacturer Newag was alleged to have been using software that prevented repair of trains by unofficial repair shops. This meant entire trains were being 'bricked' and left out of service. In response, an ethical hacker collective, Dragon

[84] Winston W. Royce, 'Managing the Development of Large Software Systems' *Proceedings of IEEE Western Electronic Show and Convention (WESCON), Los Angeles, USA* (1970) 1–9. www-scf.usc.edu/~csci201/lectures/Lecture11/royce1970.pdf.

[85] Kent Beck, Mike Beedle, Arie van Bennekum, Alistair Cockburn, Ward Cunningham, Martin Fowler, Robert C. Martin, Steve Mellor, Dave Thomas, James Grenning, Jim Highsmith, Andrew Hunt, Ron Jeffries, Jon Kern, Brian Marick, Ken Schwaber, Jeff Sutherland, Manifesto for Agile Software Development Website, http://agilemanifesto.org/history.html.

[86] Nasreen Azad and Sami Hyrynsalmi, 'DevOps Critical Success Factors: A Systematic Literature Review' *Information and Software Technology* (2023) 157 107–150. DOI: 10.1016/j.infsof.2023.107150.

[87] Seda Gurses and Joris van Hoboken, 'Privacy after the Agile Turn' in Evan Selinger, Jules Polonetsky and Omere Tene (eds.), *Cambridge Handbook of Consumer Privacy* (Cambridge University Press: New York, 2018).

[88] Kieren McCarthy, 'Nest's Bricking of Revolv Serves as Wake-up Call to Industry' (*The Register*, 6 September 2016), www.theregister.com/2016/04/06/nests_bricking_of_revolv_a_wakeup_call.

[89] Alistair Charlton, 'BMW Drops Controversial Heated Seats Subscription, To Refocus On Software Services' (*Forbes*, 7 September 2023), www.forbes.com/sites/alistaircharlton/2023/09/07/bmw-drops-controversial-heated-seats-subscription-to-refocus-on-software-services/.

[90] Christopher Boniface, Lachlan Urquhart and Melissa Terras, 'Towards a Right to Repair for the Internet of Things: A Review of Legal and Policy Aspects' *Computer Law and Security Review* (2024) 52. DOI: 10.1016/j.clsr.2024.105934.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

Sector, was hired by the independent repair shop to diagnose and fix the problem. Code on the train stopped it starting if a GPS tracker was detected in an unofficial repair location or unofficial components that lacked authentication codes were used. Manufacturer Newag threatened to sue the hacker collective and claimed their actions made the trains unsafe.[91]

1.2.6 *IoT as Invisible Witnesses: Impacts of an Ecosystem of Data Gathering and Sharing*

IoT devices set up data processing infrastructures that an ecosystem of actors may want access to, including manufacturers, deployers, and third parties like insurers and law enforcement. The visibility of data IoT facilitates poses socio-technical and legal concerns, particularly around appropriate data protection and design controls to manage who can access and share the IoT data in the first place (an area considered at length in Chapter 4).[92] For now, the Ring connected and camera enabled doorbell and iRobot Roomba robotic vacuum cleaner provide examples of types of data gathered by IoT devices and how daily life can be made visible beyond the home.

An investigation by the US Federal Trade Commission in 2023 found that Ring had failings in controlling access to videos from their domestic camera devices. Externally, insufficient privacy and security measures allowed hackers to access the videos and accounts of 55,000 customers. It was not just informational breaches where hackers tormented vulnerable customers too. Internally, their own employees and contractors were also found to be accessing footage to train AI models without user consent and watching female users in their bedrooms and bathrooms.[93]

The Roomba uses an 'Imprint Smart Mapping'[94] system to generate detailed maps of a user's house to help the device navigate different rooms and obstacles

[91] Ashley Belanger, 'Trains Were Designed to Break Down after Third-Party Repairs, Hackers Find' (*ARS Technica*, 13 December 2023), https://arstechnica.com/tech-policy/2023/12/manufacturer-deliberately-bricked-trains-repaired-by-competitors-hackers-find/.

[92] Michael Friedewald, Elena Vildjiounaite, Yves Punie, and David Wright, 'The Brave New World of Ambient Intelligence: An Analysis of Scenarios Regarding Privacy, Identity and Security Issues' in John A. Clark and others (eds.), *Security in Pervasive Computing* (Springer: New York, 2006); Rolf H. Weber, 'Internet of Things – New Security and Privacy Challenges' *Computer Law & Security Review* (2010) 26(1) 23–30. DOI: 10.1016/j.clsr.2009.11.008; Kayleen Manwaring and Roger Clarke, 'Surfing the Third Wave of Computing: A Framework for Research into eObjects' *Computer Law & Security Review* (2015) 31(5) 586–603. DOI: 10.1016/j.clsr.2015.07.001.

[93] FTC, 'FTC Says Ring Employees Illegally Surveilled Customers, Failed to Stop Hackers from Taking Control of Users' Cameras' (*FTC News*, 31 May 2023). www.ftc.gov/news-events/news/press-releases/2023/05/ftc-says-ring-employees-illegally-surveilled-customers-failed-stop-hackers-taking-control-users.

