

The Technology Abuse Clinic Toolkit



Dana Cuomo
Nicola Dell
Alana Ramjit
Thomas Ristenpart

Table of Contents

| | |
|--|----|
| Chapter 1: Introduction | 5 |
| A Guide to the Toolkit: Worksheet | 7 |
| Chapter 2: Overview of a Technology Abuse Clinic | 16 |
| Why Technology Abuse Clinics? | |
| Essential Features | |
| Overarching Principles | |
| Secondary Initiatives | |
| Chapter 3: Agency Partnerships | 22 |
| Why is an Agency Partnership Needed? | |
| Examples of Agency Partnerships | |
| Features of Successful Agency Partnerships | |
| Setting Up Agency Partnerships | |
| Managing Client Referrals | |
| Advertising Clinic Services | |
| Receiving Client Referrals | |
| Referring Clients to Other Services | |
| Maintaining Partnerships | |
| Chapter 4: Service Delivery Models | 30 |
| Care Models | |
| Scope of Services | |
| Referrals | |
| Intake, Screening, and Triage | |
| Scheduling | |
| Medium of Appointments | |
| Chapter 5: Staff and Personnel | 41 |
| Recommended Personnel | |
| Referral Coordinator(s) | |
| Technology Staff Manager | |
| Technology Consultants | |
| Digital Abuse Specialist (Optional) | |
| Traits and Qualifications | |
| Morale and Mental Health | |

| | |
|--|----|
| Chapter 6: Technology Consultants | 47 |
| Volunteer vs. Paid Technology Consultants | |
| Recruiting Technology Consultants | |
| Receiving and Screening Applications | |
| Training and Evaluation | |
| Screening Technology Consultants | |
| Leaving the Technology Abuse Clinic | |
| Chapter 7: Conducting an Appointment | 55 |
| Principles for Working with Clients | |
| Handling an Appointment | |
| Preparing for an Appointment | |
| Conducting the Consultation | |
| Understand | |
| Investigate | |
| Plan, Inform, and Advise | |
| Post Appointment Follow Up | |
| Chapter 8: Clinic IT and Data Management | 69 |
| Collecting Personal Identifiable Information | |
| Legal Risks of Data Collection | |
| Redacting Data Collected from Client Sessions | |
| Communications Infrastructure | |
| Storage, Access, and Authentication | |
| Managing Data Policies | |
| Research, Evaluation and Analytics | |
| Chapter 9: Helping with Technology Abuse | 76 |
| Introduction to Technology Abuse | |
| Understanding Intimate Partner Threats | |
| Core Security Concepts | |
| Devices and Their Security | |
| Operating Systems and Applications | |
| “Hacking” a Device | |
| Full Device Compromise | |
| Spyware, Stalkerware, and Unauthorized Device Access | |
| Electronic Monitoring Devices | |
| Recording Devices | |
| GPS and Locating Tracking Devices | |

| | |
|--|-----|
| Chapter 9: Helping with Technology Abuse Con't | 76 |
| Accounts and Their Security | |
| Authenticating Online Accounts | |
| Authentication as an Abuse Mechanism | |
| Account Recovery | |
| Security Tools to Mitigate Harassment | |
| Being Prepared to Help with Unfamiliar Technology | |
| Appendix I: Clinic Histories | 90 |
| Appendix II: Resources | 93 |
| A. Chapter 3: Agency Partnerships | 94 |
| Memorandum of Understandings (MOUs) | |
| Advertising Services | |
| Flyer | |
| Referral Guide | |
| B. Chapter 4: Service Delivery | 101 |
| Intake Forms | |
| CETA | |
| MTC | |
| TECCC | |
| C. Chapter 6: Technology Consultants | 115 |
| Call for Consultants Flyer | |
| Interview Guide | |
| Rubric for Applicants | |
| Training Plan | |
| Guidebooks | |
| Onboarding New Volunteers | |
| Technology Consultants | |
| D. Chapter 7: Conducting an Appointment | 154 |
| Note-taking Infrastructure | |
| Technology Assessment Questionnaire | |
| Tech Safety Checklist | |
| E. Other Organizations & Additional CETA Resources | 171 |

Introduction

The goal of this toolkit is to provide practical guidance and resources for people who are interested in starting and sustaining a technology abuse clinic that provides services and assistance to survivors experiencing technology abuse.

The contents of this guide are based on the authors' experiences establishing and running several such technology abuse clinics, namely the Technology Enabled Coercive Control (TECC) clinic in Seattle and the Clinic to End Tech Abuse (CETA) in New York City, both started in 2018.

An affiliate from CETA later established the Madison Tech Clinic, in a partnership with the University of Wisconsin-Madison and the Madison-based advocacy agency, DAIS.

These clinics operate independently, each taking somewhat different approaches to assist survivors who are experiencing technology abuse. This guide aims to bridge these efforts, distilling for readers the overlapping components and core insights gained as we strive towards the common goal of increasing resources for survivors experiencing technology abuse.

The following chapters provide guidance on what we consider to be the essential (as well as optional) components of technology abuse clinics, steps to take when establishing a clinic, and examples of processes/procedures that we have found successful while operating a clinic.

We note that the approaches, procedures, and services described here have undergone many iterations over the years that build on numerous lessons learned from operating technology abuse clinics, including significant changes in response to the logistical challenges faced during the COVID-19 pandemic in early 2021.

The advice and recommendations provided in this guide are not intended to be prescriptive. There are undoubtedly numerous ways to create a technology abuse clinic and the information provided here is inherently limited by our own communities, geographies, and subjective experiences.

Readers are therefore encouraged to view the guidance and examples as a starting point and adapt the content to their communities and locales as needed.

Finally, we note that this toolkit is written from the perspective of clinics serving survivors of intimate partner violence. We actively encourage others to explore service provision in the context of other forms of interpersonal abuse (:e.g., elder abuse, human trafficking).

However, we are only equipped to speak to our experiences in intimate partner violence advocacy, and we have written the toolkit accordingly.

Nonetheless, we believe that many of the tools and resources can be carefully adapted for use with other populations by considering the unique risks or differing severity of concern in other populations that we have not investigated.

A Guide to the Toolkit: Worksheet

The following worksheet provides a brief description of each toolkit chapter, along with a set of questions to consider as you read each chapter and plan your technology abuse clinic.

Not all of the guiding questions may have clear and immediate answers, but the chapters are designed to help you answer each set of questions. You are encouraged to return to the worksheet as you progress in the development of your technology abuse clinic.

Chapter 2: Overview of a Technology Abuse Clinic

This chapter introduces what a technology abuse clinic is and how its features are different from already existing technology helpdesk services. The chapter also provides a set of overarching principles that guide the development and facilitation of a clinic. Questions to consider as you review this chapter include:

- What principles will guide your clinic?
- What are the unique needs of your community?
- Will your clinic support secondary initiatives beyond providing direct services to address survivors' digital safety needs?

Notes:

Chapter 3: Agency Partnerships

This chapter discusses the importance of building and maintaining strong partnerships with survivor support services and/or community partner agencies. The chapter also provides suggestions for managing clinic referrals. Questions to consider as you review this chapter include:

- What anti-violence intervention services already exist in your community?
- Who is sitting at the table as you develop your technology abuse clinic and what are their areas of expertise (e.g.: technology experts, advocacy experts, legal experts)?
- Who is missing and how can you account for missing skill sets and knowledge that would support the development of your technology abuse clinic?
- In what way are existing services and resources in your community not meeting the needs of survivors?

Notes:

Chapter 4: Service Delivery Models

This chapter introduces different approaches for delivering services to survivors within a technology abuse clinic, from how clinic staff connect with survivors to the scope of services that the clinic offers. The chapter also provides insight to managing client requests for services, including suggestions for how to conduct intakes, screen and triage clients, and schedule appointments. Questions to consider as you review this chapter include:

- Will your clinic offer drop in appointments, short-term and/or long-term care?
- Will your clinic offer in-person and/or remote appointments?
- What scope of services will your clinic offer?
- How will survivors be referred into your clinic for services?
- How will your clinic triage referrals for services?
- What is your clinic's approach to scheduling appointments?

Notes:

Chapter 5: Staff and Personnel

This chapter provides information about options for staffing a technology abuse clinic, including considerations for recruiting and managing staff and personnel. Questions to consider as you review this chapter include:

- Will your clinic recruit new personnel to staff the clinic or will you add clinic responsibilities to the duties of already existing staff?
- Does your clinic have resources to pay technology consultants or will your technology consultants work as unpaid volunteers?
- How will you incorporate resources and practices to support staff morale and mental health?

Notes:

Chapter 6: Technology Consultants

This chapter offers insight to the role of the technology consultants, including how to recruit, support, train, and evaluate technology consultants. Questions to consider as you review this chapter include:

- Does your chosen service delivery model require that you recruit local technology consultants?
- What existing networks or professional organizations are you already connected with that can assist with recruitment?
- What traits and characteristics are you looking for in a technology consultant?
- How will you train technology consultants on IPV 101, common types of technology abuse, and how to work with clients to mitigate technology abuse?
- What kind of support structures will you implement to better ensure a positive working environment for your technology consultants?
- Do you plan to evaluate your technology consultants?
- Will you implement a process for how technology consultants can resign from the position?

Notes:

Chapter 7: Conducting an Appointment

This chapter provides insight to the process of conducting appointments within technology abuse clinics, including approaches for how technology consultants interact with survivors during appointments. Questions to consider as you review this chapter include:

- What principles will guide how technology consultants work with survivors?
- What legal considerations do your technology consultants need to be aware of when working with survivors?
- How will technology consultants prepare for meeting with clients?
- Will your clinic provide a structure for how technology consultants conduct appointments?
- What follow up or post appointment options will your clinic offer?
- What personal safety protocols will your clinic incorporate regarding the consultant-client relationship?

Notes:

Chapter 8: Clinic IT and Protecting Clinic Data

This chapter considers data security practices for technology abuse clinics that emphasize safety and privacy practices for clients, staff, and the clinic itself. Questions to consider as you review this chapter include:

- What (personally identifiable) information about clients will you gather, how will it be stored, and for how long?
- Will technology consultants take notes during appointments, will these notes be maintained, and if so, how?
- How will technology consultants and clinic staff communicate with clients and each other?
- Who will have access to client data?
- Will your clinic share data externally, and if so, what safeguards will you put in place to ensure client privacy?

Notes:

Chapter 9: Helping with Technology Abuse

This chapter is an overview of technology principles that are relevant for navigating technology abuse. It discusses the core security concepts in the context of intimate partner violence, including categories of abuse and threat models. Questions to consider as you review this chapter include:

- What is the level of comfort with technology and security among the core staff of the clinic?
- Will the clinic rely on impermanent staff to provide security expertise?
- What types of technology abuse is the clinic best and least equipped to respond to?
- What strategies and practices will the clinic build to help sift through inaccurate or misleading information when helping clients research unfamiliar issues?
- Given the rapidly changing landscape of technology, how will the clinic incorporate continuing education practices to stay atop relevant information?

Notes:

Overview of a Technology Abuse Clinic

This chapter provides a broad introduction to technology abuse clinics, including essential features that comprise a technology abuse clinic, overarching principles that guide the design and management of a technology abuse clinic, and an overview of secondary initiatives that have emerged from existing technology abuse clinics.

While these secondary initiatives are not prerequisites for a technology abuse clinic, we introduce them here as stakeholders may want to consider such secondary initiatives during the planning phases of a new clinic.

Why Technology Abuse Clinics

Technology abuse is often poorly understood and multi-faceted, with individual survivors suffering from multiple types of technology-based harm (see Chapter 9: Helping with Technology Abuse). While many written guides and apps exist for addressing technology abuse, sifting through these resources to decide which are relevant and trustworthy is an insurmountable burden for many survivors and advocates.

Clinical approaches arose out of the observation that survivors benefit from human-mediated, 1:1 support with technology issues. Unlike other technology help services aimed at the general public, technology abuse clinics are tailored to the dynamics of coercive control and in providing trauma-informed services. Technology abuse clinics complement, but do not replace, other kinds of IPV resources, such as legal aid services, housing services, healthcare, and more.

Essential Features

A technology abuse clinic is a free consultative clinic that pairs technologists who are trained in the dynamics of coercive control with survivors experiencing technology abuse.

Technologists assist survivors with identifying possible points of compromise on their device(s) and developing technology-specific safety plans.

While there is no one technology abuse clinic model, we consider a technology abuse clinic to have three essential features.

A technology abuse clinic:

1. Communicates directly with the survivor-client, whether in person or remotely.
2. Offers one or more service(s) focused on providing redress for harms (potentially) incurred from technology abuse. Such services include but are not limited to: safety checks for devices and accounts, education, forensics, and expert testimony. (A clinic does not need to provide all of these services.)
3. Tailors services to the individual survivor with the intervention situated in their context of abuse.

The final feature is crucial, as it distinguishes a technology abuse clinic from the Apple 'Genius Bar' or other commercial tech helpdesk services. The above features are purposefully general, with the intention of fostering flexibility for the readers of this toolkit.

Subsequent chapters provide insight on options for stakeholders to consider when designing a clinic and deciding which services to offer and how to offer them.

Overarching Principles

A technology abuse clinic lies at the intersection of victim advocacy and technical rigor. We structure the toolkit around five overarching principles that should guide the design and practice of a technology abuse clinic.

These are applicable to any clinic design, regardless of which of the many variations that a technology abuse clinic may assume. We introduce these principles here, with more detail provided in later chapters:

Equitable - Strive to provide all survivors with *equal access* to the same *quality of service*. This requires considering the specific needs of survivors who are marginalized in some aspect of their (intersecting) identities, e.g., low-income, LGBTQ+, non-native English-speakers, etc.

- For example: Interpreter services (and responsible use) for non-native speakers, identity affirming practices, Internet access, accessible handouts, and written materials across education levels.

Collaborative - Establish clearly defined and productive working relationships with community partners. Technology abuse clinics are one of a constellation of support services that survivors might need. Defining and respecting the clinic's role in relation to other services within the constellation of community partners benefits the clinic, community partners, and survivors.

- For example: Role delineation, a referral practice for other services, agreements for information sharing and record keeping.

Community-centered - Account for the localized needs of the community that the technology abuse clinic will be serving.

- For example: Transportation access, lack of anonymity and privacy within geographic or cultural communities, local/municipal laws.

Trauma-informed - Account for the trauma that survivors may have experienced and make active efforts to avoid retraumatization.

- For example: Prioritizing the survivor's wishes, needs, and well-being in all interactions (rather than offering prescriptive advice) to allow for agency in how survivors wish to respond to technology abuse.

Technologically rigorous - Give clear, accurate information about technology. Avoid misleading explanations or inciting unnecessary fear or doubt surrounding technology. Do not shy away from ambiguity and encourage survivors to feel comfortable with and empowered by technology, rather than isolated from what is now a central part of modern life.

- For example: Normalizing self-education and explaining different levels of technical sophistication required for "hacking".

These five principles have helped guide the work of existing technology abuse clinics, and we encourage stakeholders to frequently consider these principles at each phase or iteration of developing and facilitating a clinic.

Secondary Initiatives

Existing technology abuse clinics have also pursued secondary initiatives in addition to offering direct services to clients. These secondary initiatives illustrate how technology abuse clinics can serve to address both individual and structural gaps related to technology abuse.

The secondary initiatives are informed by experiences gleaned from within the clinics, and serve to concretize and advance broader discussions about technology abuse in meaningful and impactful ways.

While the core services of technology abuse clinics center on the digital safety needs of individual survivors, these secondary initiatives seek to address systemic and structural issues related to technology abuse through research, education, training, and policy advocacy.

Research

The Clinic to End Tech Abuse (CETA), housed at Cornell Tech in New York City, and the TECC Clinic, located in Seattle and housed by a community-based domestic violence agency, each support distinct academic research efforts. This research is classified as work with human subjects, and researchers at both clinics maintain an Institutional Review Board (IRB) ethics approval.

Clients receiving services at either clinic may be asked for their consent to participate in data collection in service of these research efforts. However, at both clinics, survivors are informed that they will receive clinic services regardless of whether they agree to participate in research. Data gathered from these sessions have been used to analyze the efficacy of the clinics, identify common types of technology abuse scenarios, and inform development of protective tooling.

Education

Two existing clinics are affiliated with universities, the Clinic to End Tech Abuse (CETA) at Cornell Tech and the Madison Tech Clinic (MTC) at the University of Wisconsin-Madison. As part of their volunteer recruitment, both clinics recruit technologists from their respective computer and information science student populations.

Volunteering at a technology clinic is an opportunity for community-engaged learning where students can gain first-hand experience and learn necessary skills for mitigating and preventing harms from technology, particularly with at-risk populations. Students can also be engaged as volunteer technology consultants (see Chapter 6: Technology Consultants).

Technology Abuse Intervention and Prevention Training

Several existing clinics have found that it is common to receive requests for educational speaking engagements and/or to deliver trainings to enhance the knowledge of those who work professionally with or respond to survivors experiencing technology abuse (e.g.: victim advocates, law enforcement, legal attorneys).

For example, CETA regularly provides trainings for service providers, organizations, and victim advocates, while developers of the TECC Clinic have worked to standardize the integration of technology-specific safety planning into the core training provided to new victim advocates

Policy and Legal Advocacy

Both CETA and the TECC Clinic use data gathered from their experiences running a technology abuse clinic to inform legal and policy advocacy. Some examples of policy efforts include:

- State Senate Bill S2678 (2019-2020) which grants New York state residents the legal right to be released from a shared family phone or cable plan if they are experiencing IPV.
- The Safe Connections Act, a federal version of the New York State bill regarding the right to leave phone plans.
- Consulting with federal policymakers on legislation that would authorize funding for additional clinics
- House Bill 1320 (2021), a bill in Washington state to modernize, harmonize and improve the efficacy and accessibility of laws concerning civil protection orders, including updating the civil definition of domestic violence to include (technology-enabled) coercive control and to standardize a process for including digital evidence of technology abuse into the court record.

Agency Partnerships

This chapter discusses the importance of building and maintaining strong partnerships with already existing survivor support services and/or community partner agencies. The goal is to ensure that survivors who receive assistance from technology abuse clinics have access to comprehensive safety planning and a wide range of support services beyond the clinic.

We begin by explaining why agency partnerships are needed and some features of good partnerships, before detailing pragmatic advice for setting up an agency partnership. We then discuss managing client referrals to and from a clinic, as well as the importance of actively maintaining strong partnerships.

Why Is an Agency Partnership Needed?

As mentioned in Chapter 2, technology abuse clinics are only one of a constellation of support services that survivors might need. It is therefore important to ensure that technology abuse clinics are embedded within a broader ecosystem of support services and/or community partner agencies that can provide survivors with comprehensive support (e.g., legal, financial, shelter, etc.) and safety planning.

In addition, although technology consultants should receive training on how to provide basic counseling and technology-specific safety planning, they may not be comprehensively trained as professional survivor advocates. More broadly, it's unrealistic to expect that any single individual has all the expertise needed to help with all facets of survivors' complex situations.

It is therefore recommended that the role of technology consultants is limited to assisting survivors with technology abuse: partnering with survivor support services and/or community partner agencies ensures that mechanisms are in place to refer clients to other expert advocates and agency partners should the need arise.

Examples of Agency Partnerships

All the technology abuse clinics that form the basis for this guide have built strong partnerships with local agency partners, utilizing different partnership models.

For example, the TECC Clinic in Seattle is housed within and operated by a local domestic violence advocacy agency, New Beginnings, that provides survivors with comprehensive support services. Technology consultants meet with clients to help solely with technology abuse, and clients can receive other support services via the parent agency, including shelter, legal advocacy, and support groups.

As another example, CETA partners with New York City's Family Justice Centers (FJC), operated by the Mayor's Office as hubs that offer services from dozens of local partner agencies. The FJCs provide case management, economic empowerment, counseling, civil legal assistance, and criminal legal assistance, among other services. Survivors receiving services from any FJC partner agency can be referred to CETA for help with technology abuse.

Likewise, CETA's volunteer technologists can refer survivors to other services and agencies at the FJC. CETA has a similar partnership with the Anti-Violence Project, an anti-violence organization in New York City serving specifically the LGBTQ+ and HIV-affected communities.

Features of Successful Agency Partnerships

We anticipate that strong and productive partnerships between technology abuse clinics and partner agencies could take many forms. That said, we have found that successful partnerships often offer at least the following:

Complementary services - A technology abuse clinic is intended to complement, not replace, other support services. In existing clinics, partner agencies provide client intake, case management and general safety planning to complement the assistance offered by the technology abuse clinic.

Community-centered expertise - Partner agencies should be deeply embedded in the local communities they serve and offer tailored, context-specific advice. The services and support available to survivors may be highly dependent on the local context and will vary across state, country, and rural and urban locations. Partnering with agencies already embedded in local communities helps ensure that the technology abuse clinic can, in turn, learn from partners about how to tailor their services to specific situations and contexts.

Capacity and resources to sustain the partnership - Partner agencies should be enthusiastic about taking on the work of building strong partnerships with the technology abuse clinic, and be willing to invest the time and resources needed to sustain the partnership. For example, leaders from the partner agency may need to do extra work to set up referral mechanisms, while advocates from the partner agencies will need to spend time communicating with technology consultants about clients. To make this work worthwhile, efforts should be made to ensure that partnerships clearly benefit all parties: the technology abuse clinic, the partner agencies, and survivors.

Clearly defined roles and expectations - Technology abuse clinics and partner agencies benefit when their respective roles and expectations are clearly defined. Examples of predefined expectations may include: the clinic capacity (e.g., number of clients per month that may be referred to the clinic), expected response times, whether clinics can provide emergency services, whether volunteer technologists are on-call 24/7, and more. We recommend using a written memorandum of understanding (MOU) to ensure all parties are well-informed and agree in advance on the roles and expectations involved in the partnership. We provide some sample MOUs among our resources in the Appendix.

Setting Up Agency Partnerships

In setting up a technology abuse clinic, one of the earliest steps will likely be identifying potential agency partners. Many municipalities or counties have intimate partner violence survivor support organizations. One can ask people working in the IPV survivor support ecosystem about what agencies operate in an area, or even simply search online.

Of course, it may be easier to contact potential partners by gaining introductions from existing contacts or relationships with relevant/adjacent organizations. If no such relationships exist, there may be opportunities to get involved via community-based activities or events, e.g., participating in local task forces, attending community meetings, or volunteering with organizations. As a last resort, one might cold call or email potential agency partners to discuss your plans and gauge interest.

Before reaching out to potential partners, it's good to already have one or more potential clinic service modes in mind (see Chapter 4: Service Delivery Models). Most survivor support agencies will not need convincing that technology abuse is a problem for their clients, but it is good to be prepared to briefly review the motivation for a technology abuse clinic and clarify with agency representatives about the types of technology abuse they see within the community they serve.

Agency representatives may be skeptical about whether non-IPV professionals are suitably prepared to work with clients. This cautiousness is a healthy check on entering into new partnerships, as even well-intended individuals who lack proper training may cause serious harm to survivors. It also emanates in part out of a painful history of ill-informed technologists hawking “solutions” that fail to sufficiently account for the complexity of IPV, potentially causing harm.

To build trust, we recommend directly addressing the issue via your service model and training plan, which should explicitly recognize and have plans to manage the expertise and experience gaps between the envisioned technology consultants and agency partners. In addition, it will likely take substantial time investment and ongoing work to build the levels of trust needed to sustain a successful partnership.

Technology abuse clinics are unlikely to succeed without understanding that the clinic’s leadership needs to learn from agency partners and adapt their clinic plans to ensure they fit into the survivor support ecosystem.

That means that the new technology abuse clinic should complement existing services (to fill a widely acknowledged technology support service gap), avoid usurping resources used by other important services (e.g., housing, counseling, legal advocacy, etc.), and by developing strong collaborative working relationships.

Managing Client Referrals

After setting up an agency partnership and agreeing on roles and expectations, the next step is to create and manage mechanisms for referring survivors to the technology abuse clinic. These should be designed with respect to your clinic’s service delivery model, which usually will be tailored based on feedback from agency partners.

For most service models, technology abuse clinics will need to work with partner agencies to (1) advertise the clinic’s services, (2) receive client referrals from partner agencies, and (3) make client referrals for other services.

Advertising Clinic Services

It is important to ensure that partner agency staff know about the technology abuse clinic and how to refer their clients for services. Advertising can be done via presentations at partner agency staff meetings, circulating (e.g., via email) handouts and instructions for making referrals, etc.

Due to partner agency staff turnover, we recommend frequent, periodic advertising and communications to ensure that new agency staff quickly learn about the technology abuse clinic and how to make client referrals.

Receiving Client Referrals

In existing service models, survivors are already receiving services from an advocate at a partner agency and, in the course of receiving these services, clients mention or discuss their concerns regarding technology abuse. The advocate at the partner agency will then make a referral for the client to the technology abuse clinic or share contact information for the technology abuse clinic with the survivor, who then initiates contact directly.

Existing technology abuse clinics have used a variety of mechanisms for receiving client referrals from partner agencies. For example, the TECC Clinic offers services on specific days. The survivor calls the partner agency that manages the clinic, an advocate completes the intake process with the survivor and then the advocate schedules the survivor to meet with a technology consultant on a dedicated clinic day.

As another example, in CETA's current referral model, clients (often with assistance from an advocate) complete CETA's online referral intake form (see sample Intake Forms in Appendix). Submission of the intake form triggers an alert for CETA leadership who, after reviewing the information provided on the form, assign a technology consultant to the client's case. The technology consultant then contacts the client to schedule services.

Client referral mechanisms could take many forms. Whatever the mechanism chosen, it is important to ensure that all client referrals are attended to in a timely manner, that clinic capacity constraints are respected, and that next steps and expected response times are clearly communicated to clients and advocates.

Referring Clients to Other Services

Technology consultants who work with clients within the technology abuse clinic may often encounter situations that call for other types of support services. For example, clients who want to document evidence of technology abuse for use in court may need legal advice, clients who discover financial abuse or fraud may need economic assistance, and clients who have experienced trauma may need counseling/therapeutic services.

To accommodate clients' diverse needs, technology abuse clinics and agency partners should create an agreed upon plan that enables technology consultants to refer clients to services outside of the clinic. This might involve, for example, creating a standardized referral sheet that the technology consultant and/or survivor fill out. Any process for how a technology consultant assists survivors with referrals for services outside of the clinic should be incorporated into the technology consultants' training.

