Finding Laws To Charge Perpetrators Who Misuse Technology

When a perpetrator, abuser or stalker misuses technology to target and harm a victim, there are various criminal and civil charges that might be applied to ensure accountability and promote victim safety. There are a number of U.S. federal and state/territory/tribal laws that might apply. To support the safety and privacy of victims, it is important to take technology-facilitated abuse and stalking seriously. This includes assessing all ways that technology is being misused to perpetrate harm, and, considering all charges that could or should be applied.

Identify laws that address violence and abuse. Identify where they explicitly or implicitly include the use of technology and electronic communications:

- Stalking and cyberstalking (felony menacing by, via electronic surveillance, etc.)
- Harassment, threats, assault
- Domestic violence, dating violence, sexual violence, sexual exploitation
- Sexting and child pornography: electronic transmission of harmful information to minors, providing obscene material to a minor, inappropriate images of minors, lascivious intent
- Bullying and cyberbullying
- Child abuse

Identify possible charges related to technology, communications, privacy and confidentiality:

- Unauthorized access, unauthorized recording/taping, illegal interception of electronic communications, illegal monitoring of communications, surveillance, eavesdropping, wiretapping, unlawful party to call
- Computer and Internet crimes: fraud, network intrusion
- Identity theft, impersonation, pretexting
- Financial fraud, telecommunications fraud
- Privacy violations: Reasonable expectation of privacy, upskirting, downblousing, voyeurism, secretly recording a person in the nude
- Confidentiality violations: including laws that apply to the agency the perpetrator works for
- Defamatory libel, slander, economic or reputational harms, privacy torts
- Burglary, criminal trespass, reckless endangerment, disorderly conduct, mischief, obstruction of justice, possession of a device for unlawful purposes
- Consumer protection laws
- Violation of no contact, protection and restraining orders
Identify if the perpetrator violated laws in multiple jurisdictions, including state and federal levels:

In addition to local/state laws, there are a range of U.S. federal laws that might be relevant. For example, the U.S. Electronic Communications Privacy Act (ECPA) addresses access, use, disclosure, interception and privacy protections of electronic communications.

- Title I of the U.S. Electronic Communications Privacy Act (ECPA) (18 USC §2511) prohibits interception and disclosure of wired, oral or electronic communication while in transit. This law may apply when a perpetrator wiretaps a phone line, does physical bugging, or puts a keylogger on someone’s computer.

- Title II of ECPA, The Stored Communications Act (18 USC §§2701-12) makes it unlawful to intentionally access stored communications without authorization or by exceeding authorized access. This law may apply when a perpetrator accesses someone else’s email, voicemail, online social networking account or information stored on a computer or with a cloud provider. See also, NNEDV’s tipsheet on *Cloud Computing*. 