[94] iRobot Privacy Policy (last updated 2024) Website, https://web.archive.org/web/20240523024559/https://webapi.irobot.com/legal/documents/Europe/United-Kingdom/Legal-Documents/Privacy-Policy.aspx?sc_lang=en-GB. Lawful basis for collection is either fulfilling a contract or legitimate

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

like furniture.[95] According to iRobot's UK Privacy Policy, the resulting 'floorplans, object detection, Wi-Fi heat maps, and images' are stored in the cloud to be shared with others.[96] This data is valuable, and it was central to a deal where Amazon tried to buy iRobot Roomba for £1.1 billion in 2022,[97] a purchase that later fell through in 2024 in part due to competition concerns.[98] Showing the breadth of third-party access possible, the policy clarifies that data collected can be shared with subsidiaries of iRobot, service providers involved with payment and data analytics, any purchasers in a merger, and even law enforcement for detecting, preventing, or addressing crimes like stalking and fraud.[99]

In a paper with Diana Miranda and Lena Podoletz, I examined how IoT devices in the home are becoming 'invisible witnesses' for everyday life, and they are increasingly being used in policing, posing risks to privacy from long term, domesticated forms of surveillance.[100] The Roomba would become yet another device with testimony to provide that can corroborate or challenge narratives around crimes that occur in the home. This is not hypothetical and has occurred in numerous cases in the US and UK, where data from smart watches,[101] doorbells,[102] pacemakers, or Apple health data[103] has been instrumental in murder investigations. In one case in the US state of Arkansas, the murder of Victor Collins involved a combination of IoT evidence, including unexpectedly high-water usage logged by the smart meter in the middle of the night (to wash away blood from a crime scene), voice data from an Amazon speaker, and motion data from the alarm system.[104]

interests, where the purposes of collection include diagnosing and fixing issues, enhancing the user experience, and creating new features.

[95] Users can also customise their floor plan by naming and labelling rooms, giving further insights; the sale was in part due to market competition concerns.

[96] Annex II iRobot Privacy Policy; iRobot also clarify data, including maps, are encrypted at rest in their cloud hosted in Amazon Web Services and during communications using 256-bit AES. Security strategies address across apps, devices, and their cloud, with data leak prevention software on devices, sensitive data stored in the cloud instead of on devices, and with tools to prevent reverse engineering built into apps.

[97] Khari Johnson, 'The iRobot Deal Would Give Amazon Maps Inside Millions of Homes' (*Wired*, 5 August 2022), www.wired.com/story/amazon-irobot-roomba-acquisition-data-privacy/.

[98] Dan Milmo, 'Amazon Drops $1.4bn Deal to Buy iRobot after EU Veto Reports' (*The Guardian*, 29 January 2024), www.theguardian.com/technology/2024/jan/29/amazon-deal-irobot-eu-veto-roomba.

[99] Framed in terms of delivering a service and developing new products/features.

[100] Lachlan Urquhart, Diana Miranda, and Lena Podoletz, 'Policing the Smart Home: The Internet of Things as Invisible Witnesses' *Information Polity* (2022) 27(2) 233–246. DOI: 10.3233/IP-211541.

[101] BBC, 'Greece Killing: Husband Confesses to Caroline Crouch Murder' (*BBC News*, 18 June 2021), www.bbc.co.uk/news/world-europe-57570042.

[102] Elna Schutz, 'Video Doorbells: Police Champion Them but Do They Cut Crime?' (*BBC News*, 14 August 2023), www.bbc.co.uk/news/business-66360030.

[103] Rory Carroll, 'Inspector Gadget: How Smart Devices Are Outsmarting Criminals' (*The Guardian*, 23 June 2017), www.theguardian.com/technology/2017/jun/23/smart-devices-solve-crime-murder-internet-of-things.

[104] Alfred Ng, 'Police Request Echo Recordings for Homicide Investigation' (*CNET*, 27 December 2016), www.cnet.com/news/police-request-echo-recordings-for-homicide-investigation/.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

Newer Roombas also include onboard cameras to support *computer vision* for object detection. This shift to using AI within IoT systems further broadens the ecosystem of actors who can surveil how users live and their intimate routines. In 2020, footage of Roomba test users sitting on the toilet famously surfaced on social media.[105] This raised questions about the data pipeline, where it transpired that workers hired by an AI gig economy platform to label the training data for AI classification had allegedly uploaded the shots online. This highlights how far data can travel beyond the physical context in which it was initially collected and also the exploitative prevalence of hiring poorly paid gig economy workers, often in the Majority World, to annotate data e.g. on platforms like Amazon's Mechanical Turk.[106] I now examine more systematically how AI is increasingly being integrated into IoT systems, under the new term Clever Computing.

1.3 WHAT IS CLEVER COMPUTING?

My working definition of Clever Computing, provided in Box 1.2, foregrounds the closer coupling of AI and the IoT, where the materiality of IoT devices is being integrated with data-driven AI ecosystems, surfacing connected and emergent regulatory and design challenges. I present six ways AI is used with the IoT to (1) facilitate *new modes of user interaction*, (2) *improve* current user interactions, (3) support *distributed* data analysis, (4) *make sense of and interpret* data, (5) *extend* existing system functionality, and (6) enable *greater autonomy*. However, these are not exhaustive, and many examples throughout the book further show the increased use of AI in the IoT. But before examining these, I need to reflect on the nature of AI, specifically machine learning (ML), in Clever Computing.