At CETA, for example, referrals for services outside of the clinic are facilitated via communication (e.g., phone calls or emails) between the technology consultant and the client's advocate at the partner agency. Typically, these communications require the client's consent to share information with their advocate. By contrast, TECC Clinic technology consultants do not directly coordinate follow up referral services, but instead encourage the survivor to connect back with their advocate for referrals.

Maintaining Partnerships

Maintaining strong and productive partnerships requires ongoing work and clear communication between partner agency and technology abuse clinic leadership. Several mechanisms that we have found useful in this regard include:

Open lines of communication - It is essential that partner agency and technology abuse clinic leadership are responsive to each other's communications and empowered to provide honest, critical feedback, especially for matters related to survivor, staff, and technology consultant safety.

Regular check-ins - Partner agency and technology abuse clinic leadership should schedule regular (e.g., quarterly) meetings to discuss progress, raise issues, ensure a space to ask/answer questions, and seek feedback regarding service delivery.

Structured feedback activities - Implementing formal feedback opportunities, such as surveys or interviews, with partner agency staff and/or technology consultants assists with assessing experiences with the technology abuse clinic and standardizing this feedback practice can improve communication and service delivery.

Service Delivery Models

A service delivery model refers broadly to how a clinic operates, including connecting to clients, interfaces with other kinds of support services, client case lifecycles, the types of services the clinic offers, and how technology consultants communicate with clients.

A service delivery model encompasses both literal means of connection (in-person/remote, scheduled/drop-ins), but also includes other aspects of care, such as the length of care and types of services offered.

In this chapter, we define and discuss the following aspects of a service delivery model:

- Care models
- Scope of services
- Referrals
- Intake, screening, and triage
- How to meet with clients

Our own service delivery models have undergone many iterations. Some changes to our models emerged due to uncontrollable circumstances (e.g., the remote-only demands of the COVID-19 pandemic), while others evolved in response to changing capacities or client needs. We share service models used in existing clinics to ground this discussion in examples. However, we recognize that there is no single 'best' service delivery model, and that the models used in existing clinics are likely to see future improvements.

In the following, we start by discussing how clinics should decide on a care model and scope of services, which inform the rest of the service model. Then we discuss other aspects of service delivery, starting with possible ways to handle referrals, followed by intake, screening, and triage, and finally scheduling and appointment medium.

Care Models

Clinics may want to consider how they handle requests for multiple appointments or long-term care. If the clinic would like to provide continuity of care between appointments by, e.g., pairing the client with the same consultant or building off of information stored in past appointments, it will need to also consider what information to store about past appointments and how to store it safely (see Chapter 8: Clinic IT and Protecting Clinic Data)

- **Drop-in appointments:** Technology consultants work with a client in some time-bounded appointment (minutes to hours); all client-consultant interactions occur within this appointment.
- **Short-term cases:** Technology consultants meet with a client multiple times over the course of a relatively short period of time (days to a month).
- **Long-term cases:** Clients are helped over a longer period (weeks to months) by the clinic, either via the same consultant assigned to the client or a collection of consultants.

Different approaches have different trade-offs. Supporting longer term care may increase the amount of work for each consultant per client, and this may reduce client capacity of the clinic overall.

Moreover, long-term care necessitates more infrastructure to manage personally identifiable information, case notes, and more. On the other hand, drop-in care may be insufficient for some complex client problems.

In our experience a lot can be done for clients via drop-in appointments, and it may be the best starting point for new clinics as it is the least complicated to set up. CETA started with drop-in care, and subsequently expanded to include short- and long-term care approaches. The TECC Clinic remains a drop-in care service. Hybrid models in which drop-in or short-term care services are the standard but more complex cases are escalated to a reserved team for longer care have not yet been explored, but may offer a balance between the shortcomings of each.

Scope of Services

Technology abuse can take many forms, and possible interventions to mitigate different types of abuse may require drastically different involvement by technology consultants. It is important for technology consultants to know beforehand what services they are expected to render and how to communicate service limitations to clients, who may ask for services that consultants are unable to provide.

As an example, a narrow service model might limit service to checking the configuration settings for accounts and devices. Even this narrow model can cover a daunting number of accounts: email, social media, iCloud and other cloud storage, phones, laptops, tablets, financial accounts, WiFi routers and modems, and Internet of Things (IoT) all fall under the category of accounts and devices, and may run different operating systems (Windows, Android, MacOS, iOS, Linux). Further scoping of this model may pre-define which devices and accounts the clinic is able to handle.

Other service models might require technology consultants to guide clients through issuing take-down requests for publicly posted information or online harassment, requests for forensics and analyzing user data, physically searching for tracking/audio devices, or digitally scanning devices for unwanted software. The scope of these services would likely be incompatible with all but long-term care models.

It's also important to consider setting boundaries on what clinics can help with. Below, we share how CETA and TECC scope their services.

CETA and the TECC Clinic: As a hard rule, neither CETA nor the TECC Clinic do home visits or vehicle scans, although we may provide instructions or advice on how clients can do this for themselves. The clinics primarily check account and device configurations, and this is typically what clients request. However, clients can share any technology-related issue, and technology consultants will do their best to provide assistance, if possible. Certain issues such as harassment, non-consensual intimate imagery (NCII or 'revenge porn'), and forensics are beyond our (and as far as we know, any technologists') ability to meaningfully help with, so technology consultants are instructed to set expectations with clients asking for help with these issues, and then direct them to whichever relevant resources of which we are aware.

Referrals

A crucial consideration for any clinic is thinking through the mechanisms by which potential clients can request service. In an advocate-driven approach, an advocate at an IPV agency is the first point of contact for the survivor. The advocate conducts an intake with the client for their agency. As part of this intake, they might determine whether a referral to the technology abuse clinic is warranted and, if so, follow instructions mutually agreed upon by the agency and the clinic to refer the survivor to the clinic.

This approach ensures that all clients seen by the technology abuse clinic are already supported by a professional IPV advocate who is trained in topics such as how to conduct **risk assessment** and **safety planning**.

In an advocate-driven approach, the technology clinic needs to decide which IPV agencies can make referrals. In areas where there are many different anti-violence service providers, technology abuse clinics might consider exclusively partnering with a single agency or, if one exists, a coalition representing a collection of existing agencies, with all other agencies going through this partner agency for referrals.

This has the advantage of having one organization act as a central clearinghouse for referrals, which can streamline the intake process for the clinic, but might be frustrating for service providers who do not have a direct line for services.

CETA: *CETA only accepts referrals from partner agencies within the New York City Metropolitan area. Its major partner is the Family Justice Centers run by the NYC Mayor's Office; the FJCs act as a central clearing house that streamlines referrals for the many domestic violence agencies operating in New York. As of 2022, CETA also accepts referrals directly from the Anti-Violence Project, an LGBTQ+ and HIV-affected serving agency in New York.*

Alternatively, a *self-referral* model allows survivors to contact the clinic directly and request services. This has the potential advantage of reaching more survivors and lowering the barrier for access, particularly in communities where there is a waitlist for advocacy services.

However, the self-referral model can introduce other challenges. A self-referral model requires dedicated resources and staffing to field incoming requests and will require a robust intake/screening process (see below). Additionally, survivors might attend the clinic without having already engaged in individualized safety-planning conversations with an advocate, and might leave the clinic without sufficient advocacy support needed for follow up conversations — including additional safety planning related to the technology issues uncovered during the clinic session. The self-referral model may also require a more public advertising scheme, which again may reduce barriers to access, but might also result in people seeking services who do not fit the clinic's criteria (e.g., people with a technology question who are not IPV survivors or even abusers seeking to misuse the clinics services).

TECC Clinic: *As of 2022, the TECC Clinic utilizes a self-referral model on a first-come, first-served basis. In previous iterations, the clinic experienced a high no-show rate that staff attributed to the delays between survivors completing an intake, being referred to the clinic by their advocate, and receiving an appointment time. The self-referral model has reduced the number of scheduling calls that the survivor receives, and the TECC Clinic is now experiencing a lower no-show rate. In practice, most clients are working with an advocate before attending the clinic, which is how they learn about the service, but the client initiates contact with the clinic directly. Future screening may harden the requirement that clients have an advocate before attending the clinic.*

Intake, Screening, and Triage

Regardless of the model by which clients request services, clinics will need to internally review incoming requests to collect basic information about the client and their needs, and to ensure that the survivor is requesting services that are appropriate for the clinic's expertise.

There are different methods for gathering this information. For example, clinics may use an online form (powered by, e.g., Google Forms or Qualtrics) that the client and/or their case worker fill out that triggers a request for service, or intakes may occur over the phone between the survivor and a contact person at the technology abuse clinic.

The information included on an intake form may vary depending on specific aspects of the service model. For example, if technology consultants contact clients directly for scheduling, the intake form will need the client's name (or a pseudonym) and contact information.

In addition, depending on the volume of requests and clinic capacity, there may also be a need to triage requests for services, rather than following a first-come, first-serve model. If the request is urgent or time-sensitive (e.g. the client is moving into a shelter or has an upcoming court date), the clinic may consider prioritizing those clients for services and include such variables on the intake form.

We encourage all technology clinics to carefully design their intake forms to ensure that they follow the principles of data minimization (i.e., only request information that is necessary for providing service), plain language, and inclusivity (see sample Intake forms in the Appendix).

CETA: *CETA maintains an intake form created in Qualtrics. The intake form may be filled out by the client directly, by a caseworker on behalf of the client, or by both together. CETA's intake does not gather information about the abuser. Most fields are optional (including the clients name, pronouns, and any demographic information) but it does require contact information for the caseworker and safe methods (call, text, voicemail, email) and times to contact the client.*

TECC Clinic: *With its current self-referral model, the TECC Clinic Coordinator completes the intake directly with the survivor. In addition to gathering information about the survivor's current technology concerns and the devices that the survivor would like to discuss, the intake also explores potential conflicts of interest by gathering minimal information about the abuser, including whether the abuser is employed in the technology industry. Because the Seattle region is a hub for technology companies and many of the clinic's technology consultants are employed in the technology industry, the intake process specifically aims to ensure that the survivor is not paired with a technology consultant who may be a colleague of the abuser.*

Scheduling

Scheduling practices determine how to arrange a time for clients to meet with technology consultants. Regardless of the order clients are seen in (prioritized, first-come first-served), there is a need to pair them with a technology consultant. Potential models include:

Drop-in services: The clinic advertises open hours during specific days and times, and clients are informed of those hours. During that time, any client seeking service contacts the clinic and is connected to an available technology consultant.

Appointment slots: Similar to drop-in services, the clinic advertises a list of available appointment slots to advocates or clients. Then clients or their advocates reserve an available appointment slot.

Client-driven scheduling: The clinic or technology consultant contacts the client directly (e.g., via phone or email) to arrange a mutually convenient time to conduct an appointment.

Our experiences at existing clinics have yielded two consistent insights. First, scheduling affects no-show rates, and no-show rates can sometimes be large (e.g., 50%). In any model, and especially in IPV contexts, clients will sometimes not show up for an appointment. Scheduling practices may elect to take this into account by, for example, offering to take drop-in clients if a client with an appointment does not show up.

Second, scheduling can be burdensome for clients, technology consultants, and advocates. Small changes to scheduling models can have outsized impact on how much work is needed to schedule an appointment and by whom that work is done.

TECC Clinic: The TECC Clinic operates on a consistent schedule in which appointments occur on the first and third Monday of each month during a two-hour block in the evenings. This offers consistency for the technology consultants who sign up for shifts upwards of two months in advance. The TECC Clinic Coordinator connects with survivors the day of the appointment to complete the intake where they also discuss safe email options for receiving the Zoom link to access the appointment. The short time between intake, scheduling and the appointment has assisted in reducing ‘no shows’. If there are more referrals than available appointments, the TECC Clinic Coordinator also schedules waitlist appointments, where a survivor waits in the Zoom waiting room and if a survivor with a scheduled appointment does not show, the survivor in the waiting room receives the appointment.

CETA: *Scheduling at CETA has gone through several iterations; during the in-person only (pre-Covid) era of CETA, the clinic offered 4-5 slots on a single day each month per location, and advocates booked clients into those slots. If clients did not show up, then walk-ins were able to take their spot. In its current iteration that requires a remote appointment first, CETA consultants schedule the appointment directly with the client via the contact information provided in the intake; we experience a no-show rate of about 20-30% using this approach.*

Medium of Appointments

Most service delivery models include scheduled appointments with a client. These appointments can be in-person or remote. Below, we explore benefits and challenges of each medium.

In-person appointments: In an in-person session, the technology consultant and client meet in a safe, physical location. This is usually provided by the partner agency.

Benefits of in-person sessions:

- Technology consultants can assist with navigating unfamiliar settings or devices
- Depending on the location of the clinic, on-site advocates may also be available for immediate follow-up support

Challenges of in-person sessions:

- Difficulties in arranging transportation, child care, or other scheduling difficulties for some clients, often contributing to higher no-show rates
- Higher time commitments for technology consultants which may contribute to difficulty staffing sessions
- Finding a safe space to utilize, especially if client is concerned about location-tracking

Remote or virtual session: In remote or virtual appointments, the technology consultant and client communicate without meeting in person. Remote assistance can occur through synchronous meetings such as speaking over the phone or through teleconferencing software with potential for video and/or screen sharing, or asynchronously, such as providing assistance over email or text message, either directly to the client or through an intermediary, such as a caseworker.

Benefits of remote/virtual sessions:

- Increased accessibility and flexibility for both clients and technology consultants
- Fewer safety concerns when client is concerned about or at-risk of location tracking
- Clients may experience a great sense of agency and empowerment by learning to navigate their devices and accounts in real-time, rather than being tempted to hand over their devices.

Challenges of remote sessions:

- Clients may only have one device, and struggle to use it both to access the session while following the instructions provided by the technology consultant.
- There may be concerns about the safety of the device or security of the connection.
 - A workaround is for the client to go to a safe physical location, such as the partner agency or a friend/family member's house, and participate in the remote session using a device belonging to the agency or friend.
- There is unlikely to be an advocate in attendance unless arranged before hand.
- Sessions may take longer, especially if technology consultants cannot see the clients device. Consequently, some clients may find the inability to hand over their devices more frustrating than empowering.

A hybrid model offers the opportunity for both or either virtual and in-person meetings, with the type of appointment defined by other aspects of the service model and the client's needs. In either type of session, technology consultants can maintain communication with their fellow consultants to collaboratively problem-solve during individual sessions over an instant messaging or email platform, but this may be easier during remote appointments.

CETA and the TECC Clinic: Both CETA and the TECC Clinic started by offering exclusively in-person services, meeting with clients at the physical location of their partner agencies. During the COVID-19 pandemic, both clinics then moved to entirely remote services.

At the time of writing, CETA currently offers a hybrid model in which appointments are remote by default, but clients may request an in-person meeting. Remote appointments are conducted using either a web-based teleservice (RingCentral) or Zoom with dial-out capabilities (see Chapter 7: Conducting an Appointment). We are also able to provide asynchronous, remote assistance via email and text, directly to clients or through caseworkers.

By contrast, the TECC Clinic remains fully virtual, with clients and technology consultants meeting on Zoom. Zoom was chosen because it became the go-to platform during the COVID-19 pandemic for advocacy agencies in the region to provide services to survivors and for survivors to access the court system for Protection Order hearings. In other words, the platform was familiar to many survivors and could be accessed without a separate download or need to create a login or account.

Staff and Personnel

This chapter introduces key personnel roles for staffing a technology abuse clinic, along with useful traits and qualifications for personnel, and important considerations for staff management.

The following topics are covered:

- What personnel are recommended for a tech clinic?
- What are desirable traits for clinic staff?
- How might one manage the mental health and morale of clinic staff?

The content in this chapter applies equally to 'leadership' (management-type) personnel and technology consultants who may be paid staff or volunteers.

Recommended Personnel

The role descriptions provided below map onto key tasks that support the management of a technology abuse clinic. How these responsibilities are distributed across personnel will depend on the clinic's organizational structure, including how or if each position is funded.

For example, it is possible that the same person who takes on the responsibilities of the *Technology Staff Manager* also fulfills the role of *Referral Coordinator* and/or the *Digital Abuse Specialist*. However, in this section we discuss each role individually to illustrate the unique skill set and time commitments associated with each.

Referral Coordinator(s)

A referral coordinator is a staff member at the IPV partner agency who serves as an intermediary between technology consultants, IPV advocates, and clients. This includes soliciting and directing referrals for clients experiencing digital abuse and coordinating between technology consultants and other specialized care services, (e.g. a technology consultant documenting evidence of digital abuse and a legal advocate pursuing an order of protection.) Within currently existing technology abuse clinics, this role has been filled by a staff member of an IPV agency who takes on this role as part of their regular job responsibilities.

Technology Staff Manager

The technology staff manager is responsible for managing the recruitment, training, and ongoing support of technology consultants. Crucially, if the technology staff manager is not the same person as the referral coordinator, then the technology staff manager should ensure that referrals for incoming clients are staffed appropriately by technology consultants.

This includes ensuring there are no conflicts of interest between the technology consultant and their assigned clients (e.g., close personal or professional relationship), and coordinating individual client accommodations, such as translation services, a safe meeting space, agreeable meeting times, or unreachability due to incorrect or out-of-date contact information.

Technology Consultants

Technology consultants work directly with clients to guide them in navigating their technology security. Because of their frontline role, we dedicate an entire chapter to practices around recruiting, training, and sustaining technology consultants (see Chapter 6: Technology Consultants). Here, as with all staff members, we simply invite the readers of this toolkit to consider whether technology consultants would be unpaid volunteers, as they currently are in existing clinics, or if they would be part/full-time paid staff.

Digital Abuse Specialist (Optional)

A digital abuse specialist refers to someone with expert knowledge of technology security, particularly in IPV contexts. This role serves as someone who can (1) act as a primary consultant for complex forms of digital abuse, and (2) facilitate on-going training with IPV advocates and/or technology consultants to enhance baseline knowledge of technology-specific safety planning.

The need for this role is situationally dependent. At CETA and MTC, which are both housed at universities with large computer science departments, this expertise is built into the structure of the clinics as the clinics are directed by digital abuse specialists. At the TECC Clinic, technology consultants are largely recruited from Seattle's technology hub and receive IPV training that complements their technology security knowledge. Over the years of volunteering, technology consultants from the TECC Clinic have gone on to become digital abuse specialists.

We label this specific position as optional because a clinic that includes a strong knowledge base of technology security and IPV among its various partners and stakeholders can work collaboratively to fulfill the role description.

Traits and Qualifications

Technology abuse clinics bridge the worlds of survivor advocacy and technology literacy. Since it may be challenging or unlikely for individuals to possess extensive background in both advocacy and computer security, we recommend that potential candidates be *trainable* in areas in which they lack experience.

In this section, we discuss several traits or qualifications to look for in all staff roles (not just technology consultants, for which we separately provide an interview guide and rubric in Chapter 6: Technology Consultants) and potential ways to evaluate them:

Empathy, empowerment, and temperament

Empathy, or the ability to inhabit another person's worldview, informs all aspects of how a clinic is run. This is not just limited to survivors as working in spaces permeated by the effects of interpersonal violence is taxing for all involved, including staff.

While it is always welcome to have coworkers who are understanding, patient, and compassionate, these traits are especially important in clinic settings for team morale and mental health (see below). It is important to carefully consider the temperament of those invited into the clinic space and how it will affect the overall dynamic.

Appreciation for the complexities of IPV

Good candidates should demonstrate an appreciation for the complexities of IPV and be open-minded about learning how to adopt trauma-informed, client-centered practices.

This means that candidates should not minimize the dangers faced by IPV survivors, exhibit victim blaming tendencies, or otherwise identify with abusers. This also means displaying humility about their (and others') ability to easily solve survivors' problems, and acknowledging the responsibility they take on when working with clients.

Appreciation for the complexities of digital security

Although a technology abuse clinic does not require a team of computer security and privacy experts, the stakes of digital privacy are high. All technology clinic staff members ought to take technical rigor seriously, both when structuring advice to clients and when structuring internal practices (see Chapter 8: Clinic IT and Protecting Clinic Data).

Good candidates should be willing to put in the work required to learn best practices and stay educated on emerging technology trends that affect the information distributed to survivor, especially with the mindset of supporting survivors continued use of technology (e.g., not defaulting to suggesting to just "get off social media").

Further, good candidates should be willing to develop and adhere to a data security plan that protects the private information of clients interacting with the clinic. This requires skills such as a baseline level of technology literacy, responsible personal digital security practices (e.g., using strong passwords, second-factor authentication), comfort with new technologies and tools, and ability to do independent research on emerging technology problems.

Morale and Mental Health

Finally, the morale and mental health of all clinic staff deserves consideration. Working with survivors of abuse and trauma can result in secondary trauma, defined by the US Dept of Health & Human Services as *the emotional duress that results when an individual hears about the firsthand trauma experiences of another*.

This phenomenon is well-documented and known in therapeutic and social work circles, but it may be a new concept for many who are interested in a technology abuse clinic.

While indicators of secondary trauma may present differently for different individuals, shared signs range from feeling numb, to feeling guilty, to feeling a lack of empathy, to feeling hypervigilant, cynical, and/or chronically exhausted.

Importantly, the degree to which exposure to someone else's trauma affects an individual is unequal, and alters and intensifies in relation to institutional and systemic oppressions like racism, (hetero)sexism, xenophobia, ableism, and classism.

Being mindful of and actively working to reduce the effects of secondary trauma are important not only for the well-being of clinic staff, but also for clients as clinic staff who experience secondary trauma can experience a reduced capacity to care for survivors, including unintentionally causing direct harm.

Incorporating an active practice to help reduce secondary trauma is important to remain effective in direct service work with survivors over time

We offer the following recommendations based on our experiences, some of which are more specific to the work of a technology abuse clinic than others:

- Offer flexibility in hours and time off
- Be mindful of (over)scheduling technology consultants
- Offer mental health care as part of insurance, if possible
- Create structured and unstructured opportunities for sharing/debriefing after client appointments
- Work to create a healthy and supportive team; the group dynamic and being comfortable with each other has important consequences for mental health
- Normalize discussions of mental health and create space for disclosures of common signs of secondary trauma
- Work to minimize the trauma encountered outside of client appointments (e.g.: reading material before falling asleep, doom scrolling, images consumed on television)

Technology Consultants

Technology consultants form the core of a technology abuse clinic. They communicate with clients, guiding them through technology safety checks, providing education and resources, and acting as the face of the clinic.

This chapter thus provides additional details around supporting and training these key staff, including:

- Differences in volunteer vs paid technology consultants
- Recruiting and screening technology consultants
- Training and evaluating technology consultants
- Supporting technology consultants
- Leaving the technology abuse clinic

Volunteer vs. Paid Technology Consultants

Existing clinics have primarily utilized a model in which most technology consultants are unpaid volunteers. As such, technology consultants have professional and personal lives outside of the clinic, and are asked to devote approximately 10 hours (CETA) or 2 sessions (TECC Clinic) a month to the clinic.

Whether or not technology consultants are compensated may have a large impact on setting reasonable expectations and workloads. Expecting volunteers to perform at a level comparable to a paid job is likely to result in frustration and disappointment. (For reference, we find that paid part-time consultants can serve roughly 3-5X more clients than volunteer staff).

Volunteers may need to take extended breaks due to vacation or work (encouraged as part of self-care), may need more reminders about procedures and training than one would expect from a paid staff member, and may be more likely to neglect clinic-related duties if there is a conflict between volunteering and their professional or personal lives.

Volunteer consultants also lack natural enforcement mechanisms; there are no consequences for volunteers who renege on their volunteering commitment, other than removing them from the clinic team. However, the lack of consequences should not be confused with an inability to establish mechanisms for *accountability* or *support* (see below), regardless of whether technology consultants are paid or not.

Recruiting Technology Consultants

Any clinic will need need to recruit technology consultants. We have found casting a wide net to yield a well-rounded pool of technology consultants to be most effective. By this we mean aiming to recruit, for example, technologists that require IPV training, as well as IPV advocates who may need technology training.

Important considerations to consider when recruiting include whether your clinic will offer in-person services, requiring consultants to be physically located in the same locale as the clinic, or if services will be offered remotely and consultants may be geographically distributed. Potential avenues for soliciting applicant technology consultants might include:

Leveraging personal and professional networks: Word-of-mouth can effectively attract potential applicants. Particularly in the early stages of setting up a clinic, tapping these networks may help reduce the need for screening. Recruits who have personal or professional affiliation with the clinic are also more likely to be patient with the unforeseen obstacles endemic to the early stages of any new organization. However, relying solely on personal or professional networks risks reinforcing the inherent biases of these networks into who is represented in the clinic staff.

Interest groups and topical newsletters: Consider reaching out to local organizations with a mission that is related to the social impact of technology and/or organizations dedicated to anti-violence, gender equity, diversifying technology and computer science, or community and neighborhood interest groups.

Local colleges, tech companies, and related professional organizations: Similar to above, programs in computer, data, or information science, social work, community health, and companies that hire those in these areas may have interested candidates.

The web and social media networks: Consider creating a website or social media accounts for your clinic and posting an open call for volunteers. You can also ask organizations with larger online followings to boost your call for applications.

Receiving and Screening Applications

Consider what applicant materials to collect in order to facilitate screening and evaluation of potential technology consultants. Existing clinics, for example, have asked applicants to submit a CV, statement of interest, contact information for 2-3 references, and additional demographic and/or location data (see sample Application Forms in the Appendix). If a clinic works with minors (under 18 years old), then some background checks for history of child abuse or other problems may be requisite.

After receiving applications, the next step is reviewing applicants and evaluating their potential to become effective technology consultants. In addition to carefully reading provided applicant materials, we recommend conducting at least one face-to-face (virtual or in-person) interview to gauge an applicant's communication skills.

While it is impossible during the early stages of any recruitment process to have perfect accuracy in assessing an individual candidate's potential, below we suggest traits that we have seen in successful technology consultants and what to look for when screening and/or evaluating candidates, either by reviewing application materials or during an interview.

Communication Skills: Technology consultants will need to explain technical concepts to people who have a range of technical literacy and/or varying language capacities. Prior experience teaching or explaining technical concepts to others will likely be an asset (e.g., tutoring experience, IT helpdesk, helping family members).

Resilience and Composure: Applicants may not realize that survivors will often share stories of abuse or become emotional during sessions. Prior experience working with traumatized populations or in sensitive settings (e.g., EMT, counseling, other social or aid work) will be advantageous. Moreover, we have found that many people who are interested in working at a clinic are themselves IPV survivors, which may add additional dynamics or potential triggers in discussions of abuse.

