The Technology Abuse Clinic Toolkit

by Dana Cuomo, Nicola Dell, Alana Ramjit, Thomas Ristenpart

Table of Contents

Chapter 1: 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, started in 2018 and the Clinic to End Tech Abuse (CETA) in New York City, started in 2018. Affiliates from CETA have brought their experience at an existing clinic to establish their own technology clinic, namely the Madison Tech Clinic at the University of Wisconsin-Madison. Established separately, these clinics have each taken different approaches and created different models for aiding 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 seek to provide useful information and guidance for what we consider to be the essential (and optional) components of technology abuse clinics, steps to take when establishing a clinic, and example processes/procedures for successfully 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 technological challenges faced during the COVID-19 pandemic in early 2021.

Importantly, 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 provided 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 a clinic 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, so we have written the toolkit accordingly. Nonetheless, many of the tools and resources provided could be adapted to serving other populations with the caveat that there may be unique risks or different severity of concern in other populations that we have not investigated.

Worksheet:
A Guide to the Toolkit

This 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. Each page leaves room for you to jot down notes or ideas.

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 help desk 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?

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?

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?

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?

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?

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?

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?
-

Chapter 9: Helping With Tech Abuse

This chapter provides a broad background on technology principles that are commonly encountered in a technology clinic. Questions to consider as you review this chapter include:

- Who or what resources can your clinic turn to for advice with unfamiliar technology questions?
- How can you create spaces for continuous learning as technology platforms change and develop?
- What types of common misconceptions might your clients encounter, and how can you clarify those misconceptions sensitively?

Chapter 2: 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.

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:

- Communicates directly with the survivor-client, whether in person or remotely
- 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.)
- **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, e.g., the Apple Genius Bar or other tech helpdesk services that are not tailored to technology abuse. 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.
    - 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 the broader discussion 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.

Technology Abuse Intervention & 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 (i.e., 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 the Clinic to End Tech Abuse (CETA) and the Technology Enabled Coercive Control (TECC) Clinic use data gathered from their experiences running a technology abuse clinic to inform legal and policy advocacy. Some examples of policy efforts in practice include:

- State Senate Bill S2678 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
- Advancing legislation in Washington state, including House Bill 1320, a bill to modernize, harmonize and improve the efficacy and accessibility of laws concerning civil protection orders. This includes updating the civil definition of domestic violence to include (technology-enabled) coercive control, to digitize the protection order process and to standardize a process for including digital evidence of technology abuse into the court record.

Chapter 3: Agency Partnerships

This chapter discusses the importance of building and maintaining strong partnerships with already existing survivor support services and/or community partner agencies to ensure that survivors who receive assistance from technology abuse clinics have access to comprehensive safety planning and a wide range of support services. 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 may (and should) receive training on how to provide basic counseling and technology-specific safety planning, they may not be comprehensively trained, 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 is embedded within NYC Family Justice Centers (FJC), which operate as hubs that offer services from dozens of local partner agencies providing, for example, case management, economic empowerment, counseling, civil legal, and criminal legal assistance. 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/agencies at the FJC.

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, rural, urban, etc. 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, that clinics do not provide emergency services, that volunteer technologists are not 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. (see sample MOU in 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 domestic violence (DV) survivor support organizations. One can ask people working in the DV 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, 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 5). 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-DV professionals are suitably prepared for working with clients. This is healthy gatekeeping since without proper training one may cause serious harm to clients. It also emanates in part out of a painful history of ill-informed technologists hawking "solutions" that fail to sufficiently address complex DV problems or, worse yet, cause 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 (possibly more) 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

Of course, 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 DV 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.

Of course, 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. Of course, the 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. Of course, any such communication should typically require client consent. 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.

Chapter 4: Service Delivery Models

What is a service delivery model?

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. So a service delivery model encompasses both literal means of connection (in-person/remote, scheduled/drop-ins) but crucially includes other aspects of care, such as the length of care and types of services offered. In this chapter, we discuss different aspects of service delivery, which we break down according to these aspects of service delivery:

- Menu 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 have emerged due to uncontrollable circumstances (e.g. the remote-only demands of the COVID-19 pandemic), while others have 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 menu of services, which informs 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. Example care models include:

- ***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 consultants assigned to the client or a collection of consultants.