Like the IoT, AI is not easy to ringfence, particularly given extensive ongoing hype around the term.[107] Leading AI experts Stewart J. Russell and Peter Norvig state that AI is 'the study of [intelligent] agents that receive precepts from the environment and take action'.[108] AI has a long history, first emerging in 1956 at a workshop at Dartmouth University, USA, with researchers working on previously

[105] Ellen Guo, 'A Roomba Recorded a Woman on the Toilet. How Did Screenshots End Up on Facebook?' (*MIT Technology Review*, 19 December 2022), www.technologyreview.com/2022/12/19/1065306/roomba-irobot-robot-vacuums-artificial-intelligence-training-data-privacy/.

[106] Clement Le Ludec, Maxime Cornet, and Antonio Casilli, 'The Problem with Annotation. Human Labour and Outsourcing between France and Madagascar' *Big Data & Society* (2023) 10(2). DOI: 10.1177/20539517231188723; James Muldoon, Callum Cant, Boxi Wu, and Mark Graham, 'A Typology of Artificial Intelligence Data Work' *Big Data & Society* (2024) 11(1). DOI: 10.1177/20539517241232632; David Martin, Jacki O'Neill, Neha Gupta, and Benjamin V. Hanrahan, 'Turking in a Global Labour Market' *Computer Supported Cooperative Work* (2016) 25(1) 39–77. DOI: 10.1007/s10606-015-9241-6.

[107] Lucy Suchman, 'The uncontroversial "thingness" of AI' *Big Data & Society* (2023) 10(2).

[108] Stewart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach, 4th US Ed.* (Prentice Hall / Pearson: London, 2022).

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

BOX 1.2 Clever computing definition

Clever Computing is the convergence of interactive *physical* computing systems which digitally sense, observe, and actuate in the analogue world (IoT), with the *inferential* and *data-driven* infrastructures of AI.

unaligned topics like neural nets, information theory, and cybernetics.[109] AI is often framed as creating systems that can complete tasks traditionally requiring human intelligence. This draws on foundational topics including logical reasoning, knowledge representation of the world through design of taxonomies, ontologies, and supporting machine perception of surroundings. As such, AI design encompasses many disciplines including psychology, philosophy, engineering, and mathematics. However, the socio-technical nature of living with and interacting with AI puts humanities, social sciences, and legal perspectives at the forefront of AI development too.[110]

For Clever Computing, ML is a key AI technology underpinning voice and natural language processing, computer vision, recommender systems, and generative adversarial systems. Samuel originally defined machine learning as 'a field of study that gives computers the ability to learn without being explicitly programmed'.[111] With Clever Computing, ML often involves task-focused work, such as sorting, classifying, filtering, or making inferences and decisions about data. Simply stated, a computational model is trained using input data, either through supervised, unsupervised, reinforcement, or combined learning approaches. A supervised learning model is provided with labelled training data (e.g. image A is a cat, image B is a dog) to explicitly help the model to differentiate inputs (Figure 1.4). An unsupervised learning approach uses algorithms that spot emergent patterns and relationships in unlabelled data. The model refines its assessment over time as it is fed more data by identifying variables and relationships between them; for example, a cluster of pixels in the bottom corner of an image may indicate a feature. Reinforcement learning rewards the model when it takes *correct* actions in the environment it is functioning in. Once trained to differentiate input data or spot patterns, the model can then make sense of new datapoints; for example, when presented with a new image, a trained model could state if it believes the image is

[109] John McCarthy, Marvin L. Minsky, Nathaniel Rochester, and Claude E. Shannon, 'A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence August 31, 1955' *Re-published in AI Magazine* (2006) 27(4) DOI: 10.1609/aimag.v27i4.1904.

[110] For a great overview, see Reuben Binns, 'Artificial Intelligence Primer for Lawyers', in Lilian Edwards, Catalina Goanta and Lachlan Urquhart (eds), *Law, Policy and The Internet* (Hart: Oxford, 2026).

[111] Arthur L Samuel, 'Some Studies in Machine Learning Using the Game of Checkers' *IBM Journal of Research and Development* (1959) 3(3) 210—229. DOI: 10.1147/rd.33.0210.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

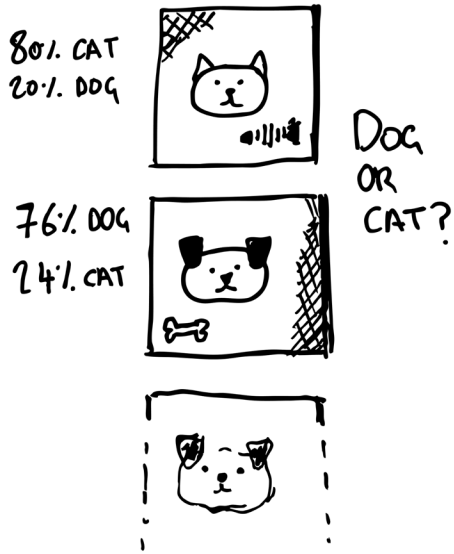


FIGURE 1.4 Example ML classification.

a cat or dog, and with what degree of certainty (e.g. 64 per cent this is a chihuahua dog, not a blueberry muffin).