Empathy and Trauma-Consciousness: All consultants should receive training in trauma-informed care during the clinic training, so it can be okay if they have misconceptions during the screening and interview stage. That said, applicants should demonstrate some level of intuitive empathy towards others, which might be gauged by asking, for example, what they would do if someone started crying or became emotional during a conversation (e.g., a reasonable answer would be "I would want to give them space and help them feel calm, but would want training for what to do").

Adaptability and Problem Solving: Successful technology consultants will be comfortable with uncertainty or dealing with "gray areas" that often arise when working with survivors. They will also need to be able to creatively problem solve and suggest options that meet survivors' individual needs and address specific technology problems.

Technology Literacy: Finally, while technology consultants do not need to be technology experts, they should feel comfortable learning about or navigating new platforms and be able to confidently learn new technology concepts.

We include as resources in the Appendix sample interview guides and rubrics that detail how existing clinics have assessed these traits in evaluating candidates.

Training and Evaluation

After screening and interviews, accepted applicants will need to undergo training. Training should cover the fundamentals of IPV, advocacy, and technology abuse mitigation. One approach for training technology consultants is to outsource general IPV and advocacy training to a partner agency with qualified trainers.

Alternatively, existing clinics (TECC Clinic) have technology consultants go through the same staff/advocate training that the host partner agency requires all its advocates to complete. Another approach is to create in-house trainings, with IPV trainings facilitated by an experienced IPV advocate, and technology abuse trainings led by a technology abuse expert.

Regardless of how trainers are sourced, we recommend technology consultants are trained, at a minimum, in the following topics:

- Introduction to IPV (aka IPV 101)
- Secondary trauma and self-care
- Skills and approaches for communicating with clients
- Common types of technology abuse and how to discover and mitigate it.'

We provide as a resources an outline of the training program used by an existing clinic (see Appendix).

We strongly encourage combining a variety of training modalities, especially learning via role-play activities or shadowing, which offer unique opportunities to evaluate how other technology consultants approach interactions with survivors.

As examples, existing clinics have utilized combinations of the following training modalities:

Lecture-based training: Trainers deliver presentations to provide trainees with background on advocacy and technology abuse. This may include the review of written materials and resources.

Scenario-based exercises: Trainees receive hypothetical client case briefs to review and discuss in small groups or among the training cohort.

Role-playing activities: Trainees are asked to play the role of a technology consultant and/or the role of a client. Trainees are given a sample role-playing activity that includes a consultation scenario along with scaffolds detailing a hypothetical client situation and possible reactions.

Listening to recordings of client consultations from previous technology abuse clinic sessions: Clients should have consented to both the recording and the recording being used for training purposes.

Field training: CETA uses an approach in which trainees first passively shadow more experienced technology consultants for a few appointments. They then graduate to a more active technology consultant role, but are still teamed up with more experienced “case leads”. Then they graduate to become case leads, handle client cases on their own, and help train future technology consultants.

Supporting Technology Consultants

Providing technology consultants with sufficient support is crucial for the safety of both consultants and clients, and for the overall health of the clinic. Technology consultants have often sought opportunities to work in a technology abuse clinic out of a sense of altruism and sincerely want to help survivors; creating a rewarding and positive environment and building a supportive community will nurture this impulse. Examples of support that may be provided include:

Self-care structurally embedded into the clinic

- Regular check-ins with supervisory clinic staff
- Organized opportunities for debrief (e.g., post-appointment chats)
- Unorganized opportunities for debrief (e.g., social events)
- Caps on client work to encourage time off
- Standardizing practices that protect boundaries around consultant's time

Physical safety

- Secure, safe place to conduct in-person appointments
- Dedicated communication lines for any communication with clients
- Use of pseudonyms in client appointments, if desired, and respect for those pseudonyms.

Supplementary Training

- Continued education (e.g. seminars, guest speakers, resources for other trainings, refreshers on existing topics).
- In-appointment resources, such as step-by-step guides, etc.

Accountability (for the consultant and clinic)

- Individualized feedback
- Transparency about clinic operations
- Opportunities to provide anonymous critical feedback
- Encouraging at least two consultants per appointment, if possible
- Checking in with individual consultants about each client they've seen.

We also recommend delivering support via multiple modalities and providing alternative ways for technology consultants to participate in clinic meetings and events. This is especially important if technology consultants are volunteers (and hence have other professional commitments) and/or are geographically distributed.

Useful mechanisms we have used to ensure technology consultants are supported include:

- Writing down and documenting policies in an easily accessible format (CETA maintains a technology consultant handbook for this purpose)
- Recording trainings for those who cannot attend
- Embedding links to procedural checklists (e.g. links to training documents embedded into case management software)
- Providing extra reminders of procedures and best practices
- Providing alternatives for those who cannot make activities (e.g., CETA sends out a newsletter for those who can't make team meetings)

Leaving the Technology Abuse Clinic

It is natural for technology consultants to eventually stop working with the technology abuse clinic. Indeed, IPV advocacy organizations commonly experience relatively high rates of staff turnover. Attrition may also be relatively high if technology consultants are donating their time as unpaid volunteers.

We recommend that technology abuse clinics build in processes that enable the graceful exit of technology consultants from the clinic. This may include creating and communicating to technology consultants the process for resigning from the clinic (e.g., who they should notify and any required notice period).

Clinic leadership will need to reassign any active client cases the departing consultant is working on and inform any affected clinic staff (e.g., Technology Staff Manager). If possible and appropriate, we also suggest creating mechanisms that celebrate the contributions of departing team members, thanking them for their service, and providing others with opportunities to show their appreciation and gratitude for the consultant's work.

Finally, we note that the rate of attrition of technology consultants (and the number of clients requiring service) will impact how often the technology abuse clinic will need to recruit and train new cohorts of technology consultants. For example, over the last few years, CETA has recruited and trained a new cohort of technology consultants annually, while the TECC Clinic experienced a gap in training new technology consultants during the COVID-19 pandemic, but has since resumed.

Conducting an Appointment

This chapter introduces principles for working with clients. We provide suggestions for structuring an appointment and include examples of consultant-client interactions in existing clinics. For an introduction to the principles of technology abuse itself, please see Chapter 9: Helping with Tech Abuse.

Principles for Working with Clients

Chapter 2: Overview of a Technology Abuse Clinic, introduced guiding ethics for technology abuse clinics. This section builds on these guiding ethics by emphasizing concrete approaches for communicating with clients that are consistent with the spirit of those ethics.

Client-centered: Respect the clients' wishes and trust them to be the final authority on what actions are best for their situation. Presenting options, explaining risks, and making recommendations reaffirms clients' agency; making decisions for them or pressuring them into an action does not.

Transparency: Let clients know why you are asking the questions you ask, what you are writing down, what you are looking for in their devices and accounts, and the nature of any communication with their care team (e.g.: advocate, lawyer, etc), if any.

Meet the client at their technical literacy level: Inquire about whether or not a client is familiar with a technological concept and offer to explain it if they are not. Avoid condescension with clients of all levels of technical literacy.

Know what the law requires of you: Are you a mandatory reporter in your state? What constitutes mandatory reporting? Be cognizant of your legal obligations, and adhere to them, as not doing so will put the clinic's legitimacy and ability to function in jeopardy. If you are collecting data for research, be aware of your institution's research ethics requirements (e.g., Institutional Review Board approval processes).

Avoid judgment: It is common for clients to share aspects of their life that do not directly relate to technology abuse, some of which you may not personally agree with or which may involve illicit or illegal behavior. However, unless you are a mandatory reporter (see above), clients seeking help should not have to fear that information they share in a vulnerable setting would be used against them. Relatedly, avoid asking questions about a client's situation that are not directly related to their technology abuse concerns.

Rely on expert DV training: While we provide tips on phrasing and language to use, this toolkit cannot replace expert-led training on how to incorporate sensitive, inclusive language and practice into interactions with clients.

Handling an Appointment

We break the appointment structure into three stages, organized chronologically: preparation, consultation, and follow up. Not all of the elements discussed in each stage may be necessary, and if the clinic service delivery model allows for tracking multiple appointments with individual clients, then some stages may be repeated.

Preparing for an Appointment

Clients often face complicated, multi-faceted technology safety risks. The difficulty of addressing all of these complexities is compounded by the limiting factor of time; we have found that even when a service model allows for repeated appointments, clients often have difficulty returning for second or third sessions. Thus, clinic sessions benefit from a structured plan to leave clients with at least some of their concerns addressed.

How much preparation prior to a client appointment that you will be able to do will largely depend on what information the clinic receives from the intake form and what amount of detail the client has given in the form. Most intake forms should, at a minimum, identify high-level categories of concerns, as well as the type and model of any devices the client is concerned about; this allows the referral coordinators to pair the client with a technology consultant familiar with those devices, if possible.

An important caveat is that, for a variety of reasons, the intake form may often contain vague, inaccurate, or out-of-date concerns. It is helpful to view it as a guide, but to avoid taking it as gospel.

Before any appointment, consider preparing the following:

A quiet, private, and appropriate space with stable Internet to conduct the appointment.

- For remote appointments, for example, it is not recommended to conduct the appointment in a coffee shop.

In-person child care and/or an appropriately staffed waiting room for clients with dependents.

A predetermined practice for using names.

- Technology consultants may not be comfortable sharing their names with clients. Some may be. In our clinics, we leave this up to individual consultants; names can help build rapport, and there is always an option to use a pseudonym, if desired.

A mechanism for taking notes.

- Taking notes is useful for keeping track of important information, such as how many devices/accounts the client has, the client's specific concerns, troubling technology behaviors and connecting these behaviors with specific devices, and dates that the person of concern may have had access to devices or accounts.
- However, ensure you also have a clear policy regarding storage, deleting, and anonymizing notes (e.g., shredding paper notes, deleting non-cloud stored notes, or saving them in accordance with established data preservation policies).

Easy access to relevant technology abuse resources (e.g., guides).

- Often consultants will benefit from having similar devices or accounts to the client's available, particularly for remote consultations where the consultant cannot see what the client is looking at.

Emotional + mental preparation.

- Clients may share difficult and detailed stories of abuse when discussing their technology concerns.
- Clients may also frequently not show up to appointments; in our experience, nearly a third to a half of appointments are cancellations or no shows (for a wide variety of often justifiable reasons).

Conducting the Consultation

One of the most challenging aspects of helping clients with technology abuse may be sifting through the information presented by the client and soliciting more details to accurately identify potential cases of technology abuse. We divide the consultation into a suggested three-phase approach for consultations: (I) understand, (II) investigate, and (III) advise. While the first two exploratory phases should happen in order, a session may need to repeatedly cycle through them before moving on to advising.

I: Understand

Clients come in with a variety of concerns, and it can be challenging for a consultant to understand precisely what the client is describing. Often, clients will have broad or ambiguous descriptions of technology *behavior* (e.g., bad cell service, hot or slow devices) or imprecise descriptions of technology abuse (e.g., "they have access to *everything*", "she can see everything I do"). It is important for the consultant to begin by working to understand what the client is experiencing. In so doing, it is important to strive to be validating and non-judgmental.

Tip: *Phrase questions in a way that affirms the client's experience.*

Example: *Client states: "They can see everything I do"*

Avoid: *Accusatory responses, such as "What proof do you have?"*

Try instead: *"What made you aware that they can see what you're doing? Can you give us some examples of when they knew something that they shouldn't have known?"*

We suggest starting with some time dedicated to letting the client explain, in their own words, why they sought out a consultation, even if the client has already provided some of this information in an intake or referral form. Clients may have many devices or accounts of different types, each obtained at different times. It is useful to have note-taking apparatus available to write down pertinent information such as the device make and model, who it was purchased and set up by, and the date that the person of concern may have last had access.

During the 'understand' phase of an appointment, the technology consultant will likely need to sort through the information provided by the client and ask questions to obtain more information about specific technology concerns. (See the Technology Safety Checklist for useful prompting questions.)

Tip: *It is not uncommon for clients to discuss other forms of abuse (e.g.: physical, sexual, verbal) as they talk about technology-specific abuse, particularly as they recall timelines. Professionalism is important, but it is okay to express sympathy that is appropriate for the gravity of the story (e.g.: "Oh wow, that's awful!" or "That's really terrifying!")*

Example: *Client shares details about an incident of physical abuse that occurred during a vacation, which was the first time they realized the abuser had access to their devices.*

Avoid:

- *Offering platitudes or ignoring the story and moving on, which can seem dismissive.*
- *Asking unnecessary follow-up questions about their abuse, which can be voyeuristic*
- *Attempting to act as a therapist for the client. Even if you are a licensed therapist, the client did not come to the clinic asking for therapy.*
- *Judgments about the abuser (judgments of **a situation or action** are okay), as clients may have a complicated or defensive relationship with the abuser.*

Try instead: *Acknowledge what they shared, express concern, and try to redirect back to the technology abuse:*

- *"I am so sorry to hear that; that sounds like it was really scary. I know it must be hard to talk about, but this information helps us understand how we might help with securing your technology from [the person who's harming you]"*
- **Note: consultant should mirror the language/pronouns used for the abuser.*

Interpersonal Challenges

Some sessions are more difficult for consultants to navigate with sensitivity than others. For example, some clients may become distressed and overwhelmed, even to the point of expressing a wish to harm themselves or others. Other clients may be hypervigilant, i.e. displaying a self-protective distrust of technology and perhaps even the technology consultant, which may manifest as an concern that all their devices are 'instantly and always hacked'.

This is not the same as an unfounded belief in conspiracy, as it is situated in their real abuse history; however, occasionally, clients may have such delusional beliefs. It is not the job of the technology consultant to try to treat or even distinguish these cases; they must simply treat each client with due diligence in checking the safety of accounts and devices.

Additionally, consultants should appreciate that clients may have sought help from other resources (e.g., law enforcement) and previously been met with disbelief or otherwise incredulous responses. Not being believed can increase trauma responses, including feelings of hypervigilance and mistrust, which can make trying to understand the client's technology concern more difficult.

Consultants may hear clients make defensive statements, such as "I know this sounds crazy, but..." As stressed elsewhere in this toolkit, consultants should respond in an affirming way, and not express skepticism about client experiences. Even if a client's fears are not technologically founded, that doesn't invalidate their feelings. That said, consultants can and should explain what is likely or unlikely in terms of a technology risk. This might include pointing out that it's not feasible for people to remotely hack up-to-date devices.

The intake process can attempt to check that the client would benefit from the specific services offered by the clinic, but no intake will be perfect. Any intake process also needs to balance against the undesirable effect of inadvertently turning away clients who could benefit from the service.

Consequently, consultants should be prepared through training for a range of dynamics that could present during a session, including the challenges of navigating difficult sessions with clients. A clinic may want to consider assigning a second consultant to sessions, when available, to provide mutual support and to assist in identifying concrete steps that can be addressed during the session.

Takeaways: Create a comfortable and affirming space for clients to share their experience. Anticipate that clients may be embarrassed about their lack of technical knowledge or fear that they won't be believed, and use language to deliberately counteract these fears. Ask for examples, details, important dates, and signs they may not have noticed.

II: Investigate

Based on information gathered from the client, the technology consultant should prioritize which problems to try to help the client with. At this point, the technology consultant can begin to work with the client to make a plan for which technology issues to begin investigating. For example, if a client has presented multiple concerns, such as belief their location is being tracked, a compromised email address, and harassment on social media, then the technology consultant can repeat these concerns back to the client, suggest which to prioritize, and ask the client if they agree with that prioritization.

Tip: Avoid making promises to clients that cannot be guaranteed. It can be tempting or even difficult to realize when you are using over-promising language in the moment, so actively work on setting expectations with clients.

Example: Client shares that they believe the abuser can read all of their messages and emails.

Avoid: "We will look into this and find out what's really happening.", or "We can make sure that that doesn't happen again."

Try Instead: "We will take a look together and do our best to help. Your safety is our priority." or, "We'll do everything within our power to help find an explanation."

A crucial feature of this phase is that the technology consultant is working with the client to examine the existing configuration of a piece of technology **while avoiding making any changes.**

Safety note: Making changes without investigating the status of the technology can result in the loss of crucial evidence or unwittingly send a notification to the abuser that may trigger an escalation of behavior, such as instigating physical violence, increased harassment, or involving friends and family members.

A non-intrusive investigation may include:

- Looking at the security or privacy settings on an account,
- Looking at a list of installed apps on a device,
- Scanning a WiFi network to find connected devices, or
- Searching for a physical tracker.

In each of these examples, the technology consultant and client are looking for detailed information about the potential causes of a technology problem, without disturbing or changing the status quo.

Tip: Clients may feel traumatized or triggered by even looking at their technology. If in-person, some clients may prefer to let the consultant physically handle the devices. Other clients may not want anyone else to touch their devices. We encourage consultants to ask the client what their preference is, and in either case, the consultant should always explain what they are doing and why.

Example: "We'd like to take a look at the settings of your device to see if we can find some information that may help us understand the situation. Would you like us to walk you through the steps, or would you prefer if we handled your device for you?"

If the client chooses the latter option, the consultant could respond by saying: "Sure, we're happy to do that for you. We'll show you what we're doing. First, I'm opening up the system's preferences menu by tapping on this icon."

Investigating the cause of certain behaviors will often require exploring several different explanations. It is helpful to ensure that consultants are equipped with resources reminding them of those explanations. Given the time-limited nature of sessions, it is also useful to investigate those explanations from most common to least common.

Consultants should also feel comfortable letting clients know that they need to do further research or consult with their colleagues when necessary to provide the most complete or up-to-date information. While we reserve a discussion of the technical explanations for the next chapter (see Chapter 9: Helping With Technology Abuse), we also provide an example of resources like the Technology Safety Checklist in the Appendix that can help consultants recall relevant investigative strategies on the spot.

Takeaways: After understanding the client's technology abuse experiences, work with the client to inspect their devices, accounts, technology, and surroundings (e.g., vehicles, IoT/spy devices, purses/backpacks) to uncover additional clues. Avoid making any changes at this stage, such as logging out accounts or changing a password.

III: Plan, Inform, and Advise

After working to understand and investigate the client's concerns, the client and consultant should ideally be able to ascertain or rule out several sources of technology abuse at this stage. (See Chapter X Helping with Technology Abuse for more details.)

If the consultant and client have found a possible source of compromise, (e.g. found an unrecognized device, unauthorized log-in, or misconfiguration), there are several next steps that could occur.

Tip: *If signs of compromise are uncovered, it is important to explain to the client what information may have been leaked to the person causing harm. However, clients will likely need time to process, and may want this information written down to remind themselves later. Tone is as appropriate as language here; try to use a calm but sympathetic voice. Clients will react to how you react, so if you feel nervous, take a moment to control your own reaction.*

Example: *Consultant and client find out that the person causing harm has been logged into the client's iCloud.*

Avoid: *Immediate problem solving, downplaying or overplaying the risks, e.g. "This is really bad! We should remove it now." or "[They] have definitely been reading all your email!", or "Don't worry, [they] probably haven't even been checking it."*

Try instead: *"How are you doing? Would you like to take a minute? We can walk through what this means now or I can send some follow up information." Or, "I'm sorry, I know this is really upsetting. Do you need a moment? There are some safety steps we can take, but we can talk through them when you're ready."*

The first step is to encourage the client to document the compromise and explain why that could be important. Even if the client is not currently pursuing legal action, they may want to in the future or may want the documentation for proof in non-legal settings. Self-documentation (e.g., the client taking screenshots of security interfaces) as a practice is strongly encouraged.

The second step is to determine whether removing the source of compromise will alert the person causing harm. If so, it is vital that the client be informed of the potential risks. If the client has a DV advocate, the consultant should talk to the client about following up with their advocate for further risk assessment and safety planning.

For example, a knee-jerk reaction to finding a physical device may be to immediately disable it; however, the consultant and client should pause to discuss what can occur should a device be disabled.

Lastly, after documentation and discussing risk, the consultant can discuss options for remediating the issue and talk through steps for preventing future compromise. It is important to thoroughly check any connected devices or accounts (for example, investigate the recovery email if it is an account, or scan the WiFi if the client finds an unknown device). We also recommend doing a thorough check of any other devices and accounts if possible, even if the client was not initially concerned about them.

More often than not, an investigation will yield some ambiguous security concerns, but little or no clear evidence of compromise. In this scenario, we still recommend following the same steps as above for identified security risks; in fact, it may be more crucial to document anything unusual if it is ambiguous.

In this scenario, it is important to explain the different possibilities and risks to the client in a way that avoids instilling fear. While the client's safety is paramount, and the risk associated with abuse escalation should be explained if possible, it is important to help normalize the everyday security risks involved with using digital technologies as distinct from abuse.

For example, a client may understandably display extreme anxiety about technology behaving in 'normal' but frustrating ways, such as a slow device or poor cell phone reception, or might be convinced that spam messages, pop up ads, texts, etc. are all sent from the person causing them harm.

Tip: It is not uncommon for abusers to threaten their victims by mixing exaggerated claims of their technological capabilities with tangible acts of harm. An advantage of a technology clinic is that consultants can help 'deprogram' the fear inculcated by abusers without dismissing the clients concerns through gentle but firm education.

Some strategies and phrasings that help with this include:

- *Relying on expertise accumulated by the technologist and clinic, such as sharing research that indicates that most tech abuse is not very sophisticated.*
- *Validating the client's concerns by sharing (anonymized) stories encountered with other clients. "A lot of clients that we see feel the same way, and it's totally understandable. We've found in practice that..."*
- *Relating stories of receiving similar harassing messages from spammers, "e.g., I get those kinds of calls, too, and they're annoying but unfortunately very common."*
- *Explicitly stating that abusers tend to over exaggerate their abilities. "We hear from a lot of clients that their abusers state that they can do X, but in practice, we know that it's technically not possible in most circumstances."*

Post Appointment Follow Up

Follow up options post-appointment will depend on the clinic and its service model. However, we suggest having set protocols to allow follow-up communication, such as recording necessary information about a client's case and contact information, along with mechanisms to ensure those protocols are followed for everyone's safety.

Some safety guidelines to consider:

If you plan to share information with another care worker (e.g., a lawyer, social worker, advocate), ensure that you have the client's explicit consent to do so and that you do not violate confidentiality agreements.

- Some clients may be concerned about how they will be portrayed to, e.g., a lawyer, especially if little concrete evidence was found.
- Transparency can help: let the client know exactly what you will say and give them the ability to edit the information you send.
- For information that affects the client's safety (e.g., abuse escalation risks, information about past compromises), confirm with the client that you have their permission to share that information and with who, specifically.

Be careful of handing out written resources, pamphlets, or flyers. If the client still shares space with the abuser, this may put them at increased risk of harm.

Adhere to the data safety practices established by the clinic for protecting private client information, discussed in detail in Chapter 8: Clinic IT and Data Management.

Technology consultants should not give out their personal information to clients or have direct follow up with clients outside of the clinic's protocols.

Clinic IT And Data Management

Data security is important for any organization that collects, retains, or otherwise comes into contact with identifying information such as individuals names, phone numbers, and email or physical addresses, particularly if those individuals are at a higher risk of danger or harm than the general population, such as survivors of intimate partner violence.

At a technology abuse clinic, data security is especially important. In addition to the safety and well-being of clients, the legitimacy of the clinic itself is at risk if the clinic cannot safeguard its own data. In this chapter, we discuss:

- Privacy-preserving practices for clients
- Data retention policies, including tracing a single client case over multiple sessions
- Communications infrastructure
- Evaluation and data analytics of clinic data

These practices are important for the safety of clients, staff, and the clinic itself.

Collecting Personal Identifiable Information

Information that can be used to identify an individual either directly or indirectly is known as **Personal Identifiable Information (PII)**. According to the United States' Department of Labor, this includes:

- Names, birthdays, social security numbers or other ID numbers
- Physical addresses, telephone numbers, or email addresses
- Online contact information, including social media handles
- Combinations of demographic information such as gender, race, age, and geographic descriptors.

This information can be stored on paper, electronically, or both. Technology abuse clinics may encounter some subset of this information while working with clients. Safeguarding PII is crucial, as failure to do so can result in substantial harm to clients.

Data minimization is the principle of collecting only the information that is **relevant** and **necessary** to provide a service. Which data meets the criteria of relevance and necessity will vary depending on the clinic's service delivery model. In some models, there may be no need to collect any PII from a survivor other than what is shared during a consultative session. In other models, it may be necessary to gather names, pronouns, and contact information. In early stages of a clinic, it may be beneficial to select a service delivery model that requires collecting zero information from potential clients, as was the case for all three existing clinics when they first started operating.

Minimal data that may be considered relevant and necessary for providing service at a technology abuse clinic, especially during intake, might include:

- Technology concerns (description of concerns, types of devices used)
- A name for the client (which may be a pseudonym)
- Contact information (phone, email) for the client and/or their DV advocate
- Limited demographic information, including languages spoken by client

Legal Risks of Data Collection

Collecting PII may also present legal risks, depending on the laws governing your clinic. For example, a client (or abuser) may be able to file a subpoena asking for data from a client appointment. Some advocacy organizations are legally shielded from subpoena, and some are not; this depends on local and state law.

A common practice among organizations that are not protected from subpoenas is to use a combination of tactics, such as not collecting identifiable information, minimizing the usefulness or specificity of any data retained, and proactively deleting any collected data. This will shape the policies of how the clinic runs, including how consultants are trained to treat note-taking, which often includes a wealth of client information.

It is useful to consult with legal experts to assess liability and risk when developing internal practices surrounding data collection discussed in the following sections.

Redacting Data Collected From Client Sessions

Technology consultants will need to take notes during appointments, either with pen and paper, or electronically. If the clinic does not keep notes from sessions, then consultants and the clinic are responsible for properly disposing of those notes. However, the clinic may choose to retain notes from sessions for various reasons.

Clients may sometimes share sensitive information during an appointment, even if not directly solicited. If the clinic retains session notes, they should incorporate a practice for anonymizing notes and not retaining sensitive information, either by not storing it or redacting it.

Some examples of data that should not be stored in a client file are:

- Home addresses, specific geographic location, social security numbers, ID cards (Note: clients may want to share this information so consultants can determine if the client is 'searchable' online or vulnerable to identity theft)
- Log-in information, including passwords or pins
- Documentation or evidence of abuse, such as screenshots of log-in history or data requests from technology platforms
- Client's personal photos, especially in cases of image-based abuse

In all of these cases, an alternative to the clinic retaining the client's information is for the technology consultant to guide clients on how to navigate the steps or interfaces themselves, on a safe device that is preferably owned by the client.

