Automation:
Violated ACM ethics and by whom

- 1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing: Violated by K Industries for valuing government contracts and profit over societal well-being, especially concerning developing lethal autonomous systems.
- 1.2 Avoid harm: Violated by K Industries for creating a product that could harm customers and others involved in development due to its lethal capabilities.
- 2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks: Violated by K Industries for ignoring engineers' concerns about security risks and moving forward with a system that introduced ethical and safety vulnerabilities.

CIPA
Violated ACM ethics and by whom

- 1.2 Avoid harm: Violated by Safe Block's Development Team for launching a corrupted model that blocked legitimate content and harmed users' access to essential information.
- 1.4 Be fair and take action not to discriminate: Violated by Safe Block for purposely blocking content related to underrepresented groups and critical topics.
- 2.9 Design and implement systems that are responsible and usable secure: Violated by Safe Block Development Team for creating a system design that allowed activists to bypass the block, demonstrating a lack of adequate safeguards.

Dark Patterns
Violated ACM ethics and by whom

- 1.2 Avoid harm: Violated by Client and the Design Team for intentionally misleading users into choosing more expensive options, causing financial harm.
- 1.4 Be fair and take action not to discriminate: Violated by Client and the Design Team for using red and green text. This causes usability issues for visually impaired users, without implementing fairness.
- 3.3 Be honest and trustworthy: Violated by Client and the Design Team for betraying users' trust by deceiving users, indirectly scamming them.

Implants:

Violated ACM ethics and by whom

1.2 Avoid harm: Violated by Beatcore because they did not correctly address the security vulnerability in the implant's wireless connectivity, which could allow hackers to manipulate device commands and potentially harm users.

1.6 Respect privacy: Violated by Beatcore as the security vulnerability could expose sensitive patient data, compromising privacy and trust in the system.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks: Violated by Beatcore because they failed to thoroughly evaluate the risks associated with the wireless connection, leaving the system vulnerable to attacks.

Malware:

1.2 Avoid harm: Violated by Uptime Services for having hosted malicious services that exploited browser vulnerabilities, and enabled botnets, causing harm to users.

1.4 Be fair and take action not to discriminate: Violated by Uptime Services for refusing to take action and stop harmful activities, allowing illegal services to continue and negatively affecting users.

2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks: Violated by Uptime Services for not properly assessing the risks of hosting negative content, which led to a lot of harm.