Different approaches have different trade-offs. The longer the lifecycle of client interactions the more consultant work per client, which increases burden on consultants and may reduce client capacity. 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. TECC remains a drop-in care service.

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 inevitably ask for services that consultants are unable to provide.
n-consensual intimate imagery (NCII or 'revenge porn'), and forensics are beyond our (and as far as we know, any technologists') ability to help, so technology consultants are instructed to set expectations with clients asking for help with these issues.

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 dauntingly large 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).

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.

It’s also important to consider setting boundaries on what clinics can help with.

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 main services are checking account and device configurations and this is commonly what clients want, but typically clients are allowed to share any technology-related issue and technology consultants will do their best to provide assistance if possible. However, certain issues such as harassment, no

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 (see *Intake* below). 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 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, a LGBTQ+ and HIV-affected serving agency in New York.

An alternative approach would be to allow 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 *screening* 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 who are abusers).

TECC Clinic: The TECC Clinic is currently utilizing 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. To clarify, 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.

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 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 served model. If the request is urgent or time-sensitive (e.g. the client is moving into a shelter soon 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 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 requires contact information for the caseworker and safe methods 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 many of the 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. 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.

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.

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% in this iteration.

Chapter 5: 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 will be 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. 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 baked into the structure of the clinics, with the clinics 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 consultants, which also have their own rubric) 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; working in spaces permeated by the effects of interpersonal violence is taxing for all involved, including staff. While it is always nice to have coworkers who are understanding, patient, and compassionate, these traits are even more important for team morale and mental health (see next section). Consider carefully 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, or, worse, exhibit a tendency to blame victims 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. 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

survivor, especially with the mindset of supporting survivors continued use of technology (e.g. not 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, 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 as *the emotional duress that results when an individual hears about the firsthand trauma experiences of another (HHS).* 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 hypervigilance, cynicism, and/or chronic exhaustion.

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)

Chapter 6: 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 about 10 hours 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* (discussed further below), regardless of whether technology consultants are paid or not.

Recruiting Technology Consultants

Any clinic will 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 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 of 2-3 references, and additional demographic and/or location data (we include as resources a sample call for applications and application form). If a clinic works with minors (under 18 years old), then some checks for history of child abuse may be requisite.

After receiving applications, the next step will be 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 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 gauging 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 (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 is 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 (ex: "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 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) 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 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. experienced “case leads”. Then they graduate to become case leads, handle client cases on their own, and help train future technology consultants.

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

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 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., case scheduling coordinator). 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. As one example, for the last few years, CETA has recruited and trained a new cohort of technology consultants annually.

Chapter 7: Clinic IT and Data Management Policies

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. It is even more important 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, the stakes are even higher. In addition to the safety and well-being of clients, the legitimacy of the clinic itself is at risk if it cannot safeguard it's 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 itself

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 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 relevancy 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.

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 pseudonymous)
- contact information (phone, email) for the client and/or their DV advocate
- limited demographic information, include 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 is often a wealth of client information.

Thus, 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 sessions notes, then best practices include 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. 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 (also known as ‘revenge porn’).

In all of these cases, an alternative is to guide clients on how to take these steps or navigate the necessary interfaces for themselves on a safe device that is preferably owned by the client, not the clinic staff.

Communications Infrastructure

Technology consultants may require communication infrastructure, especially if the clinic offers remote appointments. This includes videoconferencing 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 consultant's 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 will pass through this application? E.g. will the clients 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 have in place for the clinic to ensure that communications infrastructure are being used in accordance with the data safety protocols developed by the clinic?

Storage, access, and retention

Whatever data may be collected from clients, the clinic should maintain a policy for how that data is stored, by whom and how it can be accessed, and when that data will be deleted.