Communications Infrastructure

Technology consultants may require communication infrastructure, especially if the clinic offers remote appointments. This includes video conferencing software (like Zoom, Skype, or Google Meet), an email address, or a phone number to use for client communication.

For both the client and the consultant's safety, it is important that all accounts used by consultants to communicate with clients are **not** personal accounts. Not only does this protect the identity of consultants, it prevents client PII from being mixed into the personal accounts of consultants.

Other clinic infrastructure that does not deal directly with client PII may be connected to consultants' personal accounts. Examples of this include messaging platforms, such as an instant messaging platform (e.g., Slack, Discord, IRC) or a mailing list to communicate with other consultants during and between sessions.

When setting up communications infrastructure for technology consultants, some important considerations include:

- What client information is included in the application? (e.g.: will the client's phone number or email address be retained by the application?)
 - If so, what is the *access* and *retention* policy for this information?
 - How will you communicate this policy to technology consultants?
- Is the application traceable or connected to the **technology consultant's** personal information?
 - Technology consultants should avoid using personal phone numbers or personal emails for both their own and the client's safety.
- What safeguards will the clinic put in place to ensure that the communications infrastructure is being used in accordance with the data safety protocols developed by the clinic?

Storage, Access, and Authentication

Regardless of the client data that is collected, the clinic should maintain a policy for how that data is stored, by whom and how it can be accessed, and for how long the data will be retained.

Storage

Data should be stored in a secure location, whether physical or virtual. When selecting a virtual storage platform, considerations may include:

- What are the data storage policies of the storage platform? Does the storage platform have a policy of reading or selling data uploaded by their users? This is particularly common on free-tier services; some platforms may have a commercial licensing option that restricts sale of user data.
- What are the data storage access control policies? Can you set permissions for individual files, users, or revoke permissions easily?
- Does the data storage platform require 2-Factor Authentication for workspace members to access data?
- Encrypted storage is nice-to-have, but not necessary for clinic safety.

Most security problems relate to access control (who has access to what) and authentication (identifying who is making an access). While we discuss this in the next paragraph, it is important to keep in mind what capabilities your chosen storage platform has to support controlled access and authentication.

Access and Authentication

Data access refers to whom within the clinic has access to individual pieces of data and authentication refers to how the system identifies who is attempting to gain access.

Granting access to sensitive data should be managed with clear, transparent policies and accurate record-keeping. Each individual requesting access to each piece of sensitive data should have a clear, defensible reason for needing to access that data, and a record of who has requested and been approved access should be kept as long as the data lives. Access should also be revoked at key points, such as when a technology consultant or staff member is no longer working at the clinic.

In general, the more people who have access to a single file, the greater the likelihood that the file is compromised. To decrease the likelihood of compromise, best practice entails restricting access to data as much as possible. This also pertains to the granularity of data; an individual requesting data for a particular client should only be able to see the data for that particular client, not all client data.

Equally as important, the clinic should maintain strong authentication practices. This generally means enforcing strong passwords that are stored in secure location such as a password manager (not a sticky note on a laptop or in a plain-text document!) and mandatory 2-Factor Authentication.

Managing Data Policies

Clinics should have clear policies that limit the duration of time that data is retained and when access to existing data is revoked. Deletion of data can be triggered by an event, such as a client concluding services with the clinic or a technology consultant deciding to leave the clinic.

In these examples, a designated staff member may want to delete all data associated with that client (notes, screenshots, text messages, or emails), or revoke all access permissions granted to the technology consultant. Data deletion may also be triggered by a designated time period (e.g. deleting all data from inactive clients on every 90 days).

For each type of data about a client that the clinic collects, it is useful to write down why it is collected, who has access to it, and how long or under what circumstances it should be retained. On a regularly scheduled basis (e.g. the first of every month, or every 90 days), someone in the clinic may want to review all actively held data, revoke or reset any permissions, and purge any data that should not be kept.

Depending on how the clinic is structured, these policies may need to be developed in conjunction with the policies of any agency partners. The National Network to End Domestic Violence (NNEDV) has resources with additional guidance on managing data and records.

Research, Evaluation and Analytics

The clinic may want to collect and retain some information for evaluating their services, internal analytics, and general research. For example, a clinic may be interested in collecting certain pieces of demographic data to determine whether they are under-serving a particular community, what barriers to service clients are experiencing, or whether the clinic should invest more resources in responding to a specific technology issue that shows up disproportionately.

Data that is gathered for internal evaluation and research typically does not require approval from an Institutional Review Board, even if the clinic is affiliated with a university, unless the clinic intends to publish or share data externally (e.g., presentations, journal or conference papers, or peer-reviewed articles).

If your organization has interest in publicly releasing its data for research or other purposes, you will need to determine whether that work requires human subjects approval from an Institutional Review Board before you collect that data. When sharing data externally, be mindful that in addition to explicit personal identifiable information, such as names and addresses, client stories that are highly specific can function as identifying.

Data can be gathered passively during the service provision itself, such as by collecting or preserving notes, or recording a call. Alternatively, data can be solicited for the express purpose of evaluation, such as asking clients to fill out and pre-and-post surveys about their experience with the service and what they've learned. In the latter case, such data should not be required for or otherwise interfere with service, and this should be made clear to clients. In either case, it is important to inform clients of what data is being collected and with whom it might be shared.

Helping with Technology Abuse

This chapter provides pragmatic suggestions about how to approach helping IPV survivors with technology abuse. A key challenge is that technology changes quickly, causing advice tailored to current technology systems to rapidly become obsolete.

Relatedly, consultants who are intimidated by the complexities of cybersecurity may feel like they lack sufficient expertise to help clients. The goal of this chapter is to help readers realize that even a small amount of preparation has the potential to support many clients. In this chapter, we provide general guidance about typical abuse issues, suggestions for structuring discussions with clients about technology abuse, strategies for researching unfamiliar tech situations, and managing the inherent uncertainty about real and perceived capabilities of abusers.

Topics covered:

- Introduction to Technology Abuse
- Core concepts for tech security:
 - Devices
 - Accounts
 - Security mechanisms
- Being prepared to help with unfamiliar technology

Introduction to Technology Abuse

We begin by discussing what technology abuse is in the context of intimate partner violence. Technology abuse includes any actions taken by an abuser to threaten, monitor, harass, or otherwise harm their victim using digital means. In other words, digital technologies serve as tools to engage in long-standing patterns of coercively controlling behavior. A non-comprehensive set of examples of tech abuse include:

Monitoring: Using technology to monitor the survivor's communications (e.g.: messages, who the survivor is contacting, phone calls), data (e.g.: photos, videos, documents, emails), behavior online (e.g.: websites visited), or physical environment (e.g.: hidden cameras, microphones in the home).

Tracking/stalking: Using technology to keep tabs on the location of the survivor.

Harassment: Sending unwanted contact to the survivor, including SMS or chat messages, social media contact, phone calls, or making visible comments on social media posts, etc.

Proxy harassment: Arranging for members of a common social network or strangers to harass the survivor or signing the survivor up for unwanted messages.

Disclosure: Disclosing online (sometimes called 'doxxing') private information, such as non-consensual intimate images (NCII, frequently known as 'revenge porn'), home address or phone, sexual identity, HIV status, etc.

Impersonation: Pretending to be the survivor to cause reputational damage or to facilitate proxy harassment (e.g., pretending to be the survivor on a dating website and tricking people into visiting the survivor's home).

Financial harms: Causing financial harm by accessing online bank accounts or coerced spending through peer-to-peer payment and e-commerce apps (Venmo, CashApp, Amazon, etc).

Most of these types of abuse have non-digital analogues, and abusers may use both digital and non-digital means to coercively control the survivor. This can make it challenging to diagnose technology issues based on symptoms alone, and consultants should keep in mind that technology isn't the only plausible explanation for many harms.

For example an abuser can cause financial harm by stealing money, by using a known credit card number, and/or by accessing an online bank account. Or, they could stalk a client by physically following them, by seeing pictures of the survivor at recognizable locations online, by covertly turning on location-sharing, by installing tracking software on a survivor device, and/or by using a tracking device (GPS or Bluetooth device, like AirTags).

Understanding Intimate Partner Threats

There are unique considerations and dynamics to consider when technology abuse occurs within the context of intimate partner violence. Due to the relationship, the abuser will have some amount of personal knowledge about the survivor and may be part of their social network, may have had (coerced or freely given) access to devices and accounts, and may be motivated by coercive control rather than simply financial gain. In this context, the typical methods in which an abuser causes those harms falls into a few broad categories of abuser techniques:

Ownership-based access refers to problems that emanate out of the fact that the abuser may be the one who owns or sets up technology used by the survivor. For example, they may have been the one who pays for a cellular phone plan or who set up a family's iCloud account.

Account compromise occurs when an abuser is able to access a survivor's online accounts, such as email, iCloud, or social media, most often by simple expedient of knowing the password.

Device compromise arises when the abuser is able to access a device (and be able to unlock it, such as by knowing a PIN, password, or having access to a biometric such as fingerprint). This allows them to reconfigure the device (e.g., add a new fingerprint, turn on location sharing), access sensitive data, and more.

Fake accounts / spoofing: The abuser may set up fake accounts online, disguise their phone number ('spoofing'), or use new, unrecognized emails or phone numbers. This doesn't require compromising accounts or devices, and usually arises in the context of online harassment or impersonation.

Use of IoT devices: The abuser may set up devices, such as GPS tracking devices, webcams, WiFi routers, WiFi thermostats, and more, often termed Internet of Things (IoT) placed in the survivor's home, vehicle, or workplace.

Core Security Concepts

Helping with technology abuse benefits from some understanding of key concepts in computer security. Many technology users may be familiar with some of these concepts, but here, we reframe them in the context of tech abuse.

Devices and Their Security

Device is a catch-all term for phones, computers, "smart" devices, and the "Internet-of-Things"; essentially anything that has computing built in. Devices consist of hardware plus software, and the combination of the two define the functionality of the device. Phones can surf the internet, take pictures, record sound, and more. Home devices like voice assistants can listen to conversations, perform Internet searches, or react to particular requests.

Operating Systems and Applications

Devices have operating systems (OS's). These are the lowest layer of software running on a device, and control and limit functionality of other software programs (programs, often called "apps"). For example, Windows is the OS running on personal computers (PCs), and MacOS runs on Macbooks and other Apple computers. On phones, the most common operating systems are iOS which runs on iPads, iPhones, and other Apple products, and Android which runs on most other phones.

Other devices (tablets, IoT) are similar; in each case, you can install more programs, like word processors, Internet browsers, etc. These programs are often called "apps", short for applications.

The OS places limits on apps. For example, the OS will, by default, prevent one app installed on a phone (both spyware/stalkerware and other non-malicious apps) from reading other apps' data without asking for explicit permission. What any app can or cannot do can be nuanced, and also evolves as OS's change over time.

"Hacking" a Device

The term "hacking" is used to describe a broad variety of activities. Here, we discuss what it means within the cybersecurity field as well as within lay usage.

Full Device Compromise

When security researchers talk about a "hacked device", they are most often referring to subverting the OS and taking full control over the software on the device. For phones, a compromised phone is "rooted" for Android or "jailbroken" for Apple.

When this happens, the person who is doing the hacking can install software that deviates from the original software's intended functionality. For example, a compromised OS could access data of all apps installed and used on the device.

Jailbreaking or rooting, even when possible, requires physical access to the target device. Remote compromises, where an attacker sends a specially crafted message to compromise a device's OS, do exist, but are in general inaccessible to the general public and, by extension, abusers.

As a rule of thumb, for well-protected targets (popular OS's with good security teams, such as Apple, Android, and Windows), discovery of remotely exploitable software vulnerabilities requires extensive resources to develop or buy.

While the news may breathlessly cover the latest "zero-day" vulnerabilities and hacks, it is increasingly only feasible for specialized security teams of security experts that only do business with companies and governments.

Of course, in rare cases an abuser may themselves be an employee at such a firm or otherwise have the rarified expertise to perform remote exploits. Even here there are many limits to their “powers” and the threat can often be mitigated via a reset of a device and updating it to the most recent version of the software.

Takeaway: Full device compromise can be fixed via a factory reset or purchasing a new device.

Spyware, Stalkerware, and Unauthorized Device Access

In summary, hacking a device requires rare, expert knowledge, exceptionally so for fully updated software. On the other hand, colloquial usage of the term 'hacking' often refers to covertly gaining access to a device, and this is often how clients use this term. This type of 'hacking' just requires the ability to unlock a device. For some devices, anyone can unlock them depending on how they are configured, such as a laptop or phone that does not require a password or biometric to awaken it from sleep mode.

Security practitioners refer to the means by which access is granted only to certain individuals as an authentication mechanism. Passwords are the traditional authentication mechanism, but increasingly devices use biometrics (fingerprints or face scans).

Unlike device hacking, the ability of an abuser to unlock a device is a widespread situation in IPV. When an abuser has access to a device, they can unlock it and then can utilize it via standard user interfaces (UIs) -- the same features and functionality that a regular user utilizes. Sometimes people refer to abusers in this case as UI-bound: their bad actions are limited to the functionality the device provides.

Unfortunately, almost every device has functionality that can be repurposed for tech abuse. Two high-level categories for repurposing include reconfiguring existing features and adding new apps.

Examples of reconfiguration are plentiful. For example, an abuser might change the settings for authentication mechanisms by resetting a password or enabling their fingerprint to unlock the device. Or they might change the settings for OS-provided location tracking features or another location tracking app.

Abusers may also add new, unwanted apps to a target survivor's device. A class that people talk about routinely is IPV spyware (also called stalkerware), which in some cases can monitor the device's use quite pervasively, including location tracking and, in some cases, theft of information from the device such as text messages.

UI-bound abusers who install unwanted apps or reconfigure the OS or apps can be damaging, and will often be called "hacking" by clients. While it's fine to meet clients where they are in terms of terminology, it's good to keep in mind that the more common UI-bound adversaries do not achieve full device compromise. This has implications for abuser's capabilities and remediations: removing an unwanted app prevents its use, and changing an unwanted OS configuration setting fixes it.

Importantly, resetting a device will help with a "hacked (fully compromised) device" but may not be effective in getting rid of an unwanted app if it is downloaded to the client's account (e.g. an iCloud or Google Play account), as the unwanted app may simply be re-downloaded when the client logs back in.

Takeaway: Abusers with access to a device can install apps or reconfigure existing tools to hinder survivor safety. Helping a client remove unwanted apps or change configurations can mitigate these threats, but a full-factory reset may not be effective.

Electronic Monitoring Devices

Clients are often understandably concerned that an abuser may have placed external devices intended to monitor their activities in their personal space without the client's knowledge or consent. These often fall into the categories of either "Internet of Things" devices or Bluetooth trackers, including GPS trackers planted in a vehicle. Uncovering such devices may be difficult, as such devices are often very small or well-hidden.

The challenges to discovering physical devices is compounded by clinic practices that prevent technology consultants from helping clients physically search their personal spaces. However, some basic understanding of how such devices work can help technology consultants remotely screen for them and may help assuage client concerns.

Recording Devices

Understanding how recording devices, such as mini-cameras or hidden microphones, operate can help with identifying creative solutions for finding them. Such devices require:

- a memory or storage unit to store recordings,
- a power source (either a battery or an electric outlet),
- and, frequently, a network connection to transmit the recording (either a short-range Bluetooth connection, or a long-range WiFi or cabled Internet connection).
 - If not connected to a network, then the abuser must be able to physically access the device in order to see the data that is stored in it.
 - Bluetooth connections also require the abuser to be within a few hundred feet of the device in order to 'link' with the device.

Given the amount of data that is picked up by a camera or microphone and the limited range of Bluetooth, a recording device will most likely be connected to the Internet, usually via the client's home WiFi.

The client can therefore be instructed to check which devices are connected to their Internet account (this can be through a third-party app such as Fing, or through their account with their provider).

Likewise, changing their Internet access password will 'knock off' any recording devices. Similarly, since recording is a power-intensive operation, many devices will be plugged into an outlet, and consultants can also advise clients to check all outlets for devices.

Takeaway: Recording devices either require an Internet connection or for the abuser to have physical proximity to the client, so many devices can be disabled by changing the client's Internet password.

GPS and Location Tracking Devices

For clients who are concerned that a device is being used to track their location, it can be difficult to ascertain whether such a tracking device is being used. Tracking devices, unlike recording devices, do not have substantial power requirements, and can last for years on a battery. Scanning for tracking devices is also difficult, as a tracking device can broadcast its location to the abuser without an Internet connection and without being actively connected.

Bluetooth scanners will surface tracking devices, but will also likely surface many benign false positives without enough information to distinguish from actual threats. Clients and consultants can work together to develop creative safety plans, including seeking out information about the most common tracking devices and how to detect them, but until universal tracker detection technology is available, there are limited options for addressing survivor concerns about tracking devices. Given the rapidly changing nature of this area of technology, we refrain from offering more specific advice.

Accounts and Their Security

Online accounts are key components of our digital lives. Email, social media, work websites, banking accounts, and so much more --- each has an associated account associated. Creating and using an online account typically requires the use of a username and a method of *authentication* to verify who is accessing the account, such as a password. Your username is often, but not always, an email address.

Accounts are a prime target for abusers, likely due to the level of intrusiveness access can give them and for the often ease of remote compromise. Unlike devices, accounts are designed so that one can access them from anywhere, on any device --- assuming one can authenticate themselves.

Authenticating Online Accounts

Authentication mechanisms for accounts are still predominantly password-based, though this has been evolving.

We now see several forms of authentication:

Password/PIN authentication in which a sequence of characters or numbers grants access. Modern accounts may have requirements about the 'strength' of the password, such as minimum length, types of included characters, etc.

Email-based authentication in which a challenge (usually a numerical code or a URL to click) is sent to an email address associated with the account.

Phone-based authentication in which a code is texted to a phone number or delivered by an automated phone call.

Personal knowledge authentication in which you must provide answers to questions such as “what is your mother’s maiden name?” or “what city were you born in?”

Authenticator apps or previously registered “trusted devices” in which a challenge is sent or which shows a prompt to allow access from a certain device.

Biometric authentication in which an application grants access by recognizing the user's face or fingerprint.

Multi-factor authentication (MFA) or 2-Factor Authentication (2FA) in which an account requires a user to pass through two or more of the above authentication mechanisms, such as entering the correct password and receiving a verification code via text message. Most often, only two forms are required, hence the special case of 2FA.

Authentication as an Abuse Mechanism

Accounts allow users to configure how they authenticate their account, such as by setting which biometrics are recognized or which devices are 'trusted devices'. These configurations are often where problems arise. Abusers may reconfigure authentication approaches, by, for example, using their access to turn off 2FA, or by adding their phone number or email as a trusted device.

Reconfiguring authentication settings can grant covert access to a wealth of information, or even lock the survivor out of their own accounts. Consequently, researching the authentication settings for online accounts that are a cause for concern and reviewing them together can be helpful for many survivors.

Identifying Unauthorized, Unauthenticated Log-ins

It's helpful to understand a bit more about how logins work. Generally, users can login to a service via a web browser (by typing the URL into e.g. Safari or Chrome) or through a dedicated app solely for that service (such as the Venmo app). In either case, after a successful log-in, the browser or app stores a small piece of information.

This small piece of information is called a cookie. It is used to identify that this browser or app was recently authenticated, so that the user does not need to keep authenticating.

Some services have features to help users try to determine what browsers or apps have recently logged in, and which can still access the service. The web service keeps a list of which apps/browsers they've given a cookie to, and then shows that list to the user. This is quite valuable since it can provide insight into who is accessing a service.

For example, if the survivor sees a device logged in that matches the abuser's (e.g.: a particular version of a phone) this may be evidence that the abuser has accessed it. Sometimes these lists also show the time and approximate location of the device when login occurred.

Documenting such information by downloading it or taking a screenshot may be helpful for survivors who are involved in legal proceedings. Even if the survivor is not attempting to gather evidence, it can help with safety planning to understand what information the abuser had access to and when they had it.

Account Recovery

Finally, most services, though not all, have one or more mechanisms for account recovery. This is meant to allow the legitimate user to regain access to their account should they forget their password or otherwise have problems authenticating in the normal way.

Account recovery mechanisms typically involve sending a code to a designated email, phone number, or device; the term “recovery phone” or “recovery email” is how configurations often describe these. Security questions are sometimes also a way to recover an account.

Account recovery is a frequent “backdoor” for accessing an account. It can be useful to check an account’s settings to ensure that recovery emails/phone numbers are controlled by the survivor, rather than the abuser, or to help them navigate the account recovery process to regain access.

Security Tools to Mitigate Harassment

Many common tech safety problems don’t involve the abuser having to obtain access to a client’s devices or accounts. Instead, they involve, for example, posting harmful content online from accounts setup and controlled by the abuser.

Tools available to clients and those working on their behalf include:

Blocking mechanisms that allow a client to prevent content/accounts from interacting with them. For example, most phones allow blocking particular numbers and social media often can block particular accounts from sending content to your account. This may not prevent the abuser from using a spoofed account or phone number, such as a fake account or an app that allows the call to seem like it's coming from a different, even trusted, phone number.

Screening mechanisms such as using virtual phone numbers (e.g. Google Voice) as a 'safe' number or coordinating pass phrases with trusted contacts.

Reporting content to companies. Many companies allow reporting content or accounts to them, particularly in the context of social media. Whether or not content/accounts will be removed or banned is often up to the peculiarities of company policy and their implementation of that policy.

Takedown requests are a special type of report asking a Internet service provider or search engine to remove content from appearing. There are also professional services that issue takedown requests, and clinics may develop a relationship with them allowing their clients to obtain free services. In other cases, it helps to have lawyers assist with this effort.

Being Prepared to Help with Unfamiliar Technology

No consultant can be familiar with all the various kinds of technology that will arise in discussion with a client. This is true even for technology experts -- the number of possible apps, devices, or other artifacts is too large, and rapidly changing. Coping with the diversity and evolution of technology is a key challenge for clinics. Here we provide some advice for structuring a clinic to countenance this challenge.

Normalize the necessity of researching problems: A clinic can normalize the need for consultants to look up information, either in the moment while helping a client or doing research between appointments. This includes telling clients that the consultant needs to do some research to try to help answer the question.

Assess reputability of advice: A lot of online advice is bad. Clinics should try to cultivate a sensibility about what are trusted sources of information and how sources of information map (or not) onto typical abuse threat models. This can be useful not only for consultants but also for them to help inform clients they serve about good sources of advice.

Develop connections with the tech community: A key resource for research can be a network of people to which technical questions can be asked. Clinics might consider recruiting tech workers as consultants, and/or seek out connections with tech workers to be available as resources for the client. CETA for example uses a chat platform with a broad range of technologists who have made themselves available to answer questions about technology issues from CETA consultants (without disclosing identifying information).

Document common issues and solutions: Writing down common situations, and, ideally, sharing them with other support organizations can help build up a body of knowledge. For example, CETA has a number of guides for common issues at <http://ceta.tech.cornell.edu/resoruces>.

Appendix I: Clinic Histories

- The Technology Enabled Coercive Control Clinic (Seattle, WA)
- The Clinic to End Tech Abuse (New York, NY)
- The Madison Tech Clinic (Madison, WI)

The Origins and History of Existing Technology Abuse Clinics

This toolkit focuses on informational and discursive resources for those interested in starting a technology abuse clinic. However, in our experience there is interest in hearing about where the idea for these clinics came from and a more narrative overview of their foundation. We include this information here in the appendix.

The Technology-Enabled Coercive Control Initiative (TECCI)

The Technology-Enabled Coercive Control Clinic was established by survivor advocates in the Seattle area who observed that technology was increasingly showing up as a method or tool for abuse. Building off the literature of coercive control that encapsulates coercive behaviors that include but go beyond violence, they termed this "technology-enabled coercive control" and established a working group (TECCI) to brainstorm how they could help advocates respond to it.

Initially, they conceived of an app that could help survivors navigate their digital privacy, but after a similar app was released by the National Network to End Domestic Violence, they realized that the app alone could not replace human-mediated support.

Drawing on their advocacy backgrounds and local network, TECCI began recruiting and training technologists to staff trials of a monthly technology clinic where survivors could get 1:1 support. Today, the TECC Clinic is run by New Beginnings, a community-based domestic violence agency in Seattle.

During the development of the TECC Clinic, members of TECCI connected with Professor Ristenpart and Professor Dell who were interested in creating a similar service in New York City (see below), and who helped provide support around technology questions.

The Clinic to End Tech Abuse

Conceived around the same time as the TECC Clinic, the Clinic to End Tech Abuse formed out of a research project at Cornell Tech, the graduate campus of Cornell University located in New York City. Professor Thomas Ristenpart and Professor Nicki Dell collaborated on a project to measure the use of spyware in intimate partner violence relationships. Reaching out through contacts, they began meeting with advocates at New York City's Family Justice Centers, run by the Mayor's Office to End Gender-Based Violence.

Through these field studies designed to measure spyware, they quickly realized that (1) dedicated spyware apps were not as common as benign apps being repurposed by abusers (2) there were many other technology issues beyond spyware that survivors of intimate partner violence wanted assistance with, and (3) they needed to develop protocols and guidance on how to dispense that assistance while preserving the safety and dignity of everyone involved.

Also in touch with members of TECCI, the initial CETA team began conducting a series of focus groups with advocates and survivors to help develop protocols and guidelines for working with survivors. From those focus groups, the Clinic to End Tech Abuse grew from one-off sessions

with survivors, to monthly visits "tech clinic days" at local advocacy agencies where the research team would meet with 1-4 survivors, to the current model staffed by dozens of volunteers responding to over 160 referrals a year.

The Madison Tech Clinic

Professor Rahul Chatterjee at the University of Wisconsin-Madison was involved in the initial founding of CETA as a PhD student leading the spyware measurement project. After starting his professorship at the University of Wisconsin, he started a similar clinic in Madison. Through a chance run-in with a visiting speaker who was able to connect him with the major anti-violence advocacy network in Madison, he was able to establish an agency partnership where his students at UW-Madison would receive training and support to work with survivors wanting technology services.

Appendix II: Resources

A. Chapter 3: Agency Partners

- Memorandum of Understandings (MOUs)
- Advertising Services
 - Flyer
 - Referral Guide

An MOU (memorandum of understanding), also called a 'linkage agreement', is a document outlining the relationship and responsibilities between two entities that is typically legally non-binding. It is not intended to be a formal contract, but rather a structured outline of mutual expectations and roles.

