
# COVID-19 and Technology-Enabled Intimate Partner Violence

## Submission by the Clinic to End Tech Abuse to the UN Special Rapporteur on Violence against Women

June 30, 2020

The Clinic to End Tech Abuse (CETA), a project of Cornell University, welcomes the decision of the Special Rapporteur on violence against women to examine the impact of the COVID-19 pandemic on survivors of intimate partner violence (IPV). Our submission addresses technology-related abuse and the threats it poses to survivors' safety and recovery, particularly when lockdowns, quarantines, and other public health measures limit survivors' movements and make them more dependent than ever on smartphones and other technology to find help.

Specifically, we address the obstacles that weak State privacy laws and company privacy policies can pose to IPV survivors during the pandemic (question 8), as well as good legal and policy measures that can combat technology-enabled abuse during a public health crisis such as this one (questions 9 and 10).

Since 2018, CETA has provided IPV survivors in New York City with direct assistance in ending technology-enabled abuse such as location tracking, unauthorized access to online accounts, and the use of "spyware" (apps that facilitate monitoring and stalking). We collaborate closely with local agencies and, during the pandemic, have created innovative remote services for survivors. We are also providing remote trainings to IPV support workers such as social workers and lawyers about how to help their clients end technology abuse.[1] Our operations are based on research that our affiliated faculty and students have conducted since 2016.[2]

This submission focuses on the situation for IPV survivors in the United States. However, many of our observations will be relevant wherever survivors widely use digital technology.

[1] For more information about CETA's mission and operations, see https://www.ceta.tech.cornell.edu.
[2] To view research publications related to our clinic, please see "Computer Security and Privacy for Survivors of Intimate Partner Violence," https://www.ipvtechresearch.org/research.

## I. Applicable international human rights law

***International human rights law requires States to ensure adequate respect for the privacy of everyone in their jurisdictions. However, weak State privacy laws, a failure to enforce laws banning technology-related IPV, and inadequate regulation of technology companies' practices can leave survivors exposed to serious harms by abusers. These insufficient protections create a particular danger during emergency situations such as the COVID-19 pandemic, when survivors become more reliant on phone and online communications and have fewer safe options for seeking help in person. States should address the threat of technology-related abuse during COVID-19 by strengthening and enforcing survivors' rights to privacy and data protection.***

The International Covenant on Civil and Political Rights provides at Article 17 that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy … or correspondence," and that "[e]veryone has the right to protection of the law against such interference." The Covenant also obligates States to "undertake[] the necessary steps … to adopt such laws or other measures as may be necessary" to give effect to these rights, if they have not yet done so.[3] The UN Human Rights Committee has concluded that States must protect individuals against rights-violating privacy interferences regardless of whether those interferences "emanate from State authorities or from natural or legal persons"[4]—a group that would include abusive partners as well as technology companies.

The Human Rights Committee has further concluded that States must effectively "ensure that information concerning a person's private life does not reach the hands of persons who are not authorized by law to receive, process and use it, and is never used for purposes incompatible with the Covenant."[5]

Today, State authorities know or should know that abusers frequently interfere with IPV victims' privacy and personal data, including information stored online or on devices, to coerce and control the victims. States should also realize that emergencies such as the COVID-19 pandemic can leave IPV survivors with little choice but to use technology to remain connected to the outside world and search for vital resources.

It is therefore imperative for States to adopt and effectively enforce laws to protect IPV survivors' safety online and on their devices—including by passing data protection laws that regulate how technology companies collect and store data in users' accounts, as well as laws that deter technology-enabled coercion by abusive partners.

Unfortunately, the situation in the United States illustrates how weak laws can make survivors vulnerable to technology-enabled abuse, especially during disasters such as the COVID-19 pandemic. For example, while the federal government and US states generally prohibit private individuals from secretly intercepting the content of a conversation, a gap in federal law has created a gray area where location data

[3] UN General Assembly, International Covenant on Civil and Political Rights, 999 U.N.T.S. 171 (1966), arts. 17, 2(2).
[4] UN Human Rights Committee, "General Comment No. 16: Article 17 (Right to Privacy)," (1988), para. 1.
[5] Ibid. at para. 10.

