Ethical Case Study Analysis: The Internet of Things

The Internet of Things (IoT) has transformed from a futuristic concept into something woven into everyday life. As described in the FwThinking video, the IoT connects billions of sensors embedded in devices such as refrigerators, watches, vehicles, and buildings, creating a world “blanketed with billions of sensors” that respond to human behavior in real time (Pollina, 2013, 1:00-1:10). These systems collect, analyze, and share information constantly, making life more efficient and personalized. Yet, as that personalization deepens, it brings complex ethical challenges about privacy, consent, surveillance, and ownership of data. Understanding these implications is essential for anyone entering the information profession, where technology and human values increasingly intersect.

The Brookings Institution commentary on IoT highlights both its promise and its perils. Darrell M. West (as cited in Karsten, 2016) noted that sensors can “help humans manage the annoyances of daily life,” from traffic jams to energy waste, but warned that this same connectivity “will raise serious security, privacy, and policy issues.” Fellow scholar Susan Hennessey (as cited in Karsten, 2016) expanded on that risk, observing that IoT devices may create “prime mechanisms for surveillance,” allowing governments or private entities to monitor citizens through everyday objects. These concerns illustrate the ethical tension between convenience and control. As an information professional, it is not enough to appreciate the technology’s capabilities. We must evaluate how data is collected and who benefits from its use.

Singer and Perry (2015) provide a concrete example of these issues in their discussion of wearable technology. They explain that most wearable devices collect far more data than users realize, including “precise location data” and health metrics, which are often shared with third parties for marketing or legal purposes. The authors argue that companies must “clearly communicate what data is being collected” and “what data are being shared” to ensure users give informed consent (p. 25). However, even the best-written privacy policies often fall short because they are too complex for average users to interpret. This problem underscores a broader ethical principle: transparency alone is not enough. Users need control and comprehension, not just disclosure. For professionals who manage or design information systems, that means simplifying privacy communication, advocating for opt-in consent models, and treating data stewardship as a public trust rather than a corporate asset.

Coleman (2025) pushes this discussion further by reframing IoT as part of a larger phenomenon called the Internet of Bodies (IoB). She defines the IoB as the “extension of the Internet of Things to the human body,” where wearables, implants, and smart health systems collect real-time biometric data (para. 13). Coleman describes how this data can improve health outcomes but also warns that it transforms our physical selves into “tradable assets” within what she calls “a data extraction economy” (para. 26). Her account of the 2023 23andMe data breach, in which hackers accessed the genetic information of 6.9 million users, illustrates how these systems turn deeply personal biological information into something permanently vulnerable (para. 38). Coleman’s

central idea of infrastructure literacy, or understanding how our data flows through invisible systems, is a powerful ethical framework. It challenges us to design technologies that serve people first, ensuring transparency, consent, and community control over data.

Each of these perspectives points to a shared moral question: How do we balance innovation and human dignity? The answer lies partly in policymaking and partly in professional ethics. As Scott Andes (as cited in Karsten, 2016) argues, IoT policy should support “sound science” and “entrepreneurs’ access to capital,” but it must also safeguard equity and privacy. Policies such as Europe’s GDPR and California’s CCPA represent steps toward giving users agency, but true ethical progress depends on how organizations and information professionals implement those ideals in practice. This includes adopting dynamic consent models (Coleman, 2025), restricting unnecessary data sharing (Singer & Perry, 2015), and designing infrastructure intentionally so that data collection aligns with community values.

Applying critical thinking to this case means examining not only the technical facts but also the assumptions behind them. The IoT assumes that more data equals better outcomes, but that assumption overlooks context: not every connection improves life, and not every metric reflects truth. In evaluating IoT ethically, I asked myself whose problems the technology solves and whose it might create. From the FwThinking vision of self-regulating homes to Coleman’s warning about algorithmic “behavioral capture,”

the lesson is the same: technology is only as ethical as the intentions and policies that guide it.

In conclusion, the Internet of Things represents both progress and peril. It promises convenience, efficiency, and even improved health, yet it also invites surveillance, inequity, and loss of autonomy. The ethical path forward demands infrastructure literacy, strong privacy protections, and a commitment to designing systems that prioritize human well-being over data monetization. As a future information professional, my role will be to help build that balance, translating these insights into policies, designs, and practices that keep technology accountable to the people it serves.

References

Coleman, A. S. (2025, May 3). *Infrastructure literacy: Understanding the Internet of Bodies. Infophilia: A Positive Psychology of Information*, 3(21). https://infophilia.substack.com/p/infrastructure-literacy

Karsten, J. (2016, March 25). *Alternative perspectives on the Internet of Things. Brookings*. https://www.brookings.edu/articles/alternative-perspectives-on-the-internet-of-things/

Pollina, N. (2013). *What is the Internet of Things?* [TED-Ed video]. *FwThinking*. https://ed.ted.com/on/VGdKwYzz

Singer, R. W., & Perry, A. J. (2015). Wearables: The well-dressed privacy policy. *Intellectual Property & Technology Law Journal, 27*(7), 24–27. https://go.gale.com/ps/i.do?p=AONE&u=tamp44898&id=GALE%7CA420929651&v=2.1