Storage

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

- What are their data storage policies? 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 their access control policies? Can you set permissions for individual files, users, or revoke permissions easily?
- Do they require 2-Factor Authentication for workspace members to access data?
- Encrypted storage is nice-to-have, but not necessary for clinic safety.

Data Access

Data access refers to whom within the clinic has access to individual pieces of data. In general, the more people who have access to a single file, the greater the likelihood that the file is compromised. As a

rule of thumb, restricting access to data as much as possible decreases the likelihood of compromise. This also pertains to the granularity of data; an individual requesting data to a particular client should only be able to see the data for that particular client, not granted general access to all client data.

More importantly, 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.

Data Retention

Finally, data should be kept only as long as it is needed. Some data may need to persist indefinitely; it is best if such data is anonymized as much as possible. For data that do not need to persist indefinitely, it is often helpful to determine a maximum length of time to retain the data, and set periodic reminders at each length to purge it. For data that is condition dependent instead of time dependent (e.g. ‘client exits service’ instead of ’30 days’), it is helpful to build data deletion into the process of that event (e.g. making data deletion part of the ‘discharge client’ task)

Managing Data Policies

For each piece of data about a client collected by the clinic, it is useful to write down why it is collected, who has access to it, and how long 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 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, the 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 running into, 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 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. If your organization has any interest in publicly releasing its data for research or other purposes, then be careful to determine whether that work would require human subjects approval from an Institutional Review Board. When sharing data externally, be mindful that in addition to explicit personal identifiable information such as names and addresses, client stories that are too highly specific can still 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.

Chapter 8: Conducting an Appointment

This chapter introduces principles for working with clients. We suggest flows 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 the next chapter.

Throughout this chapter, we include snippets of scenarios that we frequently encounter within the clinic, with examples of how they be instances where consultants should **be careful to use sensitive language** or where clients may have **traumatized or highly emotional responses**, along with some suggestions for how (not) to proceed.

Principles for Working with Clients

Chapter 2 shared some guiding ethics for technology abuse clinics. This section builds on these guiding ethics by emphasizing concrete approaches to communicating with clients that are consistent with the spirit of those ethics.

- **Client centered.** It is important to respect the clients' wishes and trust them to be the final authority on what actions are best for their situation. Presenting options and associated 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 exact nature of any content that will be shared with their case worker, 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).
- **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.
- **Rely on expert DV training.** While we provide tips on phrasing and language to use, this toolkit cannot replace the urgent need for expert-led training on speaking with clients and sensitive, inclusive language and practice.

Handling An Appointment

We break the appointment structure into three stages, organized chronologically: preparation, consultation, and follow up. Not all of these stages 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 digital 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.

Nonetheless, 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.
- Any prior, relevant information provided by the client (e.g., their intake form).

- 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 as a personal decision; 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).
- Emotional + mental preparation.
    - Clients may share difficult, disturbing, and traumatizing stories when discussing their technology abuse.
    - 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 thus 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-judgemental.

Language note: *Phrase questions rooted in a place of affirming the client's experience.*
Example: *Client states: "They can see everything I can do."*
Avoid: *"What proof do you have?" which can sound accusatory.*
Try instead: *"What alerted you to the fact that they can see what you're doing? Can you give us some examples of when they knew something 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 notes handy to record the device make and model, the year purchased, who it was purchased and set up by, and the date that the abuser may last have had access.

Trauma warning: *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.*

Example: *Client shares details about an incident involving physical abuse that occurred during a vacation, which was the first time they realized the abuser had access to their social media.*
Avoid: *offering platitudes; ignoring the story and moving on, which can seem dismissive; or asking unnecessary follow-up questions about their abuse, which can be voyeuristic and re-traumatizing.. Also do not try to act as a therapist for the client.*

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 relive all this but sharing this information is helpful for us to make sure that your technology is secure from [the person who's harming you]" (Note: mirror the language/pronouns used for the abuser.)

TIP: *professionalism is important, but it is okay to express shock that is appropriate for the gravity of the story e.g. "That's awful!”*

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. Some useful guiding questions are provided in the technology assessment questionnaire.