is concerned, and abusers can exploit this gray area to track their victims.[6] Technology companies in the US are also largely free to gather personal data about their users without clear consent or persistent notification requirements—meaning that abusers who illicitly gain access to their victims' online accounts can often view large amounts of sensitive data, including information the victim did not realize the company was collecting.[7]

## II. Technology-enabled abuse

For IPV survivors, modern digital technologies are a double-edged sword—and the COVID-19 pandemic has exacerbated this situation. Access to technologies such as smartphones can help survivors stay connected to the support networks they need to survive and recover from the abuse. However, abusers can exploit weak privacy laws and policies, as well as digital security mechanisms that were designed to protect users against strangers rather than someone who knows them intimately. An abuser can misuse a survivor's technology or accounts to learn everything about the survivor, such as their location and with whom they are communicating. For many survivors, the abuser's possession of this information is highly dangerous.

*Location tracking*

There are several ways an abuser can turn a victim's own devices or accounts against them to track their location, facilitating stalking, threats, physical attacks, and other harms.

Some cloud-based accounts, such as Google and iCloud, can collect information about an individual's location—sometimes without the user's persistent awareness. Many of these accounts offer security protections that are designed mainly with potential threats posed by strangers, such as fraudsters or identity thieves unknown to the victim, in mind. By contrast, an abusive partner who can force a victim to disclose their password, or who set up the account in the first place and manipulated its settings, could get access to these accounts and thus to location data with relative ease.[8] While many companies offer extra security measures, such as two-factor authentication, that could help prevent unauthorized access by someone an IPV survivor knows, many survivors are not aware that these protections are available and companies' online interfaces usually do not highlight them prominently.

Abusers who have had physical access to a survivor's device (such as a smartphone) can also surreptitiously install "spyware"—software that can monitor the survivor's location and information about their communications. Even after the survivor ends the relationship, spyware can still enable stalking and harassment. The same is true of what our affiliated researchers have identified as "dual-use" apps: those that can have a legitimate purpose, but that an abuser could misuse to monitor a victim. Our

[6] See Danielle Keats Citron, "Spying Inc.," 72 *Wash. & Lee L. Rev.* 1243, 1250-52, 1265-66, 1274-78 (2015).
[7] Regarding access to IPV survivors' accounts by "authenticated but adversarial users," such as an abuser who knows or has guessed a survivor's password, see generally Diana Freed et al., "'A Stalker's Paradise': How Intimate Partner Abusers Exploit Technology," *ACM Conference on Human Factors in Computing Systems* (2018), available at http://nixdell.com/papers/stalkers-paradise-intimate.pdf.
[8] Ibid.

affiliated researchers have documented a thriving online market in spyware, indicating that more effective legal restrictions are needed in the US and likely other States.[9]

In the United States, family mobile phone contracts can also give abusive partners access to information about the location of the victim's phone if both people are part of the same plan. (The same is true of any phones belonging to children.) Depending on the phone service provider, abusers may be able to view the location of the other phones that are on a shared contract by logging into the account. Abusers may also misuse family tracking apps that some providers offer as safety tools.[10] Many survivors likely cannot afford the financial penalties that can result from leaving a family plan, and although some US states have laws meant to help IPV victims exit such contracts, these laws vary and their usefulness and accessibility to survivors in practice remains unclear. This situation can leave survivors tethered to devices and service plans that let abusers track their locations.

Location-tracking poses particular dangers during an emergency such as the COVID-19 pandemic. During this crisis, many IPV survivors have fewer options than ever when searching for and traveling to a safe place to reside, whether in the immediate term (for example, when escaping from a home shared with the abuser) or in the longer term. Therefore, if an abuser discovers where the survivor is living, the survivor may not be able to flee to a more secure place.

**Recommendations:**

- **States should protect privacy rights by prohibiting access to location information for the purposes of stalking or other abuse -- and should ensure that authorities enforce this prohibition effectively. Legislatures should close any legal loopholes that could enable abusers to get access to their victims' location data.**

- **States should adopt strong data protection laws that give survivors both a legal and practical ability to control their location data, as well as control over other private or personal information about them that technology companies could collect and store.**

- **States should ban spyware and enforce this ban effectively. They should also ban abusers' misuse of applications that can have legitimate purposes but can also be used for stalking or other harms ("dual-use" apps).**

- **Technology companies should secure location information and other personal data through means that are effective against illicit access by an abuser.**

---

[9] Rahul Chatterjee et al., "The Spyware Used in Intimate Partner Violence," *IEEE Symposium on Security and Privacy* (2018), available at http://nixdell.com/papers/spyware.pdf.

