



## **MEDIA ADVISORY**

**Contact:** Jim Ormond  
ACM Media Relations  
212-626-0505  
[ormond@hq.acm.org](mailto:ormond@hq.acm.org)

### **Computing Leaders Propose Measures to Combat Tech-Facilitated Intimate Partner Violence, Human Trafficking, and Child Exploitation**

#### **Association for Computing Machinery Technology Policy Group Issues Issue Brief for Expanding Scope of Laws to Address Tech Abuse**

**New York, NY, February 25, 2025** – The Association for Computing Machinery’s Technology Policy Council (TPC) has announced the publication of “[TechBrief: Technology Policy Can Curb Domestic Violence, Human Trafficking, and Crimes Against Children](#),” a new issue brief which explains how intimate partner violence, human trafficking, and child exploitation are facilitated by computing technologies. The term “tech abuse” pertains to a wide variety of abuse in this context. The ACM policy experts contend that tech abuse is being addressed inconsistently, and often separately, by law enforcement, government agencies, and civil society. Studies indicate that these technology-facilitated activities are on the rise worldwide.

In its call to action, the TPC report urges policy makers and legislators to evaluate the technologies used in committing tech abuse crimes and, where possible, expand laws, regulations, and policies to protect people in all three areas. It urges tech companies to take actions to better protect users who may be subject to tech abuse.

Outlining the scope of the problem, the TechBrief includes some disturbing statistics. For example, a UK-based study found that 95% of domestic violence cases involved tech abuse. Another study cited in the report estimated that 500,000 child predators are online each day.

“From email to text messages to online platforms, the vast majority of our communications now happen via computing technology,” said Jody Westby, Chair of the ACM’s TechBriefs Committee and a co-author of the new TechBrief. “While everyone is aware of the benefits of these innovations, greater awareness is needed of how bad actors also use these systems to threaten, intimidate, control, surveil, monitor, and exploit targeted people. This TechBrief is designed to raise awareness of this problem and educate lawmakers and policymakers on how to draft laws broadly to curb tech abuse in intimate partner violence, human trafficking, and child exploitation. It also

aims to encourage tech companies to strengthen user protections and provide safeguards for targeted persons.”

The TechBrief highlights a recent legislative example of such lawmaking: the Safe Connections Act (SCA), which was passed by the US Congress in 2022, applies to several areas of abuse, provides protections for people subjected to abuse, and notes that “safeguards within communications services can serve a role in preventing abuse and narrowing the digital divide experienced by survivors of abuse.”

Building on the SCA and similar efforts in other countries, the new TechBrief recommends that:

- Service providers should provide advocates and case workers with privileged channels to be used when their clients are being abused.
- Technology providers should develop user interfaces (UI) with the consideration that an abuser might take a logged-in device from a user and change settings to enable the device to be used against their target—becoming what experts call a “UI-bound adversary.”
- Tech platform companies should consider designing security features in their technologies and providing technically detailed forensic information that would be valuable in tracking abuse perpetrators.

“I’ve spoken with many people who have either experienced tech abuse or tried to help others. None of these people have been able to get substantive help from a major tech platform using any sort of documented channel,” says Simson Garfinkel, co-author of the new TechBrief. “Sometimes somebody has a friend at a company who can provide some kind of unofficial help, but these informal approaches simply cannot scale to address this problem. We need the tech platforms, regulators, law enforcement, and legislators to take this problem seriously and address it head-on.”

ACM’s [TechBrief series](#) is designed to complement ACM’s activities in the policy arena and to inform policymakers, the public, and others about the nature and implications of information technologies. Earlier TechBriefs have covered topics such as [data privacy](#), [automated vehicles](#), [trusted AI](#), [the data trust deficit](#), [safer algorithmic systems](#), [generative AI](#), [climate change](#), [facial recognition](#), [smart cities](#), [quantum simulation](#), and [election auditing](#). Topics under consideration for future issues include media misinformation/disinformation, accessibility, explainable AI, AI and the future of work, and more.

#### **About the ACM Technology Policy Council**

[ACM’s global Technology Policy Council](#) sets the agenda for global initiatives to address evolving technology policy issues and coordinates the activities of ACM’s regional technology policy committees in the US and Europe. It serves as the central convening point for ACM’s interactions with government organizations, the computing community, and the public in all matters of public policy related to computing and information technology. The Council’s members are drawn from ACM’s global membership.

#### **About ACM**

[ACM, the Association for Computing Machinery](#), is the world's largest educational and scientific computing society, uniting computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

###