EAST WEST UNIVERSITY

Cybersecurity, Law, and Ethics

CSE 487 / ICE 453
Section: 03

Mini Project-03

Project Title: IoT Security and Consumer Risk

Submitted to

Dr. Md. Hassanul Ferdous
Associate Professor
Department of Computer Science & Engineering
East West University

Submitted by (Group - 11)

Sumit Kumer Das	2021-3-50-002
Hrittik Chakraborty	2021-2-50-011
Dabnil Malaker	2020-3-50-003
Junayed Karim	2021-1-50-011

Submission Date: 22nd May 2025

Introduction:

The Internet of Things (IoT) has connected billions of devices across the world and connected technology with daily life. From voice assistants and fitness trackers to smart fridges and security systems, these devices constantly collect, transmit, and process user data. But hyperconnectivity comes at a cost, and producers like to emphasize innovation and time to market over robust security. Therefore, consumers become more vulnerable to cyberattacks, identity theft, and surreptitious data collection. The ethical dilemma arises where developers must balance between profit maximization and ensuring good, privacy-conscious product development. Should developers be legally and morally accountable for preventable security flaws? Can ignorance or carelessness be ethically acceptable under such risky circumstances? The challenge also puts into focus the gap between technological advancement and moral responsibility. Since the world is quickly converging towards interdependent systems, the absence of inherent security not only jeopardizes the people but also the digital ecosystem at large. The question then is whether prudence should come second to convenience, especially when millions of innocent users are collateral damage in the bargain. The expansion of IoT to the most critical sectors, such as healthcare, transportation, and home automation, has increased the stakes. The hacking of a single device can make the entire system collapse or cause physical harm.

Stakeholder Analysis:

a) Consumers:

Customers are typically technically illiterate; therefore, they are unable to appreciate how much information is being gathered or the risks of unsecured links. They are exposed and largely precluded from influencing design and security considerations about these devices. They depend more on firms to incorporate safeguards and provide full disclosures. Being uninformed about how they gather and use their data disadvantages consumers. Since they are passive actors in the technology cycle, they are innocent victims of corporate complacency or lax regulation. They even pay to repair damage when corners are cut, becoming victims of identity theft, financial loss, or emotional distress. The disparity between producers and consumers in terms of power and knowledge creates a moral obligation for the former to be transparent, proactively informing users and designing interfaces such that users' agreement and control are always at the forefront.

b) Manufacturers and Developers:

They are faced with the moral dilemma of saving money versus moral responsibility. Avoiding the use of secure practices such as encrypted data transfer, firmware download, or user authentication is a violation of their duty of care. Many also grapple with competitive forces for rapid-to-market products, typically without performing rigorous testing. Skipping careful screening, however, destroys long-term trust and damages brand credibility. Ethical duty compels such companies to care for something beyond profits and take into account the social consequences of their technological advancements. Ethical design begins at the planning phase. Component selection, data use policies, and interface behavior choices establish the ultimate safety and transparency of IoT products. Developers must embrace a security-first mindset and conduct impact assessments to reduce likely risks before devices even find their way into consumers' hands.

c) Regulatory Bodies:

They are responsible for laying down minimum security standards. In most countries, regulation has trailed the speed of technology, which has resulted in a state where companies can evade accountability until harm is caused. Additional government oversight is required to provide consistent frameworks that mandate secure design principles and sanction unnecessary security flaws. International IoT security norms could help simplify expectations and minimize cross-border vulnerabilities. By promoting security compliance certifications, governments can push the tech industry toward good behavior. Laws must also include mandatory breach reporting, consumer notification, and penalties for negligent manufacturers.

d) Retailers and Distributors:

By carrying vulnerable IoT products, retailers also bear a secondary ethical duty. Retailers ethically should require compliance certificates and offer open consumer disclosures. Retailers are gatekeepers between consumers and manufacturers and represent a key point of leverage. Providing secure product options and enabling transparency may help induce a market shift toward ethical production. Through this, they encourage responsibility throughout the supply chain and offer a culture of responsible and informed consumption.

e) Cybercriminals:

Even though they are malicious attackers, their role proves that there must be an active and not passive approach towards IoT security. Their exploitation of systemic weaknesses is a wake-up call, reminding us that security cannot be an afterthought. That these threats continue to exist should prompt all stakeholders to work together and create a tighter, more solid IoT framework. Furthermore, the sophistication of cyberattacks only grows higher. From botnets to ransomware, not only are technical vulnerabilities being exploited, but there are also breakdowns in ethical design. This further adds to the need for ethical foresight in designing systems so that they are not exploited by reducing vulnerabilities at all levels.