An MOU typically consists of: the names of the organizations entering into a partnership, a short description of each organization, and a list of services or materials that each organization pledges to provide to each other. Optionally, the MOU may also include dates that the MOU is active, expectations of compensation, and limits on service.

Below, we share two examples of MOUs used in existing technology abuse clinics between the clinic and its community partner. Out of respect for our partner organizations, we have redacted direct references to entity names.

EXAMPLE MOU #1

Pursuant to the proposal submitted by [entity], the proposer, if funded, will continue its ongoing community partnership with Cornell Tech's Clinic to End Tech Abuse ("CETA") as described below. Through this linkage agreement, [entity] and CETA agree to the following, pending funding:

- To partner in a coordinated, mutual referral program through the Family Justice Centers to ensure comprehensive, holistic services to survivors of gender-based violence.
- CETA will refer gender-based violence survivors to [entity] for culturally and linguistically sensitive immigration legal services including immigration legal screenings, legal advice and consultation, and legal representation.
- [Entity] will refer survivors to CETA for its tech abuse services focused on checking the security and privacy of a client's devices and online accounts.
- [Entity] and CETA will make a range of professional trainings in key practice areas available; and partner on community events and awareness-building activities.
- [Entity] will also make its full range of legal, clinical, and workforce services available to CETA clients who are survivors of gender-based violence.

Pending borough-based funding, [Entity]'s immigration legal services will be available in community-based NYC Family Justice Centers in Brooklyn, Manhattan, the Bronx, and Queens; as well as via virtual appointments as needed. CETA services will be available primarily virtually to survivors citywide, and in limited instances where there are safety concerns, appointments may be arranged at the Family Justice Centers or [Entity]'s Manhattan office.

EXAMPLE MOU #2

LINKAGE AGREEMENT BETWEEN [ENTITY] And CLINIC TO END TECH ABUSE (CETA)

START DATE–END DATE

[ENTITY]

[Several paragraphs briefly outlining the background, founding, and mission of the partner agency, as well as the core programs and services provided by the entity. See below for concrete example of how CETA describes its services.]

CLINIC TO END TECH ABUSE (CETA)

The Clinic to End Tech Abuse (CETA) at Cornell Tech champions the freedom of abuse survivors to use technology without fear of harm. We believe that abuse survivors should have access to the resources, knowledge, and necessary support required to safeguard themselves and their technology from digital harm.

Perpetrators of intimate partner violence use digital technologies to harm their victims. Some of their most powerful tools include the same e-mail, cloud, and social media platforms millions of people use every day. Through a variety of technological methods, abusers can gain a powerful and dangerous trove of information with which to monitor, harass, exploit, threaten, or otherwise harm their victims.

CETA was founded in 2018 out of Cornell Tech, partnering with the New York City's Mayor Office to End Domestic and Gender Based Violence, with the goal of supplying direct interventions to survivors experiencing technology abuse. At CETA, we work directly with survivors of intimate partner violence in free, consultative sessions to determine how and if someone is using technology to harm them. During these consultations, we help survivors to create an individually tailored safety plan that provides them with the education and tools needed to stay safe. We also use this firsthand knowledge to facilitate research on how abusers can misuse technology, advocate for laws and policies that create protections from technology abuse, and publish resources and trainings for others who would like to help survivors.

To date, CETA has received referrals from over 400 survivors in New York City for either remote (virtual) or in person consultations across all five Family Justice Centers in each New York City borough. CETA will offer these services to those clients referred by [ENTITY] who are eligible to receive our services.

Both agencies described above and undersigned will

- inform clients and community members of the existence of and services provided by the other agency; and
- provide organizational literature to the other agency's staff, clients and/or community members; and
- provide training and technical assistance to the other agency's staff, clients and/or community members; and
- invite staff and volunteers to its events to disseminate information or conduct specific workshops, as appropriate.

Referrals between participants will be made in accordance with their respective eligibility criteria and policies, as well as program capacity. This agreement is non-binding upon either party and will be reviewed every two years. In addition, this agreement may be modified or terminated by either party at any time upon written notice.



WORRIED ABOUT TECH SAFETY?

CETA

CLINIC TO END TECH ABUSE

**Ask your FJC caseworker about the
Clinic to End Tech Abuse to discuss problems with:**

Location tracking

Securing online accounts

Harassment

Identity theft

Device security

Spyware/Stalkerware

Social media stalking

Securing email accounts

General privacy and security advice

Contact your caseworker for a referral!

Visit www.ceta.tech.cornell.edu for more information.

CETA Referral Guide

as of Fall 2022

Cornell's Clinic to End Tech Abuse (CETA) has limited capacity to meet with clients who are experiencing technology abuse. This guide aims to help you determine when and how to refer clients for an appointment with CETA. All clients referred to CETA must be over 18 years old.

Please remember that we are a volunteer-run service. Please communicate the limitations of our service to clients by reading the below information.

If a client is experiencing a high degree of distress that may present challenges for even a well-trained volunteer, please alert our admin team at [redacted] so we can help assign the referral to an appropriately trained staff member.

What a CETA Appointment Can Help With:

1. Possible ways an abuser might have access to the client's devices/accounts especially Apple devices, Android phones, Facebook, Instagram, Tiktok, and laptops.
2. Location tracking via electronic means, but **NOT by in-person sweeps**.
3. Suspicious installed applications
4. If their social media security and privacy account settings are set to protect their personal information (e.g., tagging, blocking, etc.)
5. Free licenses for Norton Anti-Virus or DeleteMe if their information is showing up on Google Search page.
6. Security implications of shared devices (children's devices, laptops left an abuser or by an abuser)

What a CETA Appointment CANNOT Help With:

- time-sensitive emergencies (e.g. an imminent escape).
- **online harassment**, sent from an abuser or from strangers
- in-person visits to scan homes or vehicles for tracking equipment
- removing accounts created by the abuser that impersonate or doxx the client.
- general technology issues that are not perpetrated by an intimate partner
 - e.g. client a lost phone, Internet not working, poor service
- identity theft including stolen SSN or other personal information extracted online
- non-consensual intimate images also known as "revenge porn".
 - all we can do is send a referral to other organizations usually legal or group counseling that specialize in this area.
 - If the client has the images in questions, they can file a report with <https://StopNCII.org> to prevent it from being shared.

Before referring a Client to CETA:

Due to CETA's limited capacity, we suggest you first try to help the client check for basic technology-related problems that they might resolve without needing a CETA appointment, such as:

- Have they checked and followed our [Tech Disconnect Short Form](#) or [Tech Disconnect Long Form](#)?
- **Password checks:** is it possible the abuser knows the client's or child(ren)'s password(s)? These actions may be visible to the abuser.
 - Have they tried changing their password(s), if the client feels safe doing so?
 - Have they tried turning on two-factor authentication, if the client feels safe doing so?
- **Wireless family plan:** does the client share a family plan with the abuser, which gives the abuser access to information about the client's device and account?

How to Refer the Client to CETA:

To request a CETA appointment, help the client fill out our intake form and we will contact them directly:

[referral links redacted]

Other Resources: Spyware Detection via Norton LifeLock Security App

Clients who are referred to CETA from a Family Justice Center (FJC) are able to get a free copy of Norton LifeLock's security app. This is an easy-to-use, commercially available app you can download via the Apple app store / Google Play store. It can detect apps that pose privacy or surveillance threats (i.e., spyware) and can also tell if the client's device is jailbroken/rooted. The FJC Director for your borough can tell you how to get a free copy of this security app for the client.

DeleteMe Subscription to help remove personal information from showing up on people search websites.

Clients who are referred to CETA from any organization are able to get a coupon code for a free year-long subscription to DeleteMe which will make a best-effort attempt at removing personal information such as names, phone numbers, and emails from Google search results. Please contact [redacted] for information about this.

B. Chapter 4: Service Delivery

- Intake Forms
 - CETA
 - MTC
 - TECCC

English



Default Question Block

Thank you for your interest in our service. Please use this form to give us more information about your needs. It should take 10 minutes or less. Note that most questions are optional and can be skipped if needed.

Which organization referred you?

- ☐ Anti-Violence Project
- ☐ Bronx FJC
- ☐ Brooklyn FJC
- ☐ Manhattan FJC
- ☐ Queens FJC
- ☐ Staten Island FJC

What is your caseworker's name?

What are your caseworker's phone number and email?

What name would you like us to use for you? (optional)

Block 1

Is it safe for us to email you?

- ☐ Yes
- ☐ No

If yes, what is a safe email address where we can contact you?

Is it safe for us to call you on the phone?

Please be aware that if the person you are concerned about has been able to touch your phone in the past, or if you are on a shared family phone plan with that person, it may be less safe to use your phone to talk to us.

- ☐ Yes
- ☐ No

If yes, what is a safe phone number where we can call you?

Is it safe for us to leave a voicemail?

- ☐ Yes
- ☐ No

Is it safe for us to send you text messages?

Please be aware that if the person you are concerned about has been able to touch your phone in the past, or if you are on a shared family phone plan with that person, it may be less safe to use text messages to talk to us.

- ☐ Yes
- ☐ No

If yes, what is a safe phone number we can use to send you text messages?

What are some safe days and times when we can call you to discuss your needs?

What are some days and times that would be convenient for a 60 minute phone consultation?

Block 2

Are you concerned about a **device**, such as a phone or computer? If so, what kind of phone or computer are you worried about? (You can choose more than one.)

- ☐ iPhone
- ☐ Android phone
- ☐ iPad
- ☐ Android tablet
- ☐ Laptop
- ☐ Desktop computer
- ☐ Other (please say)

Are you concerned about an **online account**, such as email or social media? If so, what kind of online account are you worried about? (You can choose more than one).

- ☐ iCloud
- ☐ Gmail / Google account
- ☐ Facebook
- ☐ Instagram
- ☐ WhatsApp

☐ Other (please say)

Please briefly explain the problems you are hoping we can help with.

Block 3

What languages do you speak fluently? (You can choose more than one.)

- ☐ English
- ☐ Spanish
- ☐ Mandarin Chinese
- ☐ Something else (please say)

What pronouns should we use for you?

- ☐ She/her/hers
- ☐ He/him/his
- ☐ They/them/theirs
- ☐ Something else (please say)
- ☐ Prefer not to say

How would you describe your race or ethnicity? (You can choose more than one.)

- ☐ American Indian or Alaska Native
- ☐ Asian or Asian American
- ☐ Black or African American
- ☐ Latinx/Hispanic
- ☐ Native Hawaiian or other Pacific Islander
- ☐ White
- ☐ Something else (please say)

Madison Tech Clinic uses Google Forms to power its referral form. The content of the form is reproduced below with specific links redacted.

Madison Tech Clinic Referral Form

This form is to be filled by the case manager with the survivor who is experiencing technology abuse, such as are being spied on, tracked, or surveilled by their abusive partner.

Please fill out the form as best as you can to give us basic understanding of the case. We will go over some of the questions in more details during the consultation.

Our capabilities (please read before submitting!)

We are a group of trained volunteers with technology expertise who conduct free, confidential consultations in partnership with local domestic abuse advocacy groups to help survivors who are facing stalking or harassment via technology. We provide support to survivors of intimate partner violence by scanning iPhones, Android phones, and tablets and auditing survivors' online accounts for issues that can impact their privacy and security.

While we are developing capabilities to scan laptops and smart devices, we are currently unable to assist with these devices. We also do not yet support procedures to gather evidence of abuse. As a policy, we do not assist in counter-surveillance such as spying on someone else or gathering information about them.

Email* (required):

Your answer

Which organization are you with?* (required):

Select from:

- ☐ DAIS
- ☐ Dane County DA's office
- ☐ Project Respect
- ☐ The Rainbow Project
- ☐ Rape Crisis Center
- ☐ ROSA

- ☐ Safe Harbor
- ☐ UNIDOS
- ☐ University Health Services
- ☐ UWisconsin Police
- ☐ Other: *please fill in* _____

Case manager's preferred name and pronouns:

Your answer

Case manager's contact information (email or phone number) (required)*:

Your answer

Client's preferred name or initials:

To preserve anonymity, we don't want to use your real name in our record. So please use a pseudonym or initials only.

Your answer

Client's pronouns:

Your answer

What does the client want the Tech Clinic to help them with?:

For example, are you observing any suspicious activity that could be connected to your devices? Do you worry that your device(s) is being used to track you? Or, do you just want to be cautious?

Your answer

Does the client own or use any of these devices? (Click all that apply.):

- ☐ Apple smartphone (iPhone)
- ☐ Android smartphone (Samsung Phone, Google Pixel, LG, Motorola, etc.)
- ☐ iPad
- ☐ Android tablet (Amazon Fire tablets, Samsung Galaxy Tab, etc.)
- ☐ Windows laptop or desktop
- ☐ Mac laptop or desktop
- ☐ Other: *please fill in* _____

If you selected an Android device above, what is the specific device? (E.g., Pixel 6):

Your answer

Does the client own or use any smart devices (besides laptops, tablets, or smartphones)? Which ones?:

"Smart devices" include smart speakers, smart smoke detectors, smart door locks, smart TVs, smart doorbells, WiFi routers as well as smart personal devices such as activity trackers and smartwatches. If you aren't sure if something is a smart device, feel free to put it here anyway.

Your answer

Is the client concerned about any of the smart devices mentioned above?:

Your answer

Is the client currently living with an abusive partner?:

☐ Yes

☐ No

Check all that apply to the client's status:

☐ Full custody of children

☐ Partial custody of children

☐ No custody of children

☐ Obtained restraining order against the partner

☐ Attempting to obtain restraining order against the partner

☐ Other:

Please go ahead and book a slot that best fits your and your client's availability using the link below: *[redacted URL. MTC uses Calendly to coordinate scheduling.]*

If none of the available time slots work for you, please specify a few time slots below.

Your answer

Is there anything else you want us to know?:

TECHNOLOGY-ENABLED COERCIVE CONTROL CLINIC
Referral Form

This form is to be filled out by an Advocate or other service provider while in discussion with a participant who is interested in attending the TECC Clinic. This form is used to prepare the clinic staff and volunteers for their upcoming appointment.

*At this time the TECC Clinic will only be accepting participants who are **18 years or older**.*

All referrals will be kept in [REDACTED] database. No identifying information will be released without written consent, unless required by court order or by our status as mandated reporters. As mandated reporters, we must report any threats made to harm oneself or others, as well as, child abuse or neglect.

REFERRAL GUIDELINES

1. To refer a potential TECC Clinic participant, please complete this form and send directly to [REDACTED] via email at [REDACTED] or Faxed to [REDACTED].
2. TECC Clinics are held on [REDACTED]. Referrals are accepted on a rolling basis. Referrals will be assigned from [REDACTED] before the upcoming clinic.
3. [REDACTED] will contact participants from 11am- 1pm, **from a blocked number**, on the Wednesday before the upcoming clinic to alert them of their time slot, provide them with the TECC clinic address and discuss how to best prepare for their appointment. Participants must be available for the phone call to confirm the appointment. [REDACTED] will call twice in a row, if the participant is unable to confirm the appointment during that call back time they will be placed on a waitlist for future clinics.
4. If the number of referrals is larger than the available appointments participants will be placed on a waitlist. [REDACTED] will contact those that have been identified as having time sensitive concerns first and then will contact participants sequentially from the waitlist.
5. If the upcoming clinic is full, the referring advocate will receive an automatic reply from the [REDACTED] email address. Referring advocates will be responsible for relaying that information back to the participant that has been referred.
6. Please include to the best of your knowledge, the level of safety concern with all participants that are referred.
7. [REDACTED] cannot be held responsible for any errors made that result in damaged property or compromises victims safety.
8. This form also acts as a release of information for the referring advocate and the [REDACTED] advocate to release and obtain information regarding the participant for coordination of services and safety concerns limited to involvement in the TECC clinic.

REFERRING ADVOCATE/AGENCY

Referring Agency:

Click here to enter text.

Date:

Click here to enter text.

| | | | | | |
|---|---------------------------|------|--------------------------------|----------------------------|---------------------------|
| Referring Advocate: | Click here to enter text. | | | Click here to enter text. | |
| Advocate Email: | Click here to enter text. | | Advocate Telephone: | Click here to enter text. | |
| "I have completed a safety plan with this client" | Click here to enter text. | | Advocate Signature: | Click here to enter text. | |
| TECC CLINIC PARTICIPANT INFORMATION | | | | | |
| Participant Name: | Click here to enter text. | | | | |
| Email: | Click here to enter text. | | Is it safe to send an email? | Click here to enter text. | |
| Telephone: | Click here to enter text. | | Is it safe to leave a message? | Click here to enter text. | |
| Alternative safe contact: | Click here to enter text. | | | | |
| Zip Code: | Click here to enter text. | DOB: | Click here to enter text. | Race: | Click here to enter text. |
| | | | | Gender Pronouns: | Click here to enter text. |
| Would the participant like to have an interpreter? | | | Click here to enter text. | If so, for which Language? | Click here to enter text. |
| <u>At this time childcare is not provided. Please talk with participants about alternatives for childcare.</u> | | | | | |
| Why does the participant want to come to the TECC Clinic? What specific problems does the participant want addressed at the TECC Clinic? (Describe and/or choose from list below) | | | | | |
| Click here to enter text. | | | | | |
| Please choose all that apply | | | | | |

| | |
|---|---|
| <input type="checkbox"/> Unwanted and/or constant texts <input type="checkbox"/> Threats to or the distribution of intimate images/photos (The Clinic legally cannot assist with intimate images of a minor) <input type="checkbox"/> Online Impersonation <input type="checkbox"/> Problems setting up new, secure accounts <input type="checkbox"/> Identity theft <input type="checkbox"/> Damaging reputation online <input type="checkbox"/> Group bullying through online forums <input type="checkbox"/> Webcams <input type="checkbox"/> Home systems | <input type="checkbox"/> Unwanted social media contact <input type="checkbox"/> Location tracking (via GPS, find my iPhone, etc.) <input type="checkbox"/> Unsecured/Stolen passwords <input type="checkbox"/> Access to accounts (without permission) <input type="checkbox"/> Key-logger and/or spyware (Programs or devices that record information typed into a computer/phone or web-sites visited. For example: stealing passwords by tracking what is typed into a keyboard) <input type="checkbox"/> Call/Text spoofing (using disguised/unknown phone numbers to call or text) <input type="checkbox"/> "Doxxing" (revealing personal identification or contact information) |
| Are there specific devices and/or online accounts that the participant wants to go through to ensure that they are safe and secure? | |
| Click here to enter text. | |
| Which operating system is participant using? (IOS, Android, Windows) | |
| Click here to enter text. | |
| How long has the participant been experiencing these concerns? | |
| Click here to enter text. | |

Are there any time-sensitive events/dates coming up? Does the participant have a particular reason they need assistance by a certain date?

[Click here to enter text.](#)

Is the participant interested in learning how to preserve evidence (saving texts, emails, voicemails, ect) for future use? Reasons to preserve evidence include family law action, a criminal case, a stalking incident log, and protection orders.

[Click here to enter text.](#)

Our technology volunteers come to us from many companies in Seattle. Are there any companies that would present a safety concern for the participant? (For example, does the person targeting/harassing the participant work at a technology company).

[Click here to enter text.](#)

RELEASE OF INFORMATION

I *Click here to enter participants name.* give my permission to **[REDACTED]** and (referring organization) to obtain and release information regarding coordination of services and safety concerns limited to my involvement in the TECC clinic.

*this release expires upon 3 months of signature

☐ Participant provided verbal consent

| | |
|---------------------------|---------------------------|
| Signature of participant: | Click here to enter text. |
|---------------------------|---------------------------|

| | |
|------------------------|---------------------------|
| Signature of advocate: | Click here to enter text. |
|------------------------|---------------------------|

| | |
|-------|---------------------------|
| Date: | Click here to enter text. |
|-------|---------------------------|

FOR TECC CLINIC TEAM ONLY

| | | |
|----------------|---------------------------|---------------------------|
| Date Received: | Click here to enter text. | Click here to enter text. |
|----------------|---------------------------|---------------------------|

| | | |
|--|---------------------------|---------------------------|
| | Click here to enter text. | Click here to enter text. |
|--|---------------------------|---------------------------|

C. Chapter 6: Technology Consultants

- Call for Consultants Flyer
- Interview Guide
- Rubric for Applicants
- Training Plan
- Guidebooks:
 - Onboarding New Volunteers
 - Technology Consultants

Volunteering for CETA

Thanks for your interest in volunteering for CETA. CETA was born out of research at Cornell Tech on tech abuse in intimate partner violence (IPV), and has been operating since November 2018. CETA is powered by volunteers who believe everyone should be free to use technology without fear of harm from abusive partners or others. We work directly with survivors to help determine if someone is using technology to harm them -- and what they can do to stay safe. We also facilitate cutting-edge research to understand how abusers can misuse technology.

This is a quick description of the volunteer experience and expectations around your involvement as a CETA volunteer. The next page has more information about our volunteer training program.

IPV survivors are called clients in this context. Clients are referred to us through our partnerships with the New York City Mayor's Office to End Domestic and Gender-Based Violence (ENDGBV) and the Anti-Violence Project (AVP). The ENDGBV is a municipal organization whose mission is to support survivors of not only IPV but other forms of gender-based violence. AVP provides anti-violence support for the LGBTQ+ and HIV-affected communities in New York City.

Our clinic model has evolved over time. Currently we help 10-20 clients per month. IPV support professionals (case managers, social workers, lawyers, etc.) submit a referral to us, and we assign a volunteer to be a case lead. The case lead schedules a call or otherwise reaches out to the client to ascertain what their technology concerns are and how we might help them navigate their situation.

Our work is a combination of remote and hybrid; we screen all clients with a remote appointment first, and offer in-person service on an at-capacity basis. We only help with technology issues; existing ENDGBV and AVP resources provide safety planning, legal assistance, housing assistance, etc.

New CETA volunteers proceed through a sequence of trainings on the clinic background and history, IPV, client-centered counseling, self-care, technology abuse, and CETA procedures. The trainings in total will require 10-12 hours spread across several (e.g., 4) sessions. After completing training, volunteers proceed to become shadowers, in which they listen in on consultations between more senior volunteers and clients. After that, volunteers graduate to active roles where they can assist more senior volunteers in client cases. Finally, the volunteer moves on to being a case lead. Throughout we emphasize volunteer well-being, and will gradually help you become comfortable doing the rewarding work of helping clients.

Right now we ask that volunteers, after training, can commit ~10 hours of time per month. We purposefully want you to be able to meaningfully contribute to CETA without impeding on your work, education, or other interests. Most activities happen during business hours (Eastern time zone) Monday through Friday, with case leads running scheduling. The primary work is helping with client cases, for example, helping clients diagnose whether their email or social media accounts are compromised, helping them check for malicious spyware that may have been installed on their phone, understanding options for reporting harassment online, and more. We provide training on the most frequently encountered issues, and have resources for helping volunteers understand security concerns so that they can, in turn, help inform clients about their options.

Finally, in addition to working with clients, there are potential opportunities in CETA to get involved in academic research, legal advocacy, software development, resource development, and external tech training programs for IPV stakeholders.

New Volunteer Training

Our training program focuses on equipping all volunteers, regardless of prior background, with basic knowledge of IPV and gender-based violence, self-care and secondary trauma, trauma-informed counseling, common types of technology abuse, and how to help clients secure their technology. The training is broken down into the following four sessions, with each session lasting 2-3 hours:

Part 1. Introduction to CETA (2 hours)

- Background and history of CETA

- Mission, values, policies

- Organizational structure

 - CETA leadership and administration

 - Key partner organizations

 - Broader IPV-tech community

 - Volunteer corps

- Core CETA activities

 - Client services

 - Research

 - Legal/policy advocacy

 - Tech tools and software development

- Clinic settings and procedures

 - Case management and lifecycle

 - Data collection and record keeping

 - Team meetings and communication

- Volunteer expectations, limitations, boundaries, safety, anonymity

Part 2. IPV 101 (3 hours)

- Dynamics of IPV and gender-based violence

- Coercion, power and control

- Stalking

- Effects of trauma

- Myths and realities

- Safety planning

- Secondary trauma and self-care

Part 3. Talking with Clients (2 hours)

- Trauma, bias, and privilege

- Trauma-informed approaches

- Active listening and validating

- Working with an interpreter

Part 4. Discovering and combating tech abuse (3 hours)

- Client case management and appointment flow

- Discovering tech abuse -- questions to ask

- Conducting device and account checkups

- Spyware checks

- Follow up and post-appointment communication

- Getting additional tech support



COME JOIN CETA!

Cornell's Clinic to End Tech Abuse has opened volunteer applications!

Are you:

- looking for a rewarding volunteer opportunity?
- skilled and/or comfortable with technology?
- passionate about helping at-risk, marginalized communities?

If so, read on to learn more about CETA, where you can use your skills to help safeguard the lives of domestic violence survivors and [submit a volunteer application here!](#)

Cornell Tech, part of Cornell University, offers the groundbreaking [Clinic to End Tech Abuse \(CETA\)](#). Our volunteers meet directly with domestic violence survivors, remotely or in-person, to help survivors detect and prevent technology-related abuse.

Experiences from our clinic also help our research at Cornell to create a better understanding of tech abuse and advocate for laws that protect survivors. You can [apply here!](#)

Volunteering with CETA is an opportunity to:

- Join a **community** of friendly, supportive volunteer advocates!
- Receive training on **domestic violence, technology-related abuse**, and **advocacy** skills.
- **Directly** help domestic violence survivors deal with tech abuse.
- Contribute to cutting-edge **research**.

Please note: This volunteer role is unpaid.

Time commitment: As a volunteer, you will need to complete an interview process and approximately 10 hours of remote training via Zoom. Volunteers also

spend time "shadowing" where you will listen in as more experienced volunteers help clients.

After you complete your training, we would expect you to be available for **roughly 10 hours per month** to meet remotely with domestic violence survivors and attend clinic meetings.

Qualifications: We encourage applications from two types of volunteers: (1) those with strong computer science or technology-related qualifications, and (2) those who do not have a technical background but are comfortable navigating privacy settings and have other relevant skills.

All applicants should have:

- An understanding of basic computer security and privacy concepts, or a willingness to learn.
- The ability to explain technical concepts to people with little technical knowledge clearly, simply, and respectfully.
- Empathy, strong listening skills, and strong organizational skills.
- A commitment to diversity, equity, inclusion, human rights, and being a team player.
- **(Plus)** Fluency in a language other than English, although not required.