[10] Regarding the role that "family" phone service plans can play in abuse, see generally Freed et al., *supra* n. 7; Emily Tseng et al., "The Tools and Tactics Used in Intimate Partner Surveillance: An Analysis of Online Infidelity Forums," USENIX Security Symposium no. 29 (accepted and forthcoming, 2020).

*Illicit access to online accounts*

As suggested above, abusers can often gain access to information from IPV survivors' social media, email, banking, dating, and other online accounts by guessing the password or through other means that are not technically sophisticated but nevertheless can lead to serious and dangerous intrusions.

During the COVID-19 pandemic, many individuals have been relying on technology more than ever to work, attend classes, get help from doctors and mental health counselors, buy food and other items to meet their basic needs, and stay in touch with friends and family. For IPV survivors, many of these activities are crucial to safety and recovery, and trying to conduct them offline is impossible or creates health risks during a pandemic. This involuntary reliance on technology creates an opening for abusers to learn more about survivors than ever by secretly getting access to their online accounts—and then using this information for coercion and control.[11]

An abuser who secretly gets access to a survivor's online account(s) could view the survivor's calendar, emails or direct messages, personal photos (potentially including intimate images and images showing where the survivor is), location information, and contacts' names and numbers. Information such as calendar entries showing a survivor's appointment with a doctor could easily reveal details about COVID-19 infection status or other health matters. At a time when the COVID-19 pandemic is causing widespread unemployment, an abuser could also use private information from online accounts to harm the survivor's reputation at work, make fraudulent purchases, or otherwise harm the survivor financially.

**Recommendations:**

- **States should effectively prohibit and punish abusers' malicious accessing of personal information in IPV victims' online accounts. States should also require training for law enforcement officers on how abusers can carry out such compromises, and ensure that State authorities investigate any illicit access to personal data.**

- **To better protect survivors' rights in practice, States should increase training resources for IPV support workers so they can help survivors detect and end account compromises by abusers.**

- **States should require technology companies to give users full control over what personal data is collected and stored in online accounts. States should also require technology companies to create privacy settings that are clear, prominent, and based on genuinely informed consent.**

- **Technology companies should secure all online accounts through means that are effective against illicit access by an abuser.**

[11] See generally Alison J. Marganski & Lisa Melander, "Domestic abusers use tech that connects as a weapon during coronavirus lockdowns," *The Conversation*, June 18, 2020, https://theconversation.com/domestic-abusers-use-tech-that-connects-as-a-weapon-during-coronavirus-lockdowns-139834.

- **Technology companies should regularly notify users about the types of personal data the company or the user is collecting and storing in the user's online account.**

## III. Privacy and data protection on online platforms used for IPV services

During the COVID-19 pandemic, IPV survivors in the US have faced threats to their privacy and data protection not only from abusers, but also from technology companies whose privacy practices US law does not regulate thoroughly or effectively.

As US state authorities began issuing "stay at home" orders in response to widespread risk of infection, many doctors, mental health professionals, lawyers, and IPV support workers made a transition from in-person to online appointments. When doing so, they generally have had little choice but to use video- or teleconferencing platforms owned by private companies. A lack of strong data protection laws in the US means that—depending on the applicable terms of service—companies could use data from these appointments in ways that are inconsistent with privacy, human dignity, or other human rights. When using the platforms, neither the survivor nor the professional helping them may realize how data from the call could be stored and used, or provide genuinely informed consent.

To strengthen survivors' rights protections, we reiterate that **States should adopt strong data protection laws that give survivors a legal and practical ability to control the personal data that technology companies collect and store about them**, including data about communications.

## Conclusion

The COVID-19 pandemic has exacerbated the threat of technology-enabled abuse that IPV survivors face, and at least in the United States, federal and state legislatures and regulatory agencies have yet to respond by strengthening rights protections.

States worldwide should revisit their privacy and data protection laws during the pandemic to ensure that IPV survivors and those who support them can protect the survivors' lives, health, and access to crucial resources during public health crises such as this one. States should also ensure that their laws effectively deter, and their authorities effectively investigate and punish, technology-enabled abuse—not only during the COVID-19 crisis, but at all times.