SEMICONDUCTOR INDUSTRY ASSOCIATION

Voluntary Ethical Guidelines for Surveillance, Policing, and Semiconductors

Semiconductors are the lifeblood of modern technology products. The innovative devices produced by semiconductor companies enable everything from life-saving medical research to increased workplace productivity, green technology, and connection with people around the world. As semiconductors have become smarter, faster, and more efficient, they promise to deliver even more life-improving capabilities. However, it is possible that actors with malintent -- both private and governmental -- could use technologies enabled by advances in semiconductors to "engage in or enable violations or abuses of human rights including through violations and abuses involving censorship, surveillance, detention, or excessive use of force"[1].

Despite these concerns, modern surveillance technologies powered by artificial intelligence (AI), including software and big data analysis programs, have legitimate and beneficial uses. Among other things, these technologies offer the ability to reunite families displaced by war or famine,[2] increase public safety, manage traffic congestion, prevent accidents, and even reassure new parents that their child is sleeping safely. These same technologies, can however, also be used to enable malign ends such as human rights violations.

The vast majority of semiconductor components, however, are not specifically designed for surveillance applications. Most semiconductor products are inherently interchangeable in end-use devices, making it challenging to distinguish legitimate uses and downstream benefits from misuse and abuse. The surveillance supply chain in particular, due to its many layers, offers especially limited visibility for semiconductor producers. Although that means it may not be possible to stop all bad actors, the semiconductor industry understands the power of semiconductors as components to technologies and acknowledges our responsibility to do what we can to prevent their misuse.

Governments also have a critical role to play in this area. Among other things, government should play a lead role in the following ways:

1. With assistance and input from non-governmental organizations and human rights organizations, relevant government agencies should publicly identify activities and actors that pose ethical, privacy, and security concerns, so companies have guidance when planning business transactions.
2. Governments should identify and control technologies specifically designed to maliciously target minorities or undermine human rights, and they should monitor "neutral" technologies for disparate outcomes, regardless of design intent.
3. The US government should engage with partner countries to establish uniform principles and collaborative platforms that encourage information sharing and common ethical practices.

In addition to full compliance with all applicable laws and regulations, the industry suggests the following voluntary principles and guidelines for the sale and development of products, particularly as used in surveillance technology powered by AI. These general points are not exhaustive and serve as a starting point for future discussions to establish industry-wide standards.

---

[1] Federal Register Notice. "Amendment to Licensing Policy for Items Controlled for Crime Control Reasons". Bureau of Industry and Security, October 6, 2020. 15 CFR Part 742, RIN 0694-AH70.
[2] Murray, Laura. "Omdena Delivers Technology to Reunite Families After Earthquakes," February 11, 2020. https://omdena.com/pr/earthquake/.

Due Diligence

1. Monitor publicly available information on entities identified by governments and civil society, which pose ethical, privacy, and security concerns, and maintain internal watch lists, particularly as provided by governments and multilateral institutions driven by the protection of human rights.
2. Participate in multi-stakeholder dialogues to share new insights, best practices, information about incidents, and potential risks.

Customer Relations

1. Take appropriate steps to conduct due diligence and comply with all applicable rules and regulations for any customer on a government watch list.
2. Implement internal company policies that establish safeguards and penalties to ensure proper risk management is undertaken with regard to customers on government watch lists. These may include policies for product development, sales, end-use limitations, audits, and contract termination.

Development and Design

1. Refuse to design Application Specific Integrated Circuits (ASICs) or proprietary software known to be intended by the end-user to enable human rights violations or abuses of human rights, including those involving censorship, surveillance, detention, or excessive use of force[3].
2. Minimize bias in surveillance systems by applying the values of equality and diversity to ongoing development, testing, and data collection.
3. Prioritize the transparency of security and privacy in product design by preventing data breaches and the unlawful processing of data in compliance with the law of relevant jurisdictions.

Transparency and Traceability

1. Strive to make surveillance-related machine-learning decisions powered by semiconductor products explainable to human interrogators, including non-specialists, as well as urge customers to do the same.
2. Support stakeholders' right to know who is responsible for the consequences of decisions made by AI-powered surveillance systems.
3. Work with regulatory bodies to develop common frameworks for "mapping liability." Such frameworks should determine which actors and which levels of the surveillance supply chain are responsible for machine-learning decisions.

[3] Federal Register Notice. "Amendment to Licensing Policy for Items Controlled for Crime Control Reasons".