We currently work with survivors in New York City, but you can be based anywhere. Please apply by completing our [application form](#).

[Interviewer introduces themselves, describes what the interview will entail]

- Why are you interested in volunteering for the clinic?
 - If self-disclosure of personal experience with IPV/violence: *I'm so sorry to hear that. How do you feel your own personal experience would affect your ability to work with clients at CETA?* **Flag: composure --ability to cope with triggering materials, do you have support**
- What prior experience do you have working with vulnerable populations, with women's rights or civil rights movements, or on other social justice issues?
- How would you describe your level of technical ability? For example, are you comfortable with or have formal experience in navigating and learning a new and unfamiliar app or platform? Computer science background? Computer security background?
 - *Flag--should be at minimum very comfortable exploring settings or learning a new platform*
- Do you have experience explaining technical issues to lay audiences? What do you think are important considerations when doing this?
 - recognition that they might be embarrassed, use analogies/metaphors from other things, help build a mental model and understand their current mental model, and not overload with unnecessary details (appropriate depth)
- *In your work at CETA, it's not uncommon for clients to share stories about their own abuse history. If someone were to share this type of story or becomes emotional how would you respond?*
 - *Flag: we don't want to scare people off but at the same time, this is the reality. If someone is visibly freaked out by even the idea of this, they're probably going to have a hard time.*
--empathetic but need training, not sure what 'right' thing to say is but want to give them space.
- *[Optional--if candidate seems unsure of qualifications] When thinking about talking with survivors of IPV about their technology issues which aspects of this do you feel the most comfortable with? the least comfortable with?*
- Client appointments typically take 1.5-2 hours. How much flexibility would you have to attend a call with clients during EST working hours? Do you feel able to commit to 5-10 hours a month (1-2 a week?) to CETA?
- Do you speak any languages other than English fluently that you would feel comfortable conducting an interview with someone in?
- Questions for me?

| Criteria | None | Some | Good | Great | Why? | Rubric explanatic |
|---|-------|-------------|--------|-----------|------|-------------------|
| Prior relevant counseling, mentoring, or advising experience, or work with vulnerable groups | | | | | | |
| Comfort with talking to abuse survivors or hearing disclosures of abuse | | | | | | |
| Existing understanding/experience in tech; computer privacy/security issues | | | | | | |
| Ability to communicate clearly, concisely, and appropriately as demonstrated during interview | | | | | | |
| Willingness and ability to make time commitment and enthusiasm for involvement | | | | | | |
| Other relevant skills or background (e.g., social work, psychology, law, program evaluation, training delivery, communications) | | | | | | |
| Overall impression of candidate as a CETA volunteer | | | | | | |
| | Total | 0 | 0 | 0 | 0 | |
| Bonus | No | Semi-fluent | Fluent | Language? | | |
| Fluency in languages other than English | | | | | | |
| Flags and concerns? | | | | | | |

CETA Volunteer Handbook

This is a living document. Feel free to make comments and suggestions directly on the document or send them to CETA leadership via Slack or email. Please also let us know if you find any missing or broken links.

Most recent major revision: September 2022

Table of Contents

1. [Quick Summary: Volunteering for CETA](#)
2. [Volunteer onboarding checklist + useful links](#)
3. [CETA's Mission, Values and Policies](#)
4. [New volunteer training](#)
 - a. [Part 1: Introduction to CETA](#)
 - b. [Part 2: IPV 101](#)
 - c. [Part 3: Talking with Clients](#)
 - d. [Part 4: Discovering and Combating Tech Abuse](#)
 - e. [Part 5: Cornell IRB training](#)
 - f. [Part 6: Evidence Documentation + Legal Considerations](#)
5. [Communication, Operations, and Admin](#)
 - a. [Team Meeting](#)
 - b. [Slack](#)
 - c. [Email](#)
 - d. [Cornell NetIDs](#)
 - e. [Box](#)
 - f. [Google Drive](#)
 - g. [Zoom](#)
 - h. [RingCentral](#)
6. [Security Procedures](#)
7. [Self-care and Volunteer Wellness](#)
8. [Other CETA activities you can get involved in](#)
 - a. [Creating CETA resources](#)
 - b. [Tech safety trainings and webinars](#)
 - c. [Legal/policy reform](#)
 - d. [Developing software, analytical tools, and data infrastructure](#)
 - e. [Academic research](#)
9. [Leaving CETA](#)

1. Quick Summary: Volunteering for CETA

Thanks for your interest in volunteering for CETA. [CETA](#) was born out of [research](#) at Cornell Tech on tech abuse in intimate partner violence (IPV) and has been operating since November 2018. CETA is powered by volunteers who believe everyone should be free to use technology without fear of harm from abusive partners or others. We work directly with survivors to help determine if someone is using technology to harm them -- and what they can do to stay safe. We also facilitate cutting-edge research to understand how abusers can misuse technology.

This handbook aims to provide important information relevant to your experience and involvement as a CETA volunteer, including training, roles and expectations, links to important resources, and more.

IPV survivors are called clients in this context. Clients are referred to us through our partnerships, currently with the New York City Mayor's Office to [End Domestic and Gender-Based Violence](#) (ENDGBV) and the Anti-Violence Project (AVP). The ENDGBV is the municipal organization whose mission is to support survivors of not only IPV but other forms of gender-based violence. The Anti-Violence Project is an anti-violence organization dedicated to serving specifically the LGBTQ+ and HIV-affected communities.

Our clinic model has evolved over time. Currently, we help ~10-25 clients per month. IPV support professionals (case managers, social workers, lawyers, etc.) submit a referral to us, and we assign a volunteer to be a case lead. The case lead schedules a call or otherwise reaches out to the client to ascertain what their technology concerns are and how we might help them navigate their situation.

Most of our appointments are remote, but we offer in-person meetings on an ad hoc basis. Criteria for meeting with clients in-person is based on (1) availability of consultants located in the New York City area, (2) potential benefit to the client, and (3) the capacity of the partner agency to host an in-person meeting.

We only help with technology issues; our partner agencies provide referrals for clients to access safety planning, legal assistance, housing assistance, etc.

New CETA volunteers proceed through a sequence of trainings on the clinic background and history, IPV, client-centered counseling, self-care, technology abuse, and CETA procedures. The trainings in total will require 10-12 hours spread across several (e.g., 4) sessions. After completing training, volunteers proceed to become shadowers, in which they listen in on consultations between more senior volunteers and clients. After that, volunteers graduate to active roles where they can assist more senior volunteers in client cases. Finally, the volunteer moves on to being a case lead. Throughout we emphasize volunteer well-being, and will gradually help you become comfortable doing the rewarding work of helping clients. We provide refresher trainings in our group meetings and 1:1 or small group orientations as volunteers transition between roles.

We ask that volunteers, after training, can commit ~10 hours of time per month; approximately one appointment per week. We purposefully want you to be able to meaningfully contribute to CETA without impeding your work, education, or other interests. Most activities happen during business hours (Eastern time zone) Monday through Friday, with case leads running scheduling. The primary work is helping with client cases, for example, helping clients diagnose if their email or social media

accounts are compromised, helping them check for malicious spyware that may have been installed on their phone, understanding options for reporting harassment online, and more. We provide training on the most frequently encountered issues, and have resources for helping volunteers understand security concerns so that they can, in turn, help inform clients about their options.

Finally, in addition to working with clients, there are potential opportunities in CETA to get involved in academic research, legal advocacy, software development, resource development, and external tech training programs for IPV stakeholders.

2. Volunteer Onboarding Checklist

- Fill out and email either [redacted] ([redacted]) or [redacted]
 - a Volunteer Profile form
- Review Policies 6.3 (Consensual relationships) & 6.4 (Prohibited Discrimination, Bias, and Harassment) and 6.5 (University Volunteers)
- Join CETA's Slack Team and ask to be added to the #clinic-practice channel
- Add your information to the CETA personnel roster. We will request a Cornell NetID login for you, and login instructions will be sent to the email you provide on the roster.
- Add your name and bio to the CETA Member Gallery. Feel free to have a flick through to get familiar with faces.

Additional Useful Links

- [Website](#) (and [public CETA resources](#))
- Slack Team
- Leadership:
 - [redacted]
- [Weekly team meeting agenda + Zoom info](#)
- [Personnel roster + contact information](#)
- [Case management & appointment scheduling spreadsheet](#)
- [Client FAQs and Common Tech Topics for CETA Volunteers](#)
- [Guide for Case Leads](#)
- [Academic Research Website](#)

3. CETA's Mission, Values, and Policies

CETA's mission is to end tech abuse. We guide our work & partnerships by the following principles:

- We believe everyone should be free to use technology without fear of harm from abusive partners or others.
- We believe and respect survivors. When we provide them with advice, we aim to help give them the information they need to make their own decisions. We honor the fact that survivors know their own situations best.
- We aim to serve survivors from all walks of life and are committed to being inclusive and culturally competent. We are sensitive to the needs, desires, and perspectives of all groups of people.
- We embrace human rights and believe everyone deserves equal rights and dignity.
- We recognize intersectional discrimination and abuse, and seek to end them.
- We are collaborative and strive to create strong, equal partnerships with other organizations. We value the expertise of all IPV professionals -- and survivors.
- We believe larger societal problems such as racism, economic injustice, misogyny, homophobia and transphobia, ableism, and agism contribute to intimate partner violence. We expect everyone involved in CETA to embrace the importance of equality and justice.
- We believe accountability is an important part of justice for survivors. We are committed to ensuring that no one uses involvement with CETA as a way to avoid accountability for abuse.

Team Values and Guiding Principles

- Volunteers' well-being comes first
- We don't expect perfection – we value skills, commitment, empathy, & team spirit
- We believe and respect the survivors
- We empower survivors to make their own decisions
- We collaborate with and support each other
- We are patient, professional, and thorough
- We are sensitive to the needs, desires, and perspectives of all groups of people, and we respect everyone's equal rights and dignity
- We respect and value everyone who helps make this project a success, such as support workers and interpreters

CETA and Cornell University Policies

CETA is a part of Cornell University and ascribes to Cornell's policies, including:

- Policy 6.3: Consensual Relationship Policy
- Policy 6.4: Prohibited Bias, Discrimination, Harassment, & Sexual & Related Misconduct
- Policy 6.5: University Volunteers
- Volunteer agreement

Important: CETA has a zero-tolerance policy for sexual harassment, bigotry, and gender or race-based bias. Consensual romantic relationships between volunteers should be disclosed to CETA leadership.

4. New Volunteer Training

Our training program focuses on equipping all volunteers, regardless of prior background, with basic knowledge of IPV and gender-based violence, self-care and secondary trauma, trauma-informed counseling, common types of technology abuse, and how to help clients secure their technology. The training is broken down into the following four sessions, with each session lasting 2-3 hours:

Part 1. Introduction to CETA (2 hours)

- Organizational structure
 - CETA leadership and administration
 - Volunteer corps
 - Key partner organizations
 - Mission, values, policies
- Background and history of CETA
 - Past and ongoing research studies
- Clinic settings and procedures
 - Case management
 - Appointment flow
 - Team meetings and communication
 - Data collection and record keeping
- Volunteer roles and responsibilities
 - The Shadower Role
 - The (Second) Consultant Role
 - The Case Lead Role
 - Volunteer limitations, boundaries, safety, anonymity
- Other core CETA activities
 - Creating resources for CETA
 - Legal/policy advocacy
 - Tech abuse trainings and webinars
 - Developing software, analytical tools, and data infrastructure
 - Academic Research

Part 2. IPV 101; Secondary Trauma and Self Care (3 hours)

- Basic introduction to IPV
- Secondary trauma and self-care

Part 3. Talking with Clients (2 hours)

- Trauma, bias, and privilege
- Trauma-informed approaches
- Active listening and validating
- Working with an interpreter

Part 4. Discovering and combating tech abuse (3 hours)

Client case management and appointment flow
Common types of tech abuse
Understand-Investigate-Advise framework
Follow up and post-appointment communication
Getting further tech support

Part 5: Evidence Documentation + Legal Considerations

It is common for clients to want our assistance with collecting evidence for court cases. On occasion, they will also ask for us to provide expert or witness testimony, in writing or in person, describing what we found during a consultation. This section discusses our official guidance for navigating such requests.

Encourage self-documentation: We do not retain evidence or documentation (e.g. screenshots, records of account activity, log-in information) of personal data encountered during an appointment. However, if we find unusual or suspicious activity that corroborates the idea that the abuser was accessing or tampering with the client's devices or accounts, we can encourage them to document it themselves by taking a screenshot or saving records to auxiliary storage. This serves the dual purpose of preventing CETA volunteers from direct involvement while still allowing the client to preserve evidence.

Provide written summaries: Typically we send a post-consultation summary, detailing what steps we took and what we found. With the client's permission, we can also send this information to their caseworker. This summary provides an anonymized record of what we found and is usually sufficiently comprehensive of a client's activities with CETA.

Requests for expert testimony: We do not consider this within the scope of services provided at CETA, and would never ask nor expect a volunteer to assent to such a request. If you receive such a request, you may let the case worker know that the client asked for a documentation of service for legal purposes and remind them that this is not within our ability. You can and should feel free to contact the leadership team for additional support.

A note from our lawyers: We cannot 100% guarantee that CETA will never be subpoenaed to testify in a court case, as the clinic does not hold a confidential legal status shielding us from subpoenas. However, this has never happened in the history of CETA. We recommend the above steps (encouraging self-documentation, providing written summaries, and communicating the scope of our services) because, in addition to being good practice, they are usually sufficient to prevent the need for individual testimony.

5. Communication, Operations, and Admin

CETA Team Meeting

We hold bi-weekly team meetings / office hours that we use to discuss CETA activities, debrief on cases, do ad-hoc or refresher trainings, or check-ins with volunteers. We **strongly**


encourage all CETA members to join the meeting if they can. Please let us know if you have a conflict. Each Friday following the team meeting, we will send out a newsletter summing important news and sharing any recordings that happened during the meeting; if you cannot make the meeting, please ensure you read the newsletter.

When: The agenda, linked below, has the next date of each group meeting at the top. Currently they are every other Tuesday at 4pm EST. Agenda + Zoom

Slack

We have a Slack team that we use for the bulk of CETA communication, including letting people know about upcoming appointments to sign up for, discussing issues that arise, asking questions about cases/appointments, asking for additional support with tricky tech abuse problems, coordinating backchannel communications during appointments, and more.

Do not post any identifying client information on Slack (use case IDs instead).

 **Slack Etiquette:** We encourage everyone to set their display name to whatever they are comfortable being called. Likewise, we as a community will endeavor to use those names unless directed otherwise. We also encourage everyone to add their pronouns (although we do not require it), and to make a habit of glancing at each other's pronouns when writing messages/tagging each other on Slack. This information is also in our Members List resource, but the easy convenience of Slack display names is especially helpful. To change your display name, click on your icon in the top right-hand corner, and select **Profile**. Then click **Edit** next to your name, and make the changes in **Display Name**. You also have the option to add a phonetic pronunciation of your name if desired.

Slack Team: link (we will add you)

Ask to be added to **#clinic-practice** and feel free to explore other channels. You can browse the other channels by hovering over "channels" in the side bar and clicking on the + icon. Some useful ones to join:

#advocacy legal and policy advocacy discussion

#techsupport open channel for asking questions about technology issues encountered with clients or in other places (as opposed to clinic-practice which is limited to volunteers)

#writtenguides for developing guides published on our website

Email

We use CETA's volunteer email listserv for announcements and important communication.

Listserv: [redacted] (we will add you)

Case leads are also assigned a CETA-specific email (e.g., [redacted]) and RingCentral phone number for communicating with clients/case workers. Information about using these properly is in the case lead guidance. **Do not use personal email accounts for communicating with clients.**

[Cornell NetIDs](#)

All CETA volunteers will receive Cornell NetIDs that provide access to Cornell licensed services and software products, e.g., email, Zoom, Box, RingCentral. We will request NetIDs for you. However, note that it can take some time for NetID requests to be approved, so we also have short-term workarounds (e.g., guest access to Box files for your own email address). Ask us if you're confused or need anything.

[Box](#)

We use Cornell-licensed Box for case management and client data, including data related to specific client cases (e.g., notes, recordings) and client-related research data (e.g., coded transcripts of client interactions). We control access to Box carefully, granting access to specific volunteers and specific files on a case-by-case basis.

[Google Drive](#)

We use Google Drive for all non-client specific data and documents, such as training slides, clinic resources, academic papers, logistics, etc. Our access policy for Google Drive is fairly liberal and may include CETA volunteers, students, interns, internal and external collaborators, and others. **Do not upload or store any client data to Google Drive** (and if you find client data there, please let us know).

Case and appointment tracking: spreadsheet [redacted]

[Zoom](#)

We use Cornell-licensed Zoom for internal communication (i.e., team and 1:1 meetings), internal and external trainings (e.g., webinars), client appointments, etc. For non-client communications (e.g., meetings) you can join the Zoom meeting from any account.

For client appointments, we have a CETA-specific Zoom account. As a CETA volunteer, you will receive access credentials when necessary to participate in client appointments.

[RingCentral](#)

We use Cornell-licensed RingCentral to call and text clients from a "regular" phone number. RingCentral is a convenient option for calling a client to set up an appointment. It also provides conference call functionality that should work with remote language interpretation services should clients need them.

Case leads will receive a Cornell RingCentral account with an assigned, unique, phone number.

6. Security Procedures

CETA handles a variety of highly sensitive data. To provide service, volunteers must handle client PII (personally identifiable information) such as names, telephone numbers, and email

addresses. Details of client cases may also be quite sensitive, with identifying information (what applications or devices a client uses, the particulars of the technology issues they experienced). Finally, for research purposes we often audio record consultations.

It's everyone's responsibility to safeguard client information. A leak of sensitive information such as a transcript onto the public internet would be a disaster of the highest order.

As implied in the previous section, CETA handles two types of data: client specific and non-client specific.

Client-specific Data

Client-specific data should only be stored on Box, in a client case folder. Examples include:

- Client case notes
- Call recordings

Note that client contact information is **not** stored on Box. Explicit client PII (name and contact info) is stored only in a case lead's CETA email address (e.g., [redacted]). **Never save it anywhere else, and never post any information on Slack.** If another case lead needs access to it, you must forward this information to their CETA email. Do not use personal or other work email accounts for communications with clients.

Recordings should only be stored long term on Box, in a client's case folder. If you make a recording locally on your computer, upload it immediately to Box after the consultation, and then delete the local copy. Ensure it is removed from any trash bin.

Client case notes should be stored only on Box. If you take notes on a piece of paper, or with a local text editor on your computer, you should transcribe these to the case folder case notes document after the call and destroy/delete the local physical/digital notes.

Client-specific data must be accessed only via your Cornell NetID, which by policy must have a strong password (do not reuse passwords from your other accounts) and with 2FA enabled. You must also be responsible for ensuring any device you use to access client-specific data remains free of malware; consider installing anti-virus software, be vigilant for phishing emails, and be careful about installation of software on the device.

Non Client-specific Data

When asking for support with a case on Slack, use the client case number. You can ask about technology issues faced by a client, but avoid revealing any client-specific information. If in doubt about what is appropriate to share, ask on #clinic-practice.

Our Google Drive data is a mix of public information (such as technology guides) and more sensitive documents. The sensitive files are:

- **Appointment and case tracker.** This does not include client identifiers, but should nevertheless never be shared outside CETA.

- **CETA personnel roster.** This contains information about CETA volunteers that we should not widely share for volunteer privacy and safety.

Do not share links to these files with anyone outside CETA. If you find you need access to these documents, let us know what email address you plan to use and we will grant you access.

You may access Google drive using your personal email accounts, but any account that has access should have a strong password and have 2FA turned on.

7. Self-care and Volunteer Wellness

As covered in the volunteer training, working with IPV survivors can lead to secondary trauma. Volunteer well-being is paramount. We encourage all volunteers to practice self-care, and to reach out should they ever be feeling symptoms of secondary trauma (e.g., being exhausted, feeling depressed or overwhelmed, etc.). You can always message or email the CETA leadership (Nicki or Tom) as well as other volunteers to chat. Sometimes just talking about difficult cases can be helpful to process them. We also encourage you to come discuss with CETA leadership how you're feeling, since we may want to scale back your workload temporarily or otherwise adjust your CETA volunteer experience to make sure we avoid burnout.

8. Other CETA activities you can get involved in

Creating CETA Resources

CETA's website provides a collection of materials, tools, and resources that our volunteers have created to help survivors, support workers, and others discover and address tech-related risks (<https://www.ceta.tech.cornell.edu/resources>). Many of these are step-by-step and how-to guides for checking and managing specific apps or platforms.

All resources are publicly available and free for anyone to download and use. We often hear from other organizations that are using our resources in their work with survivors. We also frequently use them in our own work with clients.

We maintain a list of new resources that we want to create and we encourage volunteers to also propose new resources they think would be useful -- either internally, externally, or both. For example, creating a new step-by-step guide to check security and privacy settings for a specific app might take a few hours. **Please let CETA's leadership know** if you are interested and have time to devote resource creation.

Tech Safety Trainings and Webinars

In addition to meeting with individual clients, CETA's volunteers also deliver external tech trainings and webinars that aim to equip support workers, case managers, and survivors with basic knowledge about tech safety and recognizing tech abuse.

Since the start of the COVID-19 pandemic, all external trainings have been administered as webinars via Cornell-licensed Zoom. Organizations interested in receiving training often reach out to us and ask us to present to their group and, depending on volunteer time and interest, we accommodate their requests if we can. Webinars typically involve two volunteers and last 1-2 hours. We have already created training materials that can be reused/adapted to accommodate different groups, depending on the audience targeted (although we could always benefit from more). **If you are interested in participating**, feel free to respond to periodic requests on Slack about upcoming trainings we're running, or speak to CETA's leadership about your interest.

Legal and Policy Reform

We advocate for better legal/policy protections for IPV survivors at both federal and state levels. For example, we led a letter to Congress from 10 organizations calling for a law giving abuse survivors throughout the US a right to get out of phone plans they share with their abusers. This led to the [Safe Connections Act](#) in the US Senate. We are also working with NY State Senators to propose similar legislation in New York State.

Nicki and Tom are not lawyers or policy experts; we rely on enthusiastic volunteers to lead this work. We have a channel -- **#advocacy** -- on our Slack team for discussing CETA's advocacy work. Please join this channel if you are interested in following or participating. Please also **let us know** if you have new ideas/expertise in this space or capacity to lead new efforts.

Developing software, analytical tools, and data infrastructure

We also do substantial technical work. There is always room for people interested in learning or flexing technical skills to help the clinic run more efficiently, and to help us create a platform for IPV research. Current projects include:

- Building a proper infrastructure for the clinic -- data pipelines, CMS, frontends, integrations, everything. To get involved, DM [redacted] on Slack with a brief description of your experience and interests in at least one of the following:
 - Backend / frontend / full-stack web app development. We're building on Docker / Node / Express / Sequelize / Postgres / React.
 - Web interface design
 - Data engineering
- Building tools to help researchers (both ourselves and others) better analyze the data we produce in every client case. To get involved, DM [redacted] on Slack with a brief description of your experience and interests in at least one of the following:
 - NLP
 - Data engineering
 - Qualitative / interpretive analysis (esp. grounded theory)

Academic research

Nicki and Tom also run an active academic research group studying the role of technology in IPV. This includes academic research on CETA's work as well as a range of other relevant projects that are more tangential to CETA. You can peruse the academic research [website](#) to read papers we have published and learn about our research projects. Talk to Tom and Nicki if you're interested in getting involved in academic research projects.

9. Leaving CETA

Of course, we understand that you will probably not be able to work as a CETA volunteer forever. When the time comes for you to move on, we ask that you try to give us as much notice as you are able---at least a few weeks and ideally several months---so that we have time to plan and distribute the workload among remaining volunteers. Our priority will be to avoid the need to cancel client cases/appointments or other things (e.g., external trainings) that we have committed to, as well as make sure that none of our volunteers are overburdened by the need to cover extra work at the last minute.

As soon as you know that you intend to end your volunteer relationship with CETA, please email CETA leadership (Nicki and Tom) to let us know and provide your anticipated end date. You are not required to tell us your reasons for leaving (although, of course, we would welcome knowing them). We will thank you for your valuable contributions and wish you well in future endeavors!

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

CETA Case Lead Guidance V2

Updated Spring 2022

This is a revised version of the case lead guidance, based on [redacted]'s original version but incorporating feedback from volunteers who have been through the transition from consultant to case lead. While some sections have been modified, one thing hasn't: ***please*** communicate with the broad team on the **#clinic-practice**, **#case-leads**, or directly with the leadership group on Slack as new problems come up!

This document is long because it is close to (although never quite) comprehensive. You may have picked up on much of this during your time shadowing/consulting. However, I strongly recommend reading at least the first three sections before you begin leading cases and the rest as needed.

Quick Links:

Scripts for Emails/Text/Phone:

[Initial Contact: General Protocol](#)

[Scheduling Via Email \(script\)](#)

[Scheduling Via Phone \(script\)](#)

[Sending A Text/Leaving A Voicemail \(script\)](#)

[If The Client Doesn't Respond \(script\)](#)

[When The Client and Case Worker Don't Respond \(script\)](#)

[Send A Discharge Email To The Caseworker \(script\)](#)

[Help! My Client Didn't Provide a Safe Phone Number! \(script\)](#)

[Help! My Client Chose a Zoom Appointment!](#)

Contact numbers and Interpreter Account Information:

[Key Contact Information](#)

[Interpreter Services + Language Competencies](#)

[Using the Interpreter Service:](#)

Table of Contents (full)

[Quick Links:](#)

[Scripts for Emails/Text/Phone:](#)

[Getting Started: Setting Up](#)

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

[Accessing Your Secure Cornell Inbox](#)

[Accessing Your RingCentral Number](#)

[Accessing The Secure Zoom Account](#)

[The Case Tracker](#)

[Thinking About Your Name](#)

[Communicating Your Availability](#)

[Key Contact Information](#)

[CETA Leadership](#)

[Family Justice Center Leadership](#)

[Receiving A Case](#)

[Deciding How To Handle A Case](#)

[Interpreter Services + Language Competencies](#)

[Using the Interpreter Service:](#)

[Scheduling an Appointment](#)

[A Note on Scheduling + System Oriented Trauma](#)

[System-Oriented Trauma](#)

[Initial Contact: General Protocol](#)

[Help! My Client Didn't Provide a Safe Phone Number! \(script\)](#)

[Help! My Client Chose a Zoom Appointment!](#)

[Scheduling Via Email \(script\)](#)

[Scheduling Via Phone \(script\)](#)

[Sending A Text/Leaving A Voicemail \(script\)](#)

[If The Client Doesn't Respond \(script\)](#)

[When The Client and Case Worker Don't Respond \(script\)](#)

[Setting up the appointment](#)

[Conducting an Appointment](#)

[During The Appointment](#)

[Wrapping Up An Appointment](#)

[Follow Up Appointments](#)

[Closing A Case](#)

[Post Consult Communication \(PCC\)](#)

[Send A Discharge Email To The Caseworker \(script\)](#)

[Norton Referrals](#)

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

Getting Started: Setting Up

If you've completed a pseudo-lead appointment (e.g. handled a call from start to finish with backup), then congratulations: you've already cleared one of the most important hurdles of being a case lead! Many of the remaining differences between acting as a case lead versus a consultant are administrative. **You are now responsible for client PII, scheduling, and communicating the status of the case via the case and appointment trackers.** With these new responsibilities come some new tools and considerations, detailed below.