Some client behaviors may present particular challenges during sessions for consultants. Clients may be distressed, making it difficult to communicate with them. Others may be hypervigilant and/or with mental health concerns related to their technology experience. Clients may express concern that all their devices are “instantly and always hacked” or that there is a conspiracy by some unspecified, sophisticated group to undermine their technology.

Intake processing can attempt to check that the client would benefit from the specific services offered by the clinic, but no filtering will be perfect. In particular, filtering needs to balance against the undesirable effect of inadvertently turning away clients who could benefit from the service. Consequently, clients should be prepared for the challenges of navigating difficult sessions with clients, including practices such as encouraging having a second consultant available and proper training.

Appreciate that clients may have sought help for their technology concerns from other resources (e.g., law enforcement) and may have been met with disbelief or incredulous responses. Not being believed can increase feelings of hypervigilance, which can make sorting through information provided by the client even more difficult.

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 need immediate attention. 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.

Language note: *Avoid making promises to clients that cannot be guaranteed.*
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 happening."
"We can make sure that that doesn't happen again."
Try:
"We will take a look together and do our best to help. Your safety is our priority."
"We'll do everything within our power to help find an explanation."

A crucial feature of this phase is that the technology consultant is guiding the client to examine the existing configuration of a piece of technology **without 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.*

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.

Trauma note: *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 asking the client what their preference is, and in either case, always explaining what the consultant is 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, you 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."

Takeaways: After hearing the client's story, 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 an abuser or changing a password.

III:Plan, Inform, and Advise

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

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

Trauma note: *if signs of compromise are uncovered, then it is important to explain to the client what information may have been leaked by that potential compromise to the abuser. However, clients will likely need time to process, and may want this information written down to remind themselves later.*

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

Avoid: *Immediate problem solving, downplaying or overplaying the risks*

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."
"I'm sorry, that probably feels really unnerving. Do you need a moment? There are some safety steps we can take, but we can talk through them when you're ready."

TIP: *Tone is as appropriate as language here; try to use a calm but sympathetic voice.*

The first step is to encourage the client to document the compromise and explain why that is 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 as a practice is strongly encouraged.

The second step is to determine whether removing the source of compromise will alert the abuser. If so, it is vital that the client be informed of the potential risks. This information should also be shared with the client's designated safety planner who is trained in risk assessment. For example, a knee-jerk reaction to finding a physical device planted by the abuser may be to immediately disable it; however, the client should still be encouraged to take a pause to consider how disabling it might endanger their safety.

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 especially 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 an abuser.

Trauma note: *It is not uncommon for abusers to threaten their victims by mixing exaggerated claims of their technological capabilities with tangible acts of harm. One advantage of a technology clinic is that we 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 strongly suggest having set protocols for follow up communication and recording client data, and 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), you should still obtain the client’s permission to share it with anyone else.
- Be careful of handing out written resources, pamphlets, or flyers. If the client still shares space with the abuser, then this may put them at increased risk of harm.
- Be wary of where any private client information ends up, particularly if personal devices are used in appointments.
- Technology consultants should not give out their personal information to clients or have direct follow up with clients outside of t

Chapter 9: Helping With Technology Abuse

This section will give some pragmatic suggestions about how to approach helping IPV survivors with technology abuse. A key challenge is that technology changes quickly, which can rapidly render stale advice tailored to current technology systems. Relatedly, consultants may feel like they lack sufficient expertise to help clients. This chapter should help everyone realize that, with even a small amount of preparation, they can help many clients, while also providing: general guidance about typical abuse issues, suggestions for structuring discussions with clients about tech abuse, strategies for researching unfamiliar tech situations, and managing the inherent uncertainty about (perceived) person of concern (POC) capabilities.

Topics covered include:

- Core concepts for tech security:
  - devices
  - accounts
  - security mechanisms
- Being prepared to help with unfamiliar technology

Core security concepts

Helping with technology abuse benefits from some understanding of key concepts in computer security. Almost everyone will be familiar with them, at least from the perspective of technology users, and here we just reframe that user experience in the context of tech abuse.