With unsupervised ML models, the complexity and multiple layers shaping decisions make it difficult to determine how variables have shaped an outcome. When using deep learning and convolutional neural networks, for example, the model is often treated as a 'black box', where inputs and outputs can be accounted for, but algorithmic processes of analysis are more difficult to trace and verify. There have been greater calls to understand how ML functions and gives rise to certain outputs, particularly when interacting with humans. So-called Explainable AI (XAI) aims to provide insights by tracing the factors shaping model decisions; for example, why a prediction about a face is classified as happy, sad, angry, or scared. One XAI technique, Shapley Additive Explanations (SHAP), assigns values and a score to different features in a model to better understand how they feed into a specific prediction.[112] XAI techniques can help developers with auditing, verifying, and validating that the model is functioning as intended, although it is easier with 'good old fashioned' rules-based AI where decision paths are easier to trace.[113] Generative AI uses transformer-based neural networks, trained on large corpuses of multimodal data to create new audio, text, code, and video based on user

[112] Scott M. Lundberg and Su-In Lee, 'A Unified Approach to Interpreting Model Predictions' *Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS'17), Long Beach, California* (2017) 4768–4777.

[113] That is, where the system follows pre-programmed logic and sets of rules more deductively.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

prompts such as requesting creation of short stories, poems, or artworks.[114] Widely used examples include large language models with chat-based user interfaces such as Google Gemini, OpenAI's ChatGPT, Anthropic's Claude, or Microsoft's CoPilot. As discussed in more detail in Chapter 5, generative AI poses *extensive* legal and ethical issues.[115] For example, the provenance of training data is often questionable, where it has been scraped at scale from online sources without due consideration for copyright, bias, or privacy.[116] Before considering the Accountable Design approach in detail in Chapter 2, I will now outline different ways in which AI is being integrated into the IoT and the resulting regulatory concerns.

1.3.1 *AI Is* Providing New Interaction Techniques *with Physical Clever Computing Systems*

The ways users interact with IoT devices and sensors are changing through the integration of AI. As previously noted, the combination of *voice analysis and natural language processing* enables users to speak to devices like speakers, televisions, or in car entertainment. Voice data is gathered from microphones and fed into ML models to answer myriad user search queries, bringing sensing into different contexts of everyday life. Despite convenience, these systems have raised ethical and legal concerns such as gender-based harms of assigning female names like Alexa and default female voices to assistants,[117] racial harms such as not detecting black voices properly,[118] and wider privacy concerns around ensuring adequate control of often opaque data flows for voice data.[119]

It is useful to dig deeper to consider data flows within a real-life system: Amazon Alexa. Like with the Roomba, examining the privacy policy shows the design choices

[114] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Łukasz Kaiser, and Illia Polosukhin. 'Attention Is All You Need.' *Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS'17)*, Long Beach, USA (2017) 6000–6010.

[115] Emily M. Bender, Timnit Gebru, Angelina McMillan-Major, and Shmargaret Shmitchell, 'On the Dangers of Stochastic Parrots: Can Language Models Be Too Big?' *Proceedings of the 2021 ACM Conference on Fairness, Accountability, and Transparency* (FAccT '21) (2021) Virtual/Canada. 610–623. https://doi.org/10.1145/3442188.3445922.

[116] Philipp Hacker, Andreas Engel, and Marco Mauer, 'Regulating ChatGPT and other Large Generative AI Models' *Proceedings of the 2023 ACM FAccT Conference*, Chicago, USA (2023) 1112–1123 doi .org/10.1145/3593013.3594067.

[117] Nóra Ni Loideain and Rachel Adams, 'From Alexa to Siri and the GDPR: The Gendering of Virtual Personal Assistants and the Role of Data Protection Impact Assessments' *Computer Law & Security Review* (2020) 36. DOI: 10.1016/j.clsr.2019.105366.

[118] Allison Koenecke, Andrew Nam, Emily Lake, Joe Nudell, Minnie Quartey, Zion Mengesha, Connor Toups, John R. Rickford, Dan Jurafsky, and Sharad Goel, 'Racial Disparities in Automated Speech Recognition' *Proceedings of the National Academy of Sciences* (2020) 117(14) 7684–7689. DOI: 10.1073/ pnas.1915768117.

[119] Sylvia De Conca, 'Between a Rock and a Hard Place: Owners of Smart Speakers and Joint Control' *SCRIPTed – A Journal of Law, Technology, and Society* (2020) 17(2) 238–268. DOI: 10.2966/ scrip.170220.238.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

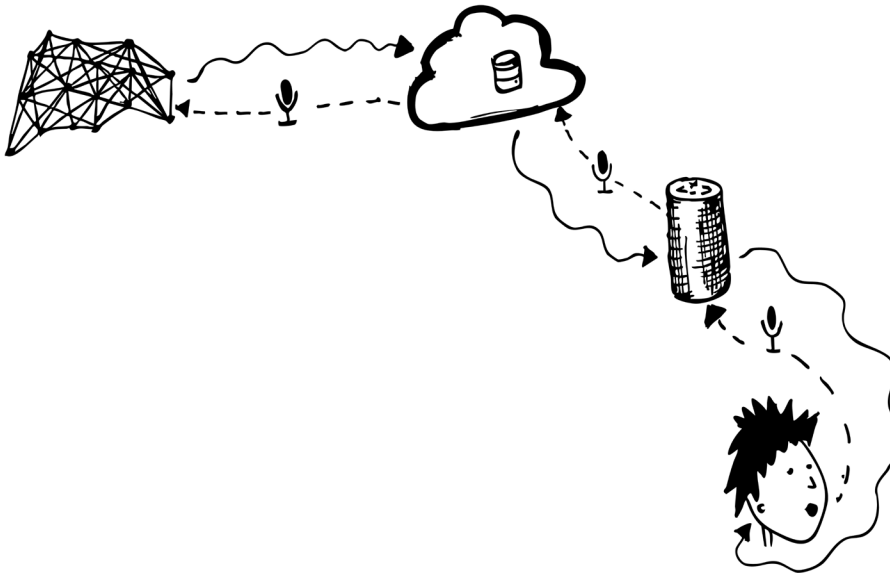


FIGURE 1.5 Voice data flows in a smart speaker system.

taken alongside strategies to manage legal risk.[120] I focus on how the system manages cloud interactions through wake words and how it manages user identification and control over recordings (Figure 1.5).