Accessing Your Secure Cornell Inbox

New case leads are assigned a secure Cornell Box in the format of [redacted]. **This email is anonymized for your safety and the clients.**

- 1) Log into your NetID (*redacted*) email at outlook.com using SSO.
- 2) Click on your initials in the top right corner to open a drop down menu (see picture).
- 3) Select "Open another mailbox" and type in your id. There is no need to add <at> cornell.edu. You can bookmark it for quick access later.

Accessing Your RingCentral Number

You are also assigned a RingCentral number. The RingCentral number is used for calling or texting clients (and/or caseworkers) usually to schedule an appointment and sometimes to conduct an appointment (see [Conducting an Appointment](#) for instructions).

! By default, your RC number voicemail includes your name, and client texts/voicemails are forwarded (with PII) to your non-secure e-mail. We highly recommend changing the voicemail (instructions below) before you use your number to call clients and require changing the notification settings.

Signing in: You can download the app to your phone or access RC from the web. To log in from the web, go to <https://login.ringcentral.com/>. Click on **Single Sign-on (SSO)** and authenticate your NetID.

! Change your voicemail message: After logging in, click on **Settings >>Messages**. Below the "Voicemail Greeting" prompt, click on **Edit**. Record a custom voicemail message. **Do not**

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

mention your name, CETA or Cornell in the voicemail message. An example voicemail is: “Hi this is <name>, leave a brief message and I’ll try to get back to you as soon as possible.”

! Change your notification settings: By default, RingCentral will forward texts and voicemail notifications, including client PII, to your NetID account. To change, you need to log into the **Administrator Portal** (this is different from the **app**) at <https://service.ringcentral.com>. Once in the portal, click on "Settings", and then "Notifications" in the left hand bar. Here, you can either uncheck email notifications altogether, or keep them on but send them to your tech_clinicXX

| | By Email | By SMS |
|--------------------------|-------------------------------------|--------------------------|
| Voicemail Messages | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Received Faxes | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Missed Calls: | <input type="checkbox"/> | <input type="checkbox"/> |
| Fax Transmission Results | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Received Text Messages | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Send Notifications to
Email

address (see above). **Do NOT** change the email address under **User Details**, only the one under **"Send Notifications to:"**. You will not be able to log back in if you change the User Details one.

Accessing The Secure Zoom Account

Similar to the secure email, the secure Zoom account is used to create anonymized meetings. [The Zoom](#) log-in credentials can be found on Box here [redacted]. (Need access? Contact leadership!).

Being booted out of the Zoom during an active session will **not** end an active meeting or remove you from the call. You will be able to continue hosting the active call while logged out as a Zoom zombie. Nonetheless, **we recommend logging into Zoom with your regular NetID via SSO, which will allow you to add your NetID as an alternate host when creating appointments in the shared secure Zoom.**

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

The Case Tracker

Up until now, you may have been blissfully ignorant about the case tracker. The case tracker is where case leads (you!) leave notes about attempts to contact the client, completed appointments, needed follow ups, and discharges. **It is important to keep us (the leadership team) updated in the case tracker, and if you don't, we ([redacted]) will unapologetically send you relentless e-mails and Slack messages.** Responding to those messages counts as an update, as we will update the case tracker *for you* if you respond. **The case tracker is our main point of reference for ensuring that our clients are receiving a care. Be warned, we will assume that a blank case tracker means that you have not contacted the client and act accordingly.**

Thinking About Your Name

Case leads have much more direct contact with clients than seconds or shadowers. Having a first name to share with a client can help build rapport and prevent awkwardness, especially when writing emails or leaving voicemails. However, not all people are comfortable using their actual name. While some of us still choose to use our real first names, we encourage you to think carefully about your personal boundaries, and consider creating a pseudonym. You may eschew a name entirely, but it may make some client communication more difficult.

Communicating Your Availability

By default, we assign a maximum of two cases to a case lead at a time, logged on the case tracker.

- DM leadership to change your capacity anywhere between 0-3.
- You never need to explain to us why you're asking for a change in capacity.
- Feel free to update us about your capacity as often as needed.

[\[top\]](#)

Family Justice Center Leadership

If you have questions about an individual case, please contact the case worker listed on the referral form first. However, if you have an urgent issue and cannot reach that case worker, or if you are trying to schedule an in-person appointment, alert the leadership team and we will assist in contacting the following FJC directors at each borough.

[redacted]

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

Receiving A Case

This section describes what happens when you receive a case and guidance on how to go about handling it. When you are assigned a case, you will receive three things.

- A message via Slack or email. **If you have a preferred method of communication for notifications, e.g. a personal email address, Slack, etc, please make sure to communicate this to the leadership to ensure you receive assignment notifications.**
- A Box folder shared to your Cornell email containing the client's intake chart
- An email to your secure inbox with the client's contact information.

Deciding How To Handle A Case

Not all cases require a full appointment, and in some cases you may want to contact the case worker before the client for more information.

- It is possible that the intake describes issues that are beyond what we are trained to do.
 - If you feel this is the case, **please feel free to contact the leadership team for support.**
- On rare occasion, you may be able to handle the majority of the client's concerns via email, although this is at your discretion.
- Most cases will require you to schedule a 1 hour initial appointment with the client.

Interpreter Services + Language Competencies

Some clients list a language other than English as their primary language.

We try to match clients with the language competencies listed on the CETA members page. You may always check if there is another consultant who has listed familiarity with the clients primary or secondary language, and invite them to work on the case with you. However, unless you (or someone you have partnered with for this case) are comfortable interpreting the client's primary language, you should use the interpreter service enlisted by the FJCs.

Each FJC has an account with Voiance interpretation services which we are allowed to use for clients. Each account has a PIN that is periodically changed, so the below information may be out of date. **If the FJC is not listed below or if the PIN does not work, contact the leadership team.**

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

[Account information redacted].

Using the Interpreter Service:

- Dial the number. Use RingCentral, not Zoom, as you need the dialpad.
- Enter the account and PIN.
- You will be asked to state the language of the interpreter you would like.
- Once connected, the interpreter will ask for your name and the name of the person you are trying to reach.
 - If you do not have a name for the client, you can explain that they did not leave their name but that they should be expecting to hear from you.
- If you're not calling to schedule, best practice is to inform the interpreter of the nature of the call so they are not caught off-guard:
 - E.g. *Hi, I have scheduled an appointment with a client. I also wanted to give you a heads up that I work with a domestic violence agency, so this call may involve some discussion of abuse.*
- The translator will dial out for you.
- If you cannot reach the client, the best practice is to not leave a message.
 - If you do want to leave a message, leave the same vague voicemail as always.
- There is no expectation for you to go through the consent form, and in fact discourage it, due to the time limit and ethical issues raised by having an interpreter. This is at your discretion.

[\[top\]](#)

Scheduling an Appointment

- Review the intake information on the chart, particularly email/text/call permission and safe contact times.
 - **It may not be safe to contact them outside of that window or by other means.**
 - For example, if the client lives with their abuser, they may only feel safe to have an appointment while at work or visiting a close friend or relative.
- If, based on the intake form, you'd like additional information from the case worker, to solicit preemptive advice/support about an unusual tech issue, or that the contact window will be very difficult for you, please reach out to us via DM or the #clinic-practice channel.
- We strongly encourage having a second for all appointments, especially first appointments.

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

- **If you are struggling to find back up, contact leadership.**
- **Contact clients to schedule an appointment within 1-3 days, and at most, *one week* from receiving the referral.**
 - **If you have doubt as to your ability to make this window, alert leadership.**
 - We won't hold it against you, but we do care deeply that our clients receive care in a timely manner, so we may step in to reassign a case or set expectations with the client.

A Note on Scheduling + System Oriented Trauma

Initial contact and scheduling an appointment with clients can sometimes be the most difficult part of case lead duties. Please don't be discouraged if the client fails to answer after an initial email or phone call. From a trauma-informed perspective, clients often have a lot of other things going on, may feel avoidant towards tasks related to their abuse history, and on top of that, we are strangers reaching out to them from out of the blue! Once we manage to get in contact, clients are often much more responsive and eager about setting up an appointment. If you're having trouble reaching a client, of course feel free to share in the #clinic-practice channels.

System-Oriented Trauma

System-oriented trauma is when a client feels as though they are undergoing another experience of trauma (*retraumatization*) in a treatment context, including in their interactions with their caseworker or staff. Sadly, many settings designed to treat or care for trauma may unintentionally create traumatizing experiences.

Examples that are particularly relevant to our work at CETA include:

- insensitivity as to how the client's traumatic history has affected their life
- minimizing or discrediting client responses
- providing substandard service to clients of marginalized identities (e.g. non-native English speakers).
- Other examples may be difficult or impossible to anticipate, such as using specific phrases, sounds or actions that have a harmful association to the client.

In the clinic, we can anticipate the risk of retraumatization caused by CETA itself by adapting our approach to working with clients. If you need a refresher on speaking to clients please review the slides we used for training or reach out to one of the leadership team directly. **If your client**

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

discloses what they have identified as unacceptable behavior from a case worker, please also let the leadership team know so we can work with the FJC directors to address it.

Initial Contact: General Protocol

Detailed information about communicating via phone, email, and voicemail is in the following sections. Regardless of communication method, the overall protocol can be summed up as:

Step 1: Send an initial outreach via the method of your choosing, in accordance with the client's contact preferences. **Update the case tracker.**

Step 2: If the client does not respond after several days, make a follow-up attempt to contact them. Try a different method of communication if possible. **Update the case tracker.**

Step 3: If a week has passed without no response, contact the case worker. You may do so yourself; however, you can simply let us know in the Slack channel that you've made a couple unsuccessful attempts at contacting the client from case XXX, and [redacted] or some other member of the leadership team can contact the caseworker on your behalf. Either way, **update the case tracker.**

Step 4: If no response from the case worker for another week (see below), mark the case as inactive, and send the case worker a discharge note letting them know to submit a re-referral if needed (see: Nonresponsive, inactive, and no-show clients). If the case worker responds, confirm the client's contact information and ask them for assistance in setting up the appointment. **Update the case tracker.**

Whatever method you use to contact the client, if you have confirmed an appointment time, it is usually helpful to let clients know that you will be calling from either a secure Zoom line or your RingCentral number, and that if they receive a call from an unknown number at that time, it's probably us.

Help! My Client Didn't Provide a Safe Phone Number! (script)

If the client does not have a safe phone number nor a safe email: Usually if this is the case, CETA leadership has already contacted the caseworker before sending you the case, and if you haven't received further instructions via Slack or email, we didn't read it carefully and made a

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

whoopsy. Let us know, but we'll have to just email the caseworker for assistance.

If the client does provide a safe email (but no phone number): Then you can email the client directly asking them how they would like to proceed with an appointment. The options are (1) provide a safe number (2) email a Zoom link created from the Tech Clinic Zoom, or (3) the client goes to the referring partner organizations physical office and use their equipment. Suggested script below:

Dear [client],

I'm reaching out from the Cornell Tech clinic; we received your referral from [organization]. Your contact information stated that you were not comfortable with us calling or texting you, so I wanted to reach out about how we can conduct an appointment.

- 1. we can help you schedule a time to come into [organization] to make a phone call using the equipment there.*
- 2. you can provide a friend or other safe contact phone number for us to call.*
- 3. we can send you a Zoom link to this email address. Please note that in this case, there is no need to turn your camera on or join with video if you are not comfortable with doing so; we are happy to conduct an audio-only appointment.*

Please let me know what your preference is among these options, and feel free to reach out to this email address or your caseworker with any questions.

Kind regards,

[chosen signoff]

Help! My Client Chose a Zoom Appointment!

You can conduct the appointment as normal but keep in mind the following for **your and other consultants comfort and safety**:

- Make sure the link you created has the waiting room enabled. It should be enabled by default, but good to double check so you have time to set up the Zoom comfortably before the client joins.
- Let the other consultants join before admitting the client so they have time to change their name and turn their camera on/off.
- Make sure you pay attention to all consultants changing their Zoom display names to something they are comfortable with! The client will be able to see display names.

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

- **Camera consent:** You and other consultants are under no expectation or obligation to turn your camera on in this situation. You can let the client know that *"We're sensitive to concerns that many of our clients may have surrounding using their cameras, so we encourage everyone to only turn on the camera if it makes them feel more comfortable. I personally choose [to keep my camera on/off]."*
- **Recording:** You can proceed with consent to record as normal, but make sure that the recording is local (not to the cloud) and to delete the video and only upload the audio file (.m4a).

Scheduling Via Email (script)

If the client's primary language is not the same as yours and email is the only safe contact point, send the email to the caseworker and ask them to help translate or set up the appointment. **Only send emails to clients or case workers from your secure inbox.**

SUBJECT: Cornell Tech Clinic Referral

Hi <client's first name>,

I'm reaching out from CETA, the Cornell University tech clinic. You were recently referred to our services by <referring organization>. Thank you for taking the time to reach out to us.

I'd like to set up an appointment for you to discuss the issues you described. We would call you from a secure conference line and talk for approximately one hour. Are you available at any of the following times?

- *Time A*
- *Time B*
- *Time C*

If none of those times work, let me know what does and we can try to accommodate you. You can also contact me via call/text at <RingCentral number>. Please let us know if you have any questions.

Kindly,

<Your name> (and/or) the CETA Team

Scheduling Via Phone (script)

If the client's primary language is not the same as yours, follow the instructions in the interpreter guidance above. **Always confirm that it is the client on the line before providing details.**

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

If you do not have a name for the client, then you can say *"I'm calling about a referral I received from <caseworker name>."* If they are still confused, you can say, *"Sorry, I don't have a name listed for the referral. <Caseworker name> said you might be interested in talking with us."* If they are still confused, then to be on the safe side, you can say, *"OK sorry, I'll reach out to <caseworker>"* and contact the caseworker.

Once you have confirmation, then you can proceed with something along the lines of:
I'm calling from CETA, the Cornell University tech clinic. You recently filled out our form on referral from the <borough> FJC. I'm calling to schedule an appointment. We would call you from a secure conference line, and talk for about an hour. Are you available ...<offer times>

Make sure to give the client your RingCentral phone number so they can get in touch with you if needed.

Sending A Text/Leaving A Voicemail (script)

It is standard practice in settings such as CETA to leave a vague voicemail unless the client specifically tells you it is okay to leave messages. A 'vague voicemail' here means leaving a voicemail on the client's device that lets a client know that we have been in touch but does not disclose confidential information.

HIPPA provides guidance in these contexts stating that to *"reasonably safeguard the individual's privacy ... [providers] should take care to limit the amount of information disclosed"*. In our case, the client's abuser may hear their message. We should limit the amount of information we leave so there is minimal risk to survivor safety if it is intercepted.

Because the same is true for text messages, we suggest a similar approach for an initial text message until you've confirmed that you've reached the client. A suggested voicemail/text script you could use is:

Hi <client name, if provided>. This is <name>. I am trying to reach you to schedule an appointment that you recently requested. You can call, text, or leave a voicemail at [RingCentral#] to reach me with any questions. Thank you.

Do not:

- Use your personal phone number, only RingCentral
- Mention your name, if you do not feel comfortable
- Mention the FJC, Cornell University, Cornell or Cornell Tech Mention the 'clinic', the Clinic to End Tech Abuse or CETA

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

If The Client Doesn't Respond (script)

If you've tried to contact the client several times through available methods to no avail, notify the caseworker and ask for assistance. If you the client isn't responding, they may be avoiding strange calls/emails; in this case, its helpful for the caseworker to let them know your email address or RingCentral so they know its a trusted number. However, often if you cannot get in touch with the client, the caseworker can't either. To cover this range of possibilities, we suggest the following script:

Dear [caseworker name],

I hope this email finds you well. We reached out to your client <name> a couple times but haven't heard back; are you able to confirm if this client is still interested in our services? If you are unable to get in touch with them or we don't hear back within the next week or so, we'll mark this client inactive and they can submit a new referral if they change their mind. If you are able to get in touch with them, feel free to share this contact email and phone number (<RC #>) with them. Please let me know if you have any questions. Thank you!

Kind regards,

[name]/[the CETA team].

When The Client and Case Worker Don't Respond (script)

If the caseworker has not responded in addition to the client, you have a couple options:

Option 1: Notify c/w of inactivity and instruct them to re-refer

You can send a variation of the following email to the caseworker:

Dear [caseworker name],

I hope this email finds you well. I'm following up regarding the client you referred to us [name]/whom we don't have a name for but whose contact information is [contact]. As we still haven't heard back from you or the client, we're going to assume this client is no longer interested in our services. However, if we are mistaken or the client changes their mind, we encourage you to contact [redacted] or submit a new referral to make sure they are connected to an active consultant. Please let me know if you have any questions. Thank you!

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

Kind regards,

[name]/[the CETA team].

Option 2: Ask Leadership to Contact the FJC Directors

We can fall back to [reaching out to the appropriate FJC directors](#). You may want to do this if you have heard from the client once or twice but since had trouble getting in contact, or if the intake form information suggested the client was high risk. If you want to reach out to the FJC directors, ask [CETA leadership](#) to help.

Setting up the appointment

After an appointment has been scheduled, you need to document the appointment in [the appointment tracker](#) and set up an appointment on Zoom. If the client is contactable by email, it may improve client no-show rates to schedule a reminder email to be sent the day of or night before the appointment. Zoom instructions are below.

Log into Zoom using the *redacted* address; instructions are above. Click on the "+" symbol next to "Upcoming" and "Recorded" to create a new appointment. Name your appointment, "<case ID>_<appointment ID>", e.g.

"0003_001" for the first appointment for case 0003.

Other important settings:

- i. Generate meeting ID automatically. **This is the default option.** Do NOT use personal meeting ID.
- ii. Enable waiting room. **This is the default option.**
- iii. Set yourself, and optionally your second, as alternative hosts via your regular Cornell NetID accounts. If you receive an error, you may need to activate your NetID-linked Zoom account by logging into Zoom via SSO with your NetID.

The screenshot shows the 'Schedule Meeting' interface in Zoom. The 'Topic' field is filled with '0003_001'. Under 'Date & Time', the date is '1/21/2021' and the time is '1:30 PM'. The 'Recurring meeting' checkbox is unchecked, and the 'Time Zone' is set to 'Eastern Time (US and Canada)'. In the 'Meeting ID' section, 'Generate Automatically' is selected. The 'Security' section has 'Passcode' (992302) and 'Waiting Room' checked. The 'Video' section shows 'Host' and 'Participants' both set to 'Off'. The 'Audio' section has 'Telephone and computer audio' selected. A 'Dial in from United States' link is visible at the bottom.

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

- iv. We encourage building 10-15 minutes of slack time for pre-meet and debrief before and around the appointment. E.g. for an appointment from 1:30-2:30, schedule it from 1:15 to 2:45.

Once you've set up an appointment, enter the appointment in the appointment tracker. and notify #clinic-practice of the upcoming appointment. You may also want to create a corresponding calendar event in whatever personal calendar you use, so you can share it with any seconds or shadowers who join the call.

[\[top\]](#)

Conducting an Appointment

You may conduct an appointment either via Zoom or via RingCentral, depending on what you are comfortable with. If other people are on the call, it is usually easier to use Zoom. **If using Zoom, make sure all names are set to whatever each person is comfortable with.** To call the client from Zoom.

- 1) Go to Participants → Invite → Call Out.
- 2) In the **Invitee Name** field, enter *Client* and in the **Phone Number** field enter the client's safe phone number.

If the client does not pick up, our general policy is to leave a vague voicemail saying that you are calling about a scheduled appointment, wait five minutes and then try calling again. If they do not pick up, wait another five minutes and then try again. At that point, if you still haven't received an answer, you are free to consider it a no-show or keep calling at your discretion. Keep in mind that once 15 minutes have passed, the remaining allotted time might be too short to get any meaningful work done. For our full guidance here, see [non-responsive, no-show, and inactive clients](#).

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

During The Appointment

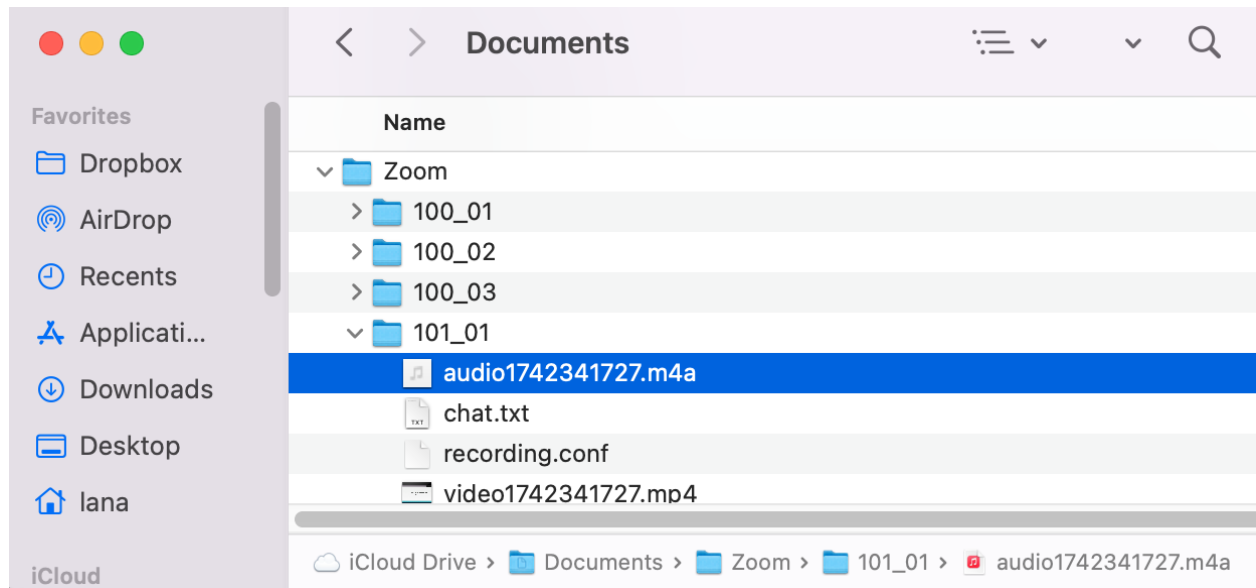
- **Always disclose how many CETA staffers are on the call.**
- Before beginning the appointment, remember to ask the client to confirm whether they are in a safe and private place to take an hour long appointment with the tech clinic.
- Use the v4 oral consent.
- If the client consents to recording for research, you may record the call directly in RingCentral or Zoom. **Always notify the client when you are turning on recording.**
- Communicate with your second and other team members on Slack
- Keep notes on the Live-Notes.docx file on Box within your case folder.

Wrapping Up An Appointment

- **Update the appointment tracker and the case tracker.**
- **Upload any recordings to the Research-Data folder in the case folder Box renamed to the appointment ID (e.g. 003 --> Research-Data --> 003_001.m4a).**
 - On RingCentral, the recording can be found under **Phone >> Call Recordings**.
 - On Zoom, a pop-up will appear that says "Converting meeting recording." **See below screenshot for the output.**
 - On MacOS, a Finder window will pop up showing the three created files. Otherwise, you can search for the **Zoom** folder.
 - On PC, it may be a bit tricky if you don't know the location the files were created in, but it's usually in a folder named Zoom, e.g. ".../Documents/Zoom/".
 - **Zoom automatically generates 3 files; we only need the audio file ending in .m4a.**
 - **Delete the recordings from your local machine or RingCentral after uploading.**

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

- If you've determined that you need a follow-up appointment, see the notes of follow up



appointments below. Otherwise, see "closing a case" below.

- (Optional but encouraged) Drop a note in #clinic-practice to share how it went!

Follow Up Appointments

If you deem a follow up appointment necessary, the process for setting up an appointment is essentially the same as scheduling an initial appointment. However, we strongly encourage trying to keep the same team (e.g. the same seconds and shadowers on the original call) by considering their schedules and giving them first options at scheduled follow ups. **On follow up appointments, remind clients about the consent form and ask if they'd like to review it. At a minimum, ask if they are still comfortable with notes and recording if they agreed last time, and always notify everyone on a call when you have begun a recording.**

[\[top\]](#)

Closing A Case

Set your case to 'inactive' in the case tracker! This is how we know you're available to take a new case. If you are not planning on scheduling another appointment, you can mark the case as "inactive" in the tracker. It is at your personal discretion whether you choose to do this before or after sending the PCC. If you are not planning on scheduling another appointment but are following up via email with the client, then feel free to mark the case as "semi-active" (which also shows you as available to take a new case). *To change these settings (i.e. to not receive a new case), DM/email/contact leadership and otherwise see ["Communicating Your Availability"](#)*

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

Post Consult Communication (PCC)

A PCC is not always needed, and whether it is needed is at your discretion. If, at the end of an appointment, there is no need to follow up with the client (by e.g. sending them additional guides or looking into outstanding problems), then a PCC may not be necessary. If you think it would be useful, you may ask the client if they'd like a summary of the appointment with a reference link to the guides for issues covered in the appointment. This is particularly useful if they have other similar devices or accounts that they'd like to secure, but often not necessary. This PCC FAQ document has some boilerplate follow-up information that consultants have written for past PCCs.

If they say no (and there are no outstanding issues to follow up on), then there's probably no need for a PCC. If they do say yes or they do have outstanding issues, then **make sure you have permission to either email** them or, as an alternative, permission to email their case worker the PCC.