Application of Ethical Frameworks:

ACM Code of Ethics and Professional Conduct

Key principles relevant here include:

- **Avoid Harm:** Harm includes psychological stress (surveillance), financial loss (hacked banking apps), or physical endangerment (tampered medical devices).
- **Respect Privacy:** Privacy is often violated by data-sharing defaults not clearly explained to users.
- **Give comprehensive evaluations:** Developers must fully assess risk and test systems accordingly. Applying these codes to IoT development highlights a clear ethical mandate. Professionals must understand that every design decision carries real-world consequences. Ethical lapses in coding, testing, or disclosure can lead to widespread damage, both personal and societal. For instance, a connected baby monitor with a weak password policy may be hijacked and used for spying, a direct violation of harm prevention. It is not enough to follow best practices; professionals must anticipate harm and integrate preventive mechanisms from the outset.

ACM/IEEE-CS Software Engineering Code of Ethics:

- **Thorough testing:** It is immoral not to test devices for weaknesses before they go on sale.
- **System accuracy:** Misdescription of device security in advertising is dishonest and immoral.

This system solidifies the need for software engineers to conduct themselves in terms of integrity and caution. Encouraging amenities while purposefully omitting risk statements is deliberate deception. All these erode customer trust and tarnish the professional image. It also emphasizes joint responsibility. Project managers, engineers, and marketing organizations all must align their conduct with ethical norms so that safety, security, and accuracy do not take a backseat to deadlines or finances.

Web 2.0 Ethical Decision-Making Framework:

- **Recognition:** The identification of social and technical threats from mass-market insecure devices.
- **Evaluation:** Trade-off of profit vs. long-term user trust and social security.
- **Action and Reflection:** Shipping secure devices only and continuously adding to security post-launch illustrates ethical maturity.

This framework offers an analytical approach to ethical decision-making. It encourages executives and developers to pause and consider the full implications of their choices, from potential reputation damage to public backlash. This transparency fosters accountability and cultivates a corporate culture of ethical reflection instead of impulsive reactions.

Group's Ethical Right Choice:

Security and privacy, in our view, should be regarded as core features rather than add-ons. Manufacturers should conduct third-party security checks before releasing the product and disclose all privacy implications straightforwardly. Regular updates and patches must also be ensured. Governments should enforce compliance with standard security requirements for companies to be certified for consumer sales. These choices align with the obligations of harm avoidance, informed consent, and respect for consumers. Furthermore, we believe that ethical deliberation should guide each stage of the IoT life cycle from development and design to deployment and deprecation. Participating in these deliberations, and perhaps by way of advisory boards or usability testing, can create mutual trust. Ethical technology enables not only secure equipment but also informed and empowered citizens. In addition, we recommend developing public awareness campaigns and labeling that inform users about device security, similar to nutritional labels for food. Ethical practice in technology must be both systematic and user-focused, fortifying a shared sense of responsibility among creators, regulators, and consumers.

Criticism and Defense of the Decision:

Criticism 1: More security will delay product release.
Defense: Postponement is acceptable if it prevents irreparable harm. Ethical practice prioritizes user well-being over profit. Second, the postponement can be a competitive strength. Companies that prioritize safety and transparency as core values build long-term brand trust and avoid costly legal wars. An approach that is secure-by-design also lessens the need for crisis management, customer refunds, or brand redemption campaigns. Ethical action early on eliminates future liabilities and fosters sustainable innovation.

Criticism 2: Technical information is too complicated to use for everyday consumers.
Defense: Simplifying design (i.e., labels, security ratings) can make it consumable. Developers must collaborate with UX designers and educators to make it easy to understand disclosures. A symbol-based, multi-language system similar to food or energy ratings can revolutionize how individuals understand and manage digital peril. Besides, device onboarding processes can be minimized in complexity with secure default values and guided walkthroughs to allow even non-technical users to select privacy-safeguarding options.

Criticism 3: Regulation stifles innovation.
Defense: Ethic-based innovation is possible. Lack of standards breeds distrust and more long-term costs through litigation, damage to reputation, and recall. Instead of limiting development, ethical legislation can steer innovation in safer directions. Through a clear definition of what is expected, governments can encourage integrity-based competition, as opposed to shortcuts or cover-ups. Ethical guidelines being transparent also set an even playing field where all businesses are held to the same accountability standards, encouraging socially harmonious innovation.

Conclusion:

With the distinction between the digital and the physical diminishing in the era of the IoT. And with that, the responsibility to protect users from the unintended damage inflicted by poor security falls on our shoulders. Ethical computing demands that we anticipate threats and act in the public interest, upholding privacy, security, and transparency in every connected device. Ultimately, IoT security is not a technical challenge alone; it is a social problem that requires ethical stewardship. A commitment to do no harm, respect autonomy, and establish trust must guide all who labor in the IoT community. It is only then that we can build a future in which technology is used to empower us, not take advantage of us. As future engineers and developers, it is our duty to uphold these standards in the home as well as in the workplace. Ethical responsibility is not the enemy of progress; it is its cornerstone.