The policy frames use of wake words as a 'data minimisation' approach, stressing Alexa is *not* always recording. By default, it only records when a wake word is detected for a few seconds before until the system determines the query has finished.[121] Under the EU Data Act 2023,[122] recorded and pre-wake word data should be accessible to users by default, without relying on data subject access rights in Article 15 GDPR. The Amazon policy clarifies that the user is interacting with a cloud-based service, and a recording of their data will be sent to the cloud for analysis by speech recognition tools, using natural language processing. Amazon is explicit that recordings are part of training data for supervised machine learning to improve the product. The user experience design helps demonstrate the temporality of that interaction through the use of colours. There is visual feedback that data will be sent to the cloud as the system light colour turns blue. Similarly, when the microphone

[120] Amazon Alexa, Echo Devices, and Your Privacy 2024 Policy, https://web.archive.org/web/20230316083913/,www.amazon.co.uk/gp/help/customer/display.html?nodeId=GVP69FUJ48X9DK8V. Privacy policies are often being tweaked and updated, as the underlying data processing practices also change.

[121] In addressing 'is Alexa listening to all my conversations', they state – 'No. Echo devices are designed to detect only your chosen wake word (Alexa, Amazon, Computer or Echo). The device detects the wake word by identifying acoustic patterns that match the wake word. No audio is stored or sent to the cloud unless the device detects the wake word (or Alexa is activated by pressing a button)'.

[122] See note 2.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

is switched off, the light will turn red. As discussed later, the affordances of devices to communicate with users can shape their experience but also address legal obligations, such as consenting to data processing. William Seymour and others have explored if GDPR-compliant consent can be achieved through verbal interactions with voice assistants. They found challenges in communicating sufficient information to end users to be compliant, and data controllers may instead rely on another legal ground altogether for processing.[123]

Voice recordings can be managed, reviewed, or deleted as users see fit. Deletion can be done automatically or after three to eighteen months, where associated voice transcripts will also be removed. Users can make a request in real time, right after they talk to the speaker.

Whilst this is what the privacy policy states, real-world practice has been different. With the Alexa Dot smart speaker targeted at children, parents could ask Amazon to delete voice recordings, transcripts, and geolocation data about their children. However, Amazon instead ignored these requests, retained the data, and even used it to refine their algorithms to better work with children, whose voices had unique features for speech recognition. As a result, they were charged in 2023 by the US Federal Trade Commission and Department of Justice and fined $25 million for breaching data protection rules.[124]

1.3.2 *Integration of AI Systems to* 'Improve' User Interactions *with a Clever Computing System*

Since late 2023, both Amazon and Google have been integrating *generative AI* into Alexa and Assistant, to enable more natural, human-like conversations between users and IoT devices. With Alexa+, Amazon acknowledges that they have extensive sensing capabilities in homes through speakers and are now using features of those to improve conversation. Non-verbal cues are being integrated by using cameras, presence detection, and voice analysis. This also includes moving away from using wake words such as saying 'Alexa' to begin the query or using face detection to capture the start of discussions more naturalistically. Amazon are aiming to create more 'empathic' interactions, where Alexa will adapt depending on the conversation topic and how the user is speaking e.g. if they are hesitating/pausing more, Alexa will slow the pace of the responses.[125] With Assistant, Google has been integrating

[123] William Seymour, Mark Cote, and Jose Such, 'Legal Obligation and Ethical Best Practice: Towards Meaningful Verbal Consent for Voice Assistants', *CHI '23: Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems, Hamburg, Germany* (ACM Press: New York 2023). DOI: 10.1145/3544548.3580967.

[124] Children's Online Privacy Protection Act of 1998, 15 U.S.C. 6501–6505 Children's Privacy 1998. www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa.

[125] Daniel Rausch, 'Previewing the Future of Alexa' (*Amazon News*, 20 September 2023). www.aboutamazon.com/news/devices/amazon-alexa-generative-ai. Amazon claims that trust is essential

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

their LLM system, Gemini, to create a more personalised experience, to help manage daily search tasks, generate text or images, and increase integration with other Google services.[126] The promise is creating more contextually aware, personal, helpful user experiences. This augments existing *recommender systems* used for personalisation, an approach familiar to many through music recommendations on Spotify, TV show suggestions on Netflix, or online shopping. Here, a user's past activity can be used to infer their preferences, while reinforcement learning or AI model training aims to help predict their future likes and dislikes. Integration of generative AI compounds existing data protection and security concerns around the IoT. For example, Meta plan to use conversations with their Meta AI Chatbots in targeting advertising.[127] On the security front, security researchers showed in 2025 that Gemini could be hacked to provide control of physical devices in the home, including the lights, boiler, and window shutters. By injecting prompts into Google Calendar invitations, which when summarised by Gemini would run the malicious script, hackers could then have control of the devices, creating real-world safety risks in smart homes.[128]