At the highest level IPV tech abuse frequently falls into one of four categories:

- The first is ***ownership-based access*****,** which refers to problems that emanate out of the fact that the POC may be the one who owns or sets up technology. For example, they may have been the one who pays for a cellular phone plan or who set up a family's iCloud account.
- The second is ***account/device compromise*****.** Often the POC is able to log into online accounts (email, social media, storage) or access devices (phones, laptops, home devices) because they know, can guess, or can compel revelation of the credentials needed to login.
- The third is ***harmful messages or posts***, such as harassment via social media, text messaging, or phone calls.
- The final category is ***exposure of private information***, such as non-consensual intimate imagery (NCII) posted by the POC, or the POC setting up webpages or fake accounts masquerading as the survivor.

To understand the first two categories in more detail, we need a bit of background on how modern technology security works.

Devices and their security

Device is a catch-all term for phones, computers, home "Internet-of-Things"; essentially anything that has computing built in. Devices consist of hardware plus software, 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.

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 and Mac OS are the OS's of PCs and Apple computers, respectively. In each case, you can install more programs, like word processors, Internet browsers, etc. Phones and other types of devices are similar: they have an OS and the ability for users to install programs. Programs have in modern vernacular come to be called apps (short for applications).

The OS places limits on apps. For example, the OS will by default prevent an app installed on a phone (spyware/stalkerware) from reading other apps' data. What an app can or cannot do can be nuanced, and also evolves as OS's change over time.

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, POCs. 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 a POC 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.

In summary, hacking a device requires rare, expert knowledge, exceptionally so for fully updated software. On the other hand, gaining access to a device just requires the ability to unlock it. For some devices anyone can unlock them (like a laptop set to 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 a POC to unlock a device is a widespread situation in IPV. When a POC 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 POCs 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 sadly plentiful. For example, a POC might change the settings for authentication mechanisms, 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.

POCs 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 POCs 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 POC capabilities and remediations: removing an unwanted app prevents its use, changing an OS configuration fixes it.

Takeaway: POCs 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 to be safer can mitigate.

Key points:

- Hacking is a term used to cover a wide variety of computer security issues. The ability to subvert modern software in practice is exceedingly rare. An unsubverted OS places limits on what a device and apps running on it can do.
- Gaining physical access to a device to install unwanted apps or reconfigure settings is more likely, and can seriously hinder a survivor's tech safety.

Accounts and their security

Online accounts are key components of our digital lives. Email, social media, work websites, your banking accounts, and so much more --- each has an account associated to it. Your username is often (but not always) an email address.

Accounts are a prime target for abusive POCs 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 --- assuming one can authenticate themselves.

Authentication mechanisms for accounts are still predominantly password-based, though we'll see that this has been evolving. In addition we now see other forms of authentication:

- 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.
- 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 to which a challenge is sent.

In addition, there is the concept of multi-factor authentication (MFA) which is what security practitioners call having to pass multiple authentication checks, such as both entering the correct password and being able to receive a text message at a phone. Most often only two forms of authentication are required, hence the special case of two-factor authentication (2FA).

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. 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 allow users 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.

Security tools to mitigate harassment

Unlike ownership-based and compromise-based risks, the latter two categories of common tech safety problems don't involve the POC having to obtain access to a client's technology. Instead, these involve posting harmful content online, from accounts setup and controlled by the POC.

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.
- ***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 punished is often up to the peculiarities of company policy and their implementation of that policy.
- ***Takedown requests*** are a special type of report. Sometimes it helps to have lawyers assist with this effort.

One aspect that complicates these efforts is the use of spoofed accounts or phone numbers, which refers to when the POC uses an account or number that is otherwise not associated with them. For example, the POC may setup fake accounts from which to harass; if they get blocked or removed from a platform, the POC can often just set up more fake accounts. Phone numbers can also work this way,

via use of virtual phone number systems (Google Voice) or malicious spoofing applications.

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.
- ***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.

Appendix and Resources