If you do deem a PCC necessary, please write the body of the PCC in the Box file as a record of your communication with the client. Do not include the client's PII, such as their first name or e-mail.

Send A Discharge Email To The Caseworker (script)

You should **always** email the client's case worker to let them know you've met with the client. If you don't have permission to communicate with the case worker about the client's situation, then don't send any other information. However, if you have permission, then you can let them know about any important findings.

Example:

Dear <case worker name>,

I'm reaching out from Cornell CETA to let you know we recently saw your client <client's name or otherwise some identifying PII> in our tech clinic. During the appointment, we went over the client's concerns about <X>. We (did/didn't) find evidence of compromise, and we took steps Y and Z to secure their accounts. We're marking this case as inactive [because they haven't reached out for a follow up appointment], but if you have any questions or if the client has new concerns, please feel free to contact the admin team at [redacted].

Best,

<name + the CETA Team>

This will of course depend on what actually happened with the client, such as letting them know if you are 'discharging' the client because you cannot get in contact with them.

[\[top\]](#)

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

Norton Referrals

If you've offered the client a Norton license and they've accepted, then let [redacted] know the case ID on Slack and he will allocate a subscription. We recommend Norton licenses if the client has one or more non-Apple devices and the client would benefit from spyware protection, either for personal comfort or because of high risk. However, this always at your discretion.

The licenses offered through the FICs are for Norton 360 Deluxe. The Norton subscription is for **1 year of free protection services for up to 5 devices**. Protection services include: anti-spyware, antivirus and malware; webcam security; dark web monitoring; password management and more. **Note that this product does not scan Apple devices for malware/spyware**. No antivirus has that capability (due to restrictions by the Apple operating system software). Most clients who accept a license will want a follow-up appointment for installation, but you can try sending them the subscription code and a guide and suggest they request an appointment if they run into issues.

An example for email text introducing a Norton subscription is below, most likely included with any other follow-up information:

The discussed Norton subscription is for 1 year of free protection services for up to 5 devices. Protection services include: anti-spyware, antivirus and malware; webcam security; dark web monitoring; password management and more. The exact services vary based on type of device.

Your personal product key for your Norton 360 Deluxe subscription is: [License Key]. Please keep this information in a safe place once you have used it to start your subscription.

Follow the steps below to set up your subscription and install on a laptop:

- 1. Go to Norton.com/setup*
- 2. Click on the Enter Product Key button*
- 3. Setup an account. Use any safe email address for your account setup.*
- 4. In the MyNorton Portal, click download*
- 5. Enter your product key (provided 25 digit code)*
- 6. Select device(s) to install on.*

Follow the steps below to set up your subscription and install on Android:

- 1. Use a browser to go to <https://norton.com/setup>*
- 2. Click on the Enter Product Key button*
- 3. Setup an account. Use any safe email address for your account setup.*
- 4. Enter the product key written above (the 25 digit code)*
- 5. On your Android phone, go to the play store, search for "Norton 360", and install it.*
- 6. Open the newly installed Norton 360 app, login and follow instructions to activate.*

This is a redacted version of CETA's technology consultant guidance document. We do not expect our consultants to have memorized all of this information; it is for them to refer to back to; often when consultants have questions, we can simply direct them to the appropriate section in the guidance first to see if that answers their questions.

If you need assistance or have questions about your subscription, please ask us or reach out to NortonLifeLock's customer support center by phone or online chat at <https://support.norton.com/sp/en/us/home/current/contact>

The following resources can be helpful when helping clients to activate their Norton 360 license:

- Lifewire's guide on installing Norton (it has images that show the process to follow): <https://www.lifewire.com/install-norton-antivirus-4589383>
- NortonLifeLock Partner's Norton 360 installation videos: <https://www.nortonlifelockpartner.com/security-center/norton-360-installation.html>

[\[top\]](#)

D. Chapter 7: Conducting an Appointment

- Note-taking Infrastructure
- Technology Assessment Questionnaire (TAQ)
- Tech Safety Checklist

SAMPLE NOTE TAKING DOCUMENT FOR CLIENT SESSIONS.

All links have been removed.

- * Appointment ID: XXX_XX
- * Scheduled Start Time:
- * Actual Start Time:
- * End Time:

Preconsult Notes:

Notes from chart, consult plan

Participation in Research:

! Consent Form (version as of Spring '22)

Questions about research participation:

- * Consent to Research (Y/N):
- * Consent to Notes (Y/N):
- * Consent to Recording (Y/N):

! Turn on recording if yes !

Consult Notes:

Tech Safety Checklist, Tech Assessment, CETA Guides, Case Lead Guide

- * Client background and concerns:

...

- * Actions Taken:

...

Wrap Up:

- * Appointment Tracker, *Case Tracker, Common PCCs

SAMPLE NOTE TAKING DOCUMENT FOR CLIENT SESSIONS.

All links have been removed.

- * Appointment End Time:
- * PCC or Follow Up Appointment Needed?
- * Permission to share info with caseworker?

! Upload/delete any recording !

Technology Assessment Questionnaire (TAQ)

Make sure to cover the most pressing concern widely expressed by clients thus far

- Do you worry that your device(s) is being used to track you?
 - Does the abuser show up unexpectedly or know things they shouldn't know?

Probe for risks of device compromise

- What devices do you use in your home or carry with you?
(e.g., smartphone, iPad, tablet, desktop, laptop, kindle, echo, etc.)
- Do you currently (or have you in the past) share(d) your devices with your abuser? ●
- Is there any chance that your abuser has (or had) physical access to your devices? ○
- Does (Did) your abuser ask or demand physical access to your devices? ●
- Who set up the screen locks or passwords on your devices?
 - Do you use fingerprint or facial recognition to unlock your devices?

Probe for risks from ownership-based attacks

- Do have a shared family plan?
- Do you or does someone else pay for your phone plan or Internet access plan?

Probe for risks of account compromise

- Who set up your email account or other online accounts?
- Have you ever shared any passwords with your abuser (or anyone)?
 - When did you last update your passwords for your email or other online accounts?
 - How do you remember your passwords?
 - Do you ever take photos of your passwords?
 - Is there a chance your abuser knows (or could guess) the answers to your password reset questions?
- Do you think your abuser has access to your accounts online?
 - Do you have an iCloud or Google account?
 - Do you think the abuser knows the password or has access to your bank account? ○
 - Do you think the abuser knows the password or has access to your email accounts? ○
 - Do you think the abuser knows the password or has access to your social media accounts? (Facebook, Instagram, WhatsApp, etc.)

Probe for risks from children's devices

- Do you have any children?
 - Do you share devices with your children?
 - Do you or does someone else pay for your children's devices?
 - Who gave your child their device?
 - Does the abuser have access to the child's device?

- Does your child bring their device to visitation with the other parent?

Introduction

This document identifies the most common tech safety issues that clients describe to us. Each issue is paired with a checklist of potential indicators of concerns, common causes roughly ordered by likelihood, and solutions.

There is redundancy in many of these checklists, as a single point of compromise can manifest in multiple different ways. **It is intended as a quick reference for volunteers to map client concerns to potential remedies.**

These lists are not intended to be, nor can they ever be comprehensive. If you are in doubt as to whether or not you've missed a potential avenue of attack or if you run into an unfamiliar issue, *always* consult with the Slack channels #clinic-practice and #techsafety. It is never too late to send follow up information, and remember, we are not an emergency service!

It also links to, but does not replace, the existing step-by-step guides used to walk through a solution. Please always consult the guides for a full walkthrough, including warnings about visibility to abusers and evidence documentation.

Legend

- ⚠ Course of action may be visible to the abuser. Notify client.
- 🔍 Evidence documentation checkpoint. Remind client to take screenshots.
- ❓ Probe the client for more information.
- ▲ Hypervigilance indicator.

Table of Contents:

- [General](#)
- [Location Tracking](#)
- [iCloud/Email Monitoring/Tampering](#)
- [Text Messages Monitoring/Tampering](#)
- [Phone Conversation Monitoring](#)
- [Harassment \(social media + phone calls\)](#)
- [WiFi and Network Compromise](#)
- [SIM swapping and cloning](#)
- [Video/Audio Recording Devices](#)

General

It is not uncommon for clients to omit details that provide helpful clues without additional probing. Particularly relevant probing prompts are noted in each section. However, it is always a good idea to prompt the client with the following questions:

- Do you worry that your device(s) is being used to track you?
- Does the abuser show up unexpectedly or know things they shouldn't know?
- What devices do you use in your home or carry with you? (e.g., smartphone, iPad, baby monitor, tablet, desktop, laptop, kindle, echo, etc.)
 - Do you currently (or have you in the past) share(d) your devices with your abuser?
 - Is there any chance that your abuser has (or had) physical access to your devices?
 - Do you share a phone/Internet plan with the abuser?
- If abuser is a former spouse/partner, do you share custody of any children who may have devices?

[\[top\]](#)







Location Tracking

If an abuser can track a survivor's real-time location via spyware or a dual use app, they may show up in person and harass or harm them. Alternatively, knowing a survivor's agenda (e.g. an e-calendar) is enough to know where they will be at what time. Knowing where a survivor has been in the past — for example because they are able to see where payments have been made — can be used by an abuser to intimidate or stalk a survivor.

Client Indicators

- The abuser always or sometimes seems to know where the client is
- The abuser is using information about the client's whereabouts in legal proceedings (e.g. child custody)
- The abuser explicitly states they are tracking the client
- Client has general safety concerns and would like to check overall safety

Possible Causes + Actions

- **[If iPhone]** Location settings on iCloud.
 - Check iCloud location settings including FindMy.  
 - Check family sharing settings  
 - [Check iCloud security.](#)
- **[All devices]** Location settings on Google Account (Google Maps)  

- Possible unidentified tracking device ⚠️🔍
 - **[If Android]** Apple app to scan for AirTags on Android: **AirGuard or Tracker Detect**
 - **Note that Tracker Detect is notably difficult to use.**
 - Check devices in bluetooth + WiFi range (for e.g. Tile or other trackers)
- If location tracking seems limited to vehicle, OBD ports, SmartCar apps, or built-in tracking for registered owner of car can be checked by mechanic.
- Child devices and trackers in child items if shared custody
 - in particular tablets (e.g. Kindle Fire), smartphones, laptops, and trackers
- Abuser may have proximal (indirect) info about client's location via access to text messages/calendar or financial accounts (e.g. credit card logs or receipts indicating location) with details about client's schedules or travel history.
 - Refer to sections on [text message](#), [Gmail/email](#) access and [financials](#).
 - **? Probe:** Ask about client's social media usage and whether location information might be shared on social media (including geotags).
- **? Probe:** Does the client have any devices they haven't mentioned?
- [All devices] **? Probe:** Has the abuser had physical access to the device? Does the client still have physical contact with the abuser?
 - If yes, **high risk** for spyware/dual-use app. Check apps with location access. ⚠️🔍

iCloud Monitoring/Tampering



For clients with iPhones or Apple devices, an abuser who has access to an iCloud can access a host of information such as location data, Notes app, photos, text messages and iMessages, voicemail. This is a standard safety check for any client with an Apple device and should almost always be performed if applicable.

Client Indicators

- Client has iPhone or Apple device (always a good check)
- Abuser can access information stored in a wide array of applications installed on iPhone or Apple computer, such as Notes app, photos
- Text messages and/or e-mails are disappearing or mysteriously marked as read
- Client has general concerns about online safety and wants holistic check up

Possible Causes + Actions

- Check for suspicious log-ins in iCloud ⚠️🔍

- If not currently logged in, may be signing in and out. 2FA + password change and/or suggest that client use a password manager.
- **! Check email ([Gmail](#) or [other email](#)) used as AppleID**
 - **!** Check recovery email and recovery phone numbers and do this **recursively** e.g. check recovery accounts for the recovery account.
- Check location settings  
 - See location check for iPhone above
 - FindMy + apps with location access
- Check for old devices used by client that were given to abuser
- Ask about shared phone plan

[\[top\]](#)










Gmail/Google Account Monitoring/Tampering

Gmail accounts are linked to Google accounts. We distinguish Gmail (and their associated Google accounts) from other email providers. Access to a Google account discloses far more information (e.g. real-time location) than other emails, and may also be linked to an Android phone.

Client Indicators

- Client has a Google account, Android, or Gmail (always a good check)
- Emails or texts in messaging app are disappearing, mysteriously marked as read
- Abuser seems to see or have access to photos
- Abuser has location access
- Client has general concerns about online safety and wants holistic check up

Possible Causes + Actions

- Check for suspicious log-ins in Google Account 
 - If not currently logged in, may be signing in and out. 2FA suggestion.
- Check Google accounts linked to Android phone (guide)  
- **!** Check recovery email and recovery phone numbers  
 - **!** recursively check recovery accounts!
- Check location sharing settings (Family + Sharing Tab)  
- Google Family Link settings  

- default system app but need to check if abuser is added
- 💡 **Probe:** Ask about old devices used by client that were given to abuser
- Check email forwarding and shared email settings ⚠️ 🔍
- Is client on shared Internet plan? Are they the account owner? ⚠️
 - Won't give direct access to email but may explain some "web monitoring" behavior if abuser can access Internet history
- If interested in offering Norton LifeLock, it is only beneficial for Android phones

[\[top\]](#)

Email Monitoring/Tampering

Email access not only grants the abuser visibility into sensitive or personal information in the emails themselves, but can also be the root cause of other harms: email is often used to sign into other online accounts including social media and financials, may be linked to a calendar giving clues as to location, may be a recovery email for an iCloud/Google account, and may impact the client's ability to earn a living if it is a work or business account. While non-Google accounts typically don't directly track location, they can give alarming proximal information or allow access to an account that does.

Client Indicators

- Client has a non-Gmail account and/or recovery email is not Gmail)
- Emails are disappearing, mysteriously marked as read
- Abuser seems to know content of emails
- Most other emails do not have location access but proximal info such as receipts (indicating travel history) or calendars may be linked to email
- Client has general concerns about online safety and wants holistic check up

Possible Causes + Actions

- Check for suspicious log-ins. May need to search for email specific guide. ⚠️ 🔍
 - If not currently logged in, may be signing in and out. 2FA suggestion
- Check recovery email and recovery phone numbers ⚠️ 🔍
 - ! recursively check recovery accounts!
- 💡 **Probe:** Ask about old devices used by client that were given to abuser
- Check email forwarding and shared email settings ⚠️ 🔍
- Is client on shared Internet plan? Are they the account owner? ⚠️
 - Won't give direct access to email but may explain some "web monitoring" behavior if abuser can access Internet history

[\[top\]](#)

Text Message Monitoring/Tampering

Client Indicators

- ▲ Not receiving text messages
- Text messages deleted
- Abuser knows content of text messages
- 💡 **Probe:** what text application does client use? iMessage? WhatsApp? SMS ("regular" text messaging)? Facebook's Messenger?

Possible Causes + Actions

- [iPhone] [Check for iCloud compromise/access](#)
 - Check if iCloud storage is at capacity
 - Check which phone numbers and emails are allowed to send and receive messages associated with this AppleID, including message forwarding
 - Check how long messages are saved for until automatically deleted
- Ask client if using shared phone plan
 - Refer client/caseworker to legal counsel for exit under [NY State Law](#)
- [Android] Google Family Link settings (default system app in Android but need to check if abuser is added to settings)
- Check for suspicious apps that have permission to SMS/text messaging
 - May include default provider apps. Ask about phone service/model.

[\[top\]](#)

Phone Conversation Monitoring ▲

It's vanishingly rare for abusers to have the technical capacity to listen in on phone conversations. Clients who express concerns about phone conversation monitoring may be experiencing hypervigilance surrounding technology. Nonetheless, we should still treat their concerns with dignity and do due diligence in probing for information and checking for spyware, especially in high-risk cases,

Client Indicators

- ▲ client reports that abuser knows information spoken about on telephone calls
- client reports or consultant hears beeps, mechanical sounds on phone lines
- ▲ dropped calls/client misses incoming calls that do not show up on log
- abuser claims that they are listening to phone calls and conversations
- ▲ Frequent spam calls

Possible Causes + Actions


- Check for other evidence of account compromise
 - abuser may be accessing knowledge through other technical means (e.g. text messages, voicemail) or through non-technical (e.g. mutual contacts) means, and claiming that they can "hear phone calls" to scare client
 - Probe for and check [iCloud](#), [text message](#), and [Gmail](#) or [email](#) security
- **? Probe:** Is client on same/shared phone plan?
 - Refer client/caseworker to legal counsel for exit under [NY State Law](#)
- Possibly (and more likely) non-technical means of learning about phone calls, e.g. through shared/mutual contacts or children
- [SIM swapping](#) where the POC took control of the phone number (for a period of time)
- Spyware/malware, especially if other IOCs evident like dropped calls, short battery, phone running hot.
 - **? Probe:** did abuser have physical access to device?
- [V/AR installed in home](#). More likely if client is currently separating from abuser.
 - **? Probe:** did abuser ever have physical access to home?



[\[top\]](#)

Harassment (social media + phone calls + spoofing)

Harassment usually doesn't need to be diagnosed, as clients know if they're being harassed. It is unfortunately difficult to proactively prevent, especially without limiting the functionality of the client's technology. Setting expectations with client is important. However, here are some potential solutions.

Possible Solutions

- If abuser is directly contacting client, the client can request order of protection from lawyer
 - note that this is punitive, not preventative. We do not give legal advice but can contact case worker to request legal services (with client permission)
- "Allowlist" by blocking/filtering calls/messages from unknown numbers.
 - only if client does not need to receive phone calls from unknown number (e.g. client not receiving calls for a court case or doctors appointments)
 - Can purposefully delete contact information of harassers to filter them
- Client may set up a Google Voice or other ersatz phone number and distribute it to trusted contacts, in order to help with filtering calls. **Discuss pros/cons.**
- Privacy settings on social media may be set to more conservative level. 

- We can also contact social media sites to help report harassment
- Check if number has been publicly listed on any websites/Google
- Check if Call Forwarding is configured  
- "Code phrases" with trusted contacts to avoid/prevent spoof attacks

[\[top\]](#)

WiFi and Network Compromise ▲

Suspicion of WiFi and network monitoring is often a catch all for suspicious and may be an indicator of hypervigilance/mistrust in technology. Even if the abuser can access the clients WiFi, there is very little they can do with that access. However, we can and should still recommend common sense measures such as ensuring their WiFi is not private, changing the password, and not visiting suspicious sites or links.

Client Indicators

- ▲ client reports that abuser can see all their internet traffic
- unusually slow WiFi/Internet, especially across multiple devices
- ▲ client reports abuser has used network in past and fears they still have access

Possible Causes

- **? Probe:** is the monitored activity specific to one to two potentially compromised accounts? might it be hacked email(s) used for wide access, e.g. as the log in to many accounts? did the abuser inherit any old devices?
- **? Probe:** if client reports slow network, is the network slow across multiple devices?
 - If it is limited to one device, it may be benign (obsolete hardware, uninstalled software/OS updates, full hard disk) or suspicious (spyware/malware).
- **? Probe:** is abuser named on the Internet service account?
 - Refer client/caseworker to legal counsel for exit under [NY State Law](#) (applies to cable accounts as well as phone)
- WiFi scan using router page or Fing app to show devices on network
- Encourage client to change WiFi password to strong password.
 - warn client that this will sign out all of the other (legitimate) client devices on the network so they are not frightened/surprised later.
- **Inform:** useful to let client know that if the client is using their own private network of which they are the sole account holder, even other legitimate devices

cannot see their network traffic on most webpages, including most banks/social networks.

[\[top\]](#)

SIM Swapping and Cloning

Client Indicators

- client reports that they lost use of their phone number
- reports that SIM was removed from phone
- POC has had physical access to phone

Possible Causes

- **Probe:** what did client observe that led them to believe they lost access to phone number?
 - ▲ Temporary service failures (bad signal) are not good evidence of SIM swapping.
 - Received text message from cellular company that the SIM was being changed for the phone number
 - Cellular connectivity bars are X'd or greyed out, cannot make phone calls/texts
 - The above, combined with notifications about account activity (password reset or sign in) on accounts tied to phone number
- **Probe:** did client contact cellular provider?
 - If cellular service confirmed that phone was moved to another SIM as requested by someone (but not the client), then this is possibly a SIM swap.
- **Probe:** did clients obtain access to the phone number again?
 - Still may have happened in past, consider discussing account security
- **Probe:** does client have an online account with cellular provider?
 - Access to account by POC could help enable SIM swap or other cellular monitoring
- **Actions:**
 - Suggest contacting cellular company, regaining control of phone number, asking about and enabling additional protection against SIM swaps. For

example, many allow setting a secret PIN that must be given to change SIM

- Enumerate accounts to which phone number may have given POC access, check their security
- **Inform:**
 - SIM cloning is not feasible for modern SIM cards. Losing use of phone number always happens with SIM swapping.

[\[top\]](#)

Video/Audio Recording Devices ▲

V/AR is most likely with clients who either live with their abuser or who used to live with their abuser in their current home until recently. It is also especially likely if they share children ("nanny" cams) or have installed their own V/AR devices for safety and security. However, suspicion of V/AR can also be an indicator of hypervigilance.

Detecting V/AR is difficult for us to do, and you should set expectations with the client that we cannot do home scans. However, we can guide the client through some steps to find and/or disable V/AR. **V/AR will usually need both a power source and access to the Internet/Bluetooth in order to transmit any recorded data.** Changing WiFi password can knock off many V/AR devices.

Client Indicators

- Client has received direct threats from abuser (e.g. "I'm watching you")
 - Abuser may be bluffing or overstating
- Has installed their own V/AR for security but is worried about access
- Experiencing frequent electronic disruptions
- Has documented many instances of spying with no evidence of account/device compromise
- Client shares children with abuser who at some point had physical access to home, especially having recently lived together

Possible Causes + Actions

- **? Probe:** has abuser had physical access to space? do they still? child devices/mutual contacts?
- **? Probe:** do you have an Amazon Ring or other online camera account?
- However, V/AR requires a power source and usually requires bluetooth WiFi.

- Guide <TODO: link to home sweep guide>

[\[top\]](#)

suspicious or sensitive permissions for remote spyware check:
location, keyboard, microphone, camera

Financial Attacks

A client may have loans, credit cards, joint bank accounts, and shared assets with an abuser. A survivor's financial account can contain more than just financial information, such as a mailing address, contact information, location information (transaction meta-data), and more. Most often, financial abusers use technical attacks to monitor a survivor's financial activities (e.g., tracking and monitoring for finances), exploit their financial assets, restrict their access to financial accounts, and sabotage their financial stability. These attacks are difficult to prevent, just like harassment. It is possible to curtail some aspects of financial attacks, however, by enforcing good security and privacy practices.

Other scammers and fraudsters can be responsible for financial attacks, so an abuser might not be responsible. Financial concerns can seem like technical problems (e.g. incorrect credit report information online) but are sadly beyond CETA's scope to resolve. Nevertheless, there **are** some ways we can help! If in doubt, see about sending **Rosie Bellini** (rbellini@cornell.edu) a message on slack or email around anything you are unsure of.

Client Indicators

- Client has received direct threats from abuser (e.g. "I know how much money you have/make")
 - Abuser may be bluffing or overstating
 - Abuser may have survivor accounts added to a third-party personal finance management app (e.g., Mint, INTUIT)
- Client is receiving emails/receipts about purchases they have not authorized
- Client may have received a push notification from their mobile wallet that their registered card was used.
- Client may have received a security alert from a financial institution about someone attempting to access a bank account.
 - These may be phishing if further information is requested from a client!

- Client sees ‘suspicious’ activity on any financial account (e.g., fraudulent transactions, missing money, new accounts being opened without their knowledge)
 - Encourage client to take evidence 🔍
- Client may have received calls or letters sent to them describing financial products they have no knowledge of.

Possible Causes

- **? Probe:** has an abuser ever had physical access to your wallet/purse? what about your cards?
- **? Probe:** do you have any shared financial accounts with abuser? have you ever had one in the past? are they still active now (e.g., not closed)?
- **? Probe:** are you an authorized user on abuser’s accounts (i.e. can you use any of their cards)? is the abuser an authorized user on any of your accounts?
- **? Probe:** do you use a browser-based password manager? a standalone password manager? do you store financial information there?
- **? Probe:** does abuser know about all of your financial history or just some of it?
- **? Probe:** is any of this financial information already available online? (e.g., on open business pages)

Actions

- Check for evidence of account compromise; each financial service will have a ‘Security Center’ which gives a breakdown of connected devices + logins 🔍
- Encourage client to change account username and password ⚠️
 - This will sign an abuser out of any shared devices
 - Changes to log in information will also uncouple any personal financial management app accounts too (e.g., INIUIT mint, yolt etc.)
- Encourage client to change answers to security questions ⚠️
 - If all answers to a security question are known, enter a mismatched pairing of question to answer. “E.g. What was your first model of car?”
“Answer: Portland” (The answer to “Where were you born?”)
- Turn on an additional stage of security for financial accounts (e.g., 2FA, required branch visit) ⚠️
 - Warn client this may sign an abuser out of any shared devices
- Encourage client to remove an abuser numbers from any monitoring alerts ⚠️
 - Alternatively, setting up credit alerts via Experian/CreditKarma to a secure email address could alert a survivor to changes in their credit.

Other Organizations and Resources

For additional CETA Resources, including the safety guides referenced in Chapter 9: Helping with Technology Abuse, visit the [CETA Resource Page](#)

Existing clinics have benefitted from the research, advice, and resources provided by other organizations. We include a non-comprehensive list of other organizations addressing technology abuse here, but note that inclusion does not indicate a partnership, endorsement, or any formal linkage between the clinics, the toolkit, and these organizations.

[Chayn \(global\)](#)

- (Non-technical) resources for support and healing.

[Refuge \(UK\)](#)

- UK-based anti-domestic violence organization, which has a technology safety team.

[The National Network to End Domestic Violence's Safety Net \(USA\)](#)

- US-based anti-domestic violence organization's technology safety team.

[The Cyber Civil Rights Initiative \(USA\)](#)

- A non-profit organization with resources and advocacy for survivors of image-based abuse, often known as "revenge porn".

[Coalition Against Stalkerware \(Global\)](#)

- Cybersecurity expert coalition providing resources specifically for stalkerware victims, including within intimate partner violence.

[Electronic Frontier Foundation \(Global\)](#)

- A global digital privacy rights organization.