

In this journal I will review [Andriy Slynychuk's](#) article describing eleven things Internet users do that may be illegal and describe the five I think are the most serious violations and why those offenses are serious.

I consider collection of children's information to be number one on my list of serious offenses. The US child safety agency received over thirty-two million reports of online enticement, abuse material and child trafficking in 2022. Parents and caregivers are very aware of the threats that children face day to day in both their school and social environment. Their digital environment is no less dangerous, considering the harms of enticement, financial exploitation and sex trafficking that can occur in an environment where attribution and prosecution of offenders becomes an order of magnitude more difficult. This makes protection of their personal information and location data even more critical and why the children's online privacy protection act was passed in 1998 (Federal Trade Commission 2023). Especially when considering the level of anonymity that our modern digital environment can provide to predators masquerading as figures of trust or authority. Or companies like Roblox that are being sued for financially exploiting children by allowing users including kids to use their in-game Robux that's purchased with cash to gamble on virtual items. (Gach, 2023).

Bullying and trolling would be my number two most offense for several reasons. The psychological harms to the victim produced by these online acts can lead to depression, self-harm, suicidal ideations and in many cases deaths. Various forms of harassment such as swatting and stalking can also ensue, escalating to threats of violence, bodily harm or death. The threat created by this online behavior threatens young adults, teens, and children had increased in such magnitude that by 2021, forty-eight states in the U.S. had electronic harassment laws which explicitly included cyberbullying and criminal sanctions for cyberbullying. With forty-five

crafting laws regarding school sanctions for cyberbullying. The third would be faking your identity online. There is a wide array of criminal behaviors associated with identity fraud, using a faked identity to steal medical or financial data, to commit credit card fraud all for financial gain. This can lead to potential legal and reputational consequences for victims, as they spend money and time trying to clear their name with credit bureaus and banks due to debts caused by fraudulent accounts opened by the identity thieves while avoiding being potentially charged for a crime they didn't commit. The identity theft and restitution act of 2008 increases penalties for identity theft and authorizes criminal restitution orders to compensate victims for the time spent to remediate the actual harm. (H.R.6060, 2008). Sharing passwords, addresses or photos of other would be number four. Making individuals private addresses and locations public without permission is a form of harassment and is now more common when talking about cyberstalking. While not specifically illegal, if the information is obtained illegally such as breaking into an account or installing malware on a device to access location data. The individuals or groups involved could and should be charged with violating the computer fraud and abuse act. These types of behaviors often precede calls for violence against the individual, putting other innocent family members and bystanders at risk.

Number five on the list is recording a voice over Ip call without consent. This can become an issue of infringement on the privacy rights of the individuals involved. Federal laws only require a single party to consent to recording a telephone conversation. Individual states do have laws that require two party consent to record. However, collecting or capturing private conversations of which you have no part is illegal under the electronic communications privacy act (ECPA, 1986). The bottom line for all eleven items in the list, is that while some of those actions may seem innocuous on the surface, they often result in the form of some kind of serious

harm to others. Which is why for most, if not all of those listed have state and federal statutes in place to mitigate and punish offenders engaged in those types of malicious behavior

References

- Technology, T. O. of. (2023, February 3). *Children's Online Privacy Protection Rule ("coppa")*. Federal Trade Commission. <https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa>
- Gach, E. (2023, August 18). *Popular online game accused of profiting off child gambling*. Kotaku. <https://kotaku.com/roblox-gambling-robux-lawsuit-metaverse-court-kid-safe-1850751687>
- H.R.6060 - 110th congress (2007-2008): Identity Theft Enforcement and Restitution Act of 2008 | congress.gov | library of Congress. (n.d.). <https://www.congress.gov/bill/110th-congress/house-bill/6060>
- Electronic communications privacy act of 1986 (Ecpa)*. Bureau of Justice Assistance. (n.d.). <https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1285>