1.3.3 *AI Enabling* Distributed *Data Analysis*

A shift in AI-enabled IoT has been an ability to utilise *federated machine learning* (Figure 1.6).[129] This aligns with the trend towards putting computational resources and data storage at the *edge* of the network, so-called edge computing.[130] As IoT devices can be more computationally well-resourced, data can now be processed locally, reducing the need to stream all data to the cloud. Instead, an AI model can be distributed across different IoT devices in the network and then fine-tuned on data sourced locally, sharing only limited information with the global model to improve it. Analysis of sensitive data from home devices or wearables can be conducted in situ and closer to the end user.[131] This helps address concerns around overreliance on

to creating a good user experience where 'we will design experiences to protect our customers' privacy and security, and to give them control and transparency'; Amazon Alexa+ website: www.aboutamazon.com/news/devices/new-alexa-generative-artificial-intelligence

[126] Sissie Hsiao, 'Assistant with Bard: A Step toward a More Personal Assistant' (*Google Blog*, 4 October 2023). https://blog.google/products/assistant/google-assistant-bard-generative-ai/.; In 2025, Google started phasing out Assistant, to be replaced wholesale by Gemini on phones and IoT devices.

[127] Maxwell Zeff, 'Meta Plans to Sell Targeted Ads Based on Data in Your AI Chats' (*TechCrunch*, 1 October 2025). https://techcrunch.com/2025/10/01/meta-plans-to-sell-targeted-ads-based-on-data-in-your-ai-chats/.

[128] Matt Burgess, 'Hackers Hijacked Google's Gemini AI with a Poisoned Calendar Invite to Take over a Smart Home' (*Wired*, 6 August 2025). www.wired.com/story/google-gemini-calendar-invite-hijack-smart-home/.

[129] Google AI Online Comic, 'Federated with Google' 2025 Website, https://federated.withgoogle.com/.

[130] Mahadev Satyanarayanan, 'The Emergence of Edge Computing' *Computer* (2017) 50(1) 30–39. DOI: 10.1109/MC.2017.9.

[131] Gartner Hype Cycle 2023 showed both edge computing and federated analytics at 'Peak of Inflated Expectations'. www.gartner.com/en/articles/what-s-new-in-the-2023-gartner-hype-cycle-for-emerging-technologies.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

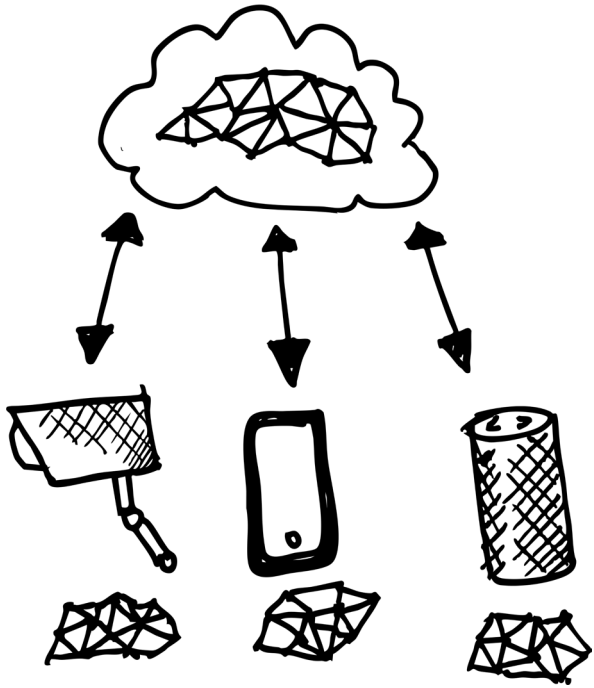


FIGURE 1.6 Federated machine learning.

cloud such as data latency or insufficient bandwidth, but more crucially can enable more privacy-preserving architectures. For example, by keeping data more proximate to users, avoiding third-country international data transfers outside the EU, it avoids many of the regulatory concerns around data being sent to US servers as seen with the Schrems decisions.[132] Edge-based approaches can support increased transparency around data processing and provide greater control for data subjects over their personal data, as discussed further in Chapter 3 with the 'Databox' architecture.[133]

1.3.4 *AI to* Make Sense of and Interpret *Data*

Computer vision is increasingly integrated into camera-based IoT systems. It is used to analyse footage to detect features or patterns in video, often recognising

[132] Laura Drechsler and Irene Kamara, 'Essential Equivalence as a Benchmark for International Data Transfers after Schrems II' in Eleni Kosta, Ronald Leenes, and Irene Kamara (eds.), *Research Handbook on EU Data Protection* (Edward Elgar Publishing Ltd: Cheltenham, 2022); European Data Protection Supervisor, *EDPS Opinion on Personal Information Management Systems: Towards More User Empowerment in Managing and Processing Personal Data* (EDPS: Brussels, 2020). https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf.

[133] Lachlan Urquhart, Neelima Sailaja, and Derek McAuley, 'Realising the Right to Data Portability for the Domestic Internet of Things' *Personal and Ubiquitous Computing* (2018) 22, 317–332. DOI: 10.1007/s00779-017-1069-2.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

objects and faces. Such systems are considered at length in Chapters 3–5, so only mentioned briefly here. Example applications like smart home doorbells or locks, discussed in Chapter 4, use cloud-based analysis to verify and authenticate permitted home visitors and flag unexpected ones.[134] In contrast, facial recognition on mobile devices ordinarily involves more privacy-preserving storage of facial templates in the trusted execution environment on the device itself. Live facial recognition technology (FRT) by law enforcement is examined in Chapter 5. Object detection in airports or train stations is used to spot unattended luggage in real time, considered in Chapter 3.[135] Even animals cannot escape the gaze of Clever Computing. In 2025, Ring cameras added an AI feature to track down lost dogs in the local neighbourhood. If a pet is lost, users can upload a photo to the Ring community app and cameras in the area become part of a distributed 'dog-veillance' system, scanning for the missing pet and alerting the owners if it is spotted.[136] How long until the system is repurposed for evidence gathering for identifying dog fouling? Occasionally, AI also appears to be in use when it is not. Amazon's Fresh stores used a 'Just Walk Out' system, which allegedly used AI to detect what items customers were buying without the need to go to a check-out. It transpired that AI was not used at all and 1,000 staff in India were remotely watching footage and labelling data.[137]

1.3.5 *AI Is Being Layered into Existing Clever Computing Systems to* Extend Existing Functionality

Emotion recognition technology is often layered into the IoT. ERT analyses biometric and physiological data to infer intent or the emotional state of subjects with on-and off-body sensors.[138] ERT is being used in wearables like fitness bands and smart watches but also more interestingly, smart jewellery. For example, the Oura

[134] Nest Aware Help, 'Familiar Face Detection' Website 2025, https://support.google.com/googlenest/answer/9268625?hl=en.

[135] Daniel Neyland and Norma Möllers, 'Algorithmic IF … THEN Rules and the Conditions and Consequences of Power' *Information, Communication & Society* (2017) 20(1) 45–62. DOI: 10.1080/1369118X.2016.1156141. Discussing the ambiguity in classifying and creating parameters for defining objects of interest, which also shaped how objects were treated (e.g. requiring investigation or not from officers).

[136] Lauren Forristal, 'Ring Cameras Can Now Recognize Faces and Help to Find Lost Pets' (*TechCrunch*, 30 September 2025). https://techcrunch.com/2025/09/30/ring-cameras-can-now-recognize-faces-and-help-to-find-lost-pets/.

[137] James Bridle, 'So, Amazon's "AI-Powered" Cashier-Free Shops Use a Lot of … Humans. Here's Why That Shouldn't Surprise You' (*The Guardian*, 10 April 2024). www.theguardian.com/commentisfree/2024/apr/10/amazon-ai-cashier-less-shops-humans-technology.

[138] Rosalind W. Picard, *Affective Computing* (MIT Press: Cambridge, 2000). Computers that can have abilities to 'recognize, understand, even to have and express emotions'; Andrew McStay, *Emotional AI: The Rise of Empathic Media* (SAGE Publications: London, 2018) 'Technologies that use affective computing and artificial intelligence techniques to sense, learn about and interact with human emotional life'.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

Ring uses sensors like infrared photoplethysmography (PPG)[139] to track physiological signals like blood oxygen levels, body temperature, and heart rate, alongside sleep patterns.[140] Similarly, the Leaf Urban is a leaf-shaped piece of jewellery made of wood and silver that tracks similar datapoints.[141] When combined with an app, both systems promise to support well-being, for example, by tracking stress and supporting strategies to increase resilience (by suggesting breaks) and even learning menstrual cycles to make inferences about fertility. Samsung's smart ring, shares similar features and aims to link into wider health data and medical records, coupled with an LLM based AI well-being assistant to provide more personalised support.[142]

Beyond wearables, affective computing is being layered into our two prior examples, with off-body sensing. Voice-based systems are analysing for timbre, pitch, and tone, again to infer an individual's mood. Camera-based ERT analyses faces for the presence of facial action units such as upturned lips or furrowed brows that are cross referenced to basic emotional states to make inferences about how the subject is feeling. The science underpinning this approach is often challenged, for example, computer vision systems Microsoft AI and Face ++ were both found to associate negative emotion more frequently for black faces more than white faces.[143] Yet the (flawed) approach of trying to sense how someone is feeling is being rolled out by advertisers, police, security services, and recruiters, despite legal concerns. ERT and its regulatory challenges are discussed at length in Chapter 5.

1.3.6 *Enable Greater* Autonomy *of Clever Computing Systems*

Due to physical sensors and actuators, the IoT can directly respond to real-world inputs, increasingly autonomously. This could be as simple as connected light sensors that reach a certain level of lumens and then trigger actuators to open blinds around the house. However, not all IoT requires AI; for example, smart meters that only log and visualise hourly energy use data to an in-home display but conduct no prediction and recommendations around future use. Similarly, not all AI requires real-time input from physical sensors; for example, automated content moderation systems focused purely on identifying harmful online content on social media. However, with Clever Computing, the focus is on the convergence of physicality of the IoT coupled with inferential AI infrastructures.

[139] Photoplethysmogram, which measures blood oxygen levels.

[140] Oura Ring Website, https://ouraring.com/.

[141] Bellabeat Ivy+ Website, https://eu.bellabeat.com/. This bracelet is 'specifically designed for women' supporting wellbeing, pregnancy planning, and hormonal changes.

[142] Hon Pak, 'Solving the Digital Health Dilemma: Samsung's Vision for an Intelligent Health Platform' (*Samsung Mobile Press*, 26 February 2024). www.samsungmobilepress.com/feature-stories/editorial-solving-the-digital-health-dilemma-samsungs-vision-for-an-intelligent-health-platform.

[143] Lauren Rhue, 'Racial Influence on Automated Perceptions of Emotions' *Working Paper SSRN* (2018). DOI: 10.2139/ssrn.3281765.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

As AI may support increased autonomy of IoT systems, more advanced Clever Computing systems drawing together multiple physical sensors and AI technologies migrate into the territory of *robotics*. Robotics research and development has traditionally involved more complicated, embodied machines interacting with their environment with a higher level of autonomy, completing a wider range of complex tasks, such as autonomous mobile machinery, as discussed in Chapter 5.[144] Autonomous vehicles utilise AI with onboard sensors, like LiDAR, to support navigation and make real-time assessments about collision hazards and how to respond. Yet, it can be difficult to strictly demarcate between existing technological labels. For example, is a Roomba vacuum cleaner a robot or an IoT device? What about a home security drone? Is a smart watch that infers emotions from collecting our heart rate and makes lifestyle suggestions AI or IoT? As I explored in work with Natalie Leesakul and Dominic Reedman Flint, domestic IoT devices are increasingly being augmented and adapting with the growth of home robotics.[145] Thus, as systems get more advanced and autonomous due to the complexity of sensors and actuators they are using, the boundaries between Clever Computing and robotics will blur further. The emergence of 'agentic AI' i.e. 'autonomous systems designed to pursue complex goals with minimal human intervention' is further confounding this blurring.[146] Agentic AI involves systems that can adapt, react and multi-task with greater independence, often over longer periods of time, not just assisting humans in tasks e.g. autonomous cybersecurity threat detection on networks.[147] Currently, Clever Computing provides a useful umbrella term to encapsulate the ways interactive, material IoT systems will continue to change through the addition of AI.

1.4 CONCLUSIONS

This chapter proposed the nascent concept of Clever Computing. Physical IoT sensing devices and ecosystems, which have been around for some time, are now changing through the integration of advanced data-driven AI techniques. AI is augmenting the IoT in many ways and will continue to do so. Currently, it is altering how users interact with devices, supports new data management architectures, layers

[144] Alan Winfield, 'What Is a Robot?' in Alan Winfield (ed.), *Robotics: A Very Short Introduction* (Oxford University Press: Oxford, 2012).

[145] Lachlan Urquhart, Dominic Reedman-Flint, and Natalie Leesakul, 'Responsible Domestic Robotics: Exploring Ethical Implications of Robots in the Home' *Journal of Information, Communication and Ethics in Society* (2019) 17(2) 246–272. DOI: 10.1108/JICES-12-2018-0096.

[146] Deepak Acharya, Karthigeyan Kuppan and B. Divya, 'Agentic AI: Autonomous Intelligence for Complex Goals—A Comprehensive Survey' *IEEE Access*, 13. 18912–18936, 2025, DOI: 10.1109/ACCESS.2025.3532853

[147] Nir Kshetri, 'Transforming Cybersecurity with Agentic AI to comDOI: Bat Emerging Cyber Threats' *Telecommunication Policy* (2025) 49, 6. https://doi.org/10.1016/j.telpol.2025.102976

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001

new AI functionality into systems, and increases autonomy of decision-making by IoT devices. But AI-enabled IoT will continue to adapt and shift.

Clever Computing is a necessary new label that encapsulates the convergence of the data, software, and hardware aspects of the IoT, with AI infrastructures, as an analytical focus. It centres the importance of sensing the physical world and the associated socio-technical and legal impacts of materiality posed by data-driven AI. It foregrounds how AI further amplifies regulatory issues already present in the IoT, through increasing the complexity and uncertainty of how these systems interact in the world.

The chapter also looked backwards to contextualise these shifts within the history of precursors to Clever Computing, particularly Ubicomp. As the IoT and AI become more closely coupled, examining Ubicomp research and development showed how user requirements were often neglected in favour of techno-driven visions that promised better futures but did not deliver. These systems were often not integrated into users' lives in the clean, unencumbered way that designers anticipated. Instead, the reality of technology deployment surfaced the messy, social complexities that design needs to contend with and which shape processes of domesticating technologies into everyday life. This shows why human-centred approaches that foreground user best interests, which extends to legal rights and responsibilities, are central to Accountable Design.

Present-day AI-enabled IoT often adopts a similar narrative of fixing or at least improving responses to complex societal problems through technology, whilst neglecting the complexity and lived experience of users, often leading to significant socio-technical and legal harms when released into the wild. In drawing inspiration from scholars who championed the need to understand the *social* in system design processes, I now propose Accountable Design to argue for accounting for the *legal* in design. This is necessary to move towards building more secure, trustworthy, safe, and privacy-preserving Clever Computing.

Downloaded from https://www.cambridge.org/core. UNIVERSIDAD AUTONOMA METROPOLITANA, on 12 Nov 2026 at 17:02:13, subject to the Cambridge Core terms of use, available at https://www.cambridge.org/core/terms. https://doi.org/10.1017/9781108985734.001