Transgender Media Lab Safety Plan (Public)

Carleton University

Written by Aliisa Qureshi, Jada Gannon-Day, Laura Horak, Aaron Mauro, Adam Milling

Acknowledgements: Edited by Kate Higginson. Ideation and conversations by Rina Khan, Orvis Starkweather, Kit Chokly, Maddie Murakami, and Constance Crompton.

Special thanks to Aaron Mauro for meeting with us and sharing your invaluable knowledge on safety and security.

Contact: laura.horak@carleton.ca

Version 1.0
Last Modified: 23 March 2026

Table of Contents

What to Do in an Emergency

If you think you might be in immediate danger, your first lines of contact are:At Carleton: Campus Safety Services Emergency Line: 613-520-4444 (ext. 4444 from any campus phone)

In the Lab Office: Campus Safety or the panic pendant. If you press the panic pendant in the lab office, it will send a notification to Campus Safety Services. They will call the office and/or come to the office in person.

Elsewhere in Canada and US: 9-1-1

If you are not comfortable interacting with police or campus safety services: call a member of the Safety Working Group.

As soon as you are safe, call or text the Safety Working Group.

In all other cases (e.g., if you feel uncomfortable or suspect a personal threat, a cybersecurity threat, or a threat at an event), call or text someone from the Safety Working Group. The Safety Working Group will help you and the team through the protocols outlined in this plan.

We recognize that for our communities, the police or campus safety officers may bring more danger than safety. Therefore, when possible, our first approach is always de-escalation.

Dealing with these kinds of things can be very stressful and bring up feelings of anxiety, embarrassment, and shame. For information on available options and support, see Appendix C Care Plan.

Notes:

- Even if you are not on campus or in Ottawa, Campus Safety Services can coordinate an investigation and connect you with relevant resources and authorities where you are. However, if they judge that there is an unmanageable risk to you or other people on campus, they may call Ottawa police even without your consent.

- If you can't speak freely, you can call Campus Safety and leave the line off the hook and they will come investigate. If you are using a cell phone to call, you will have to indicate verbally where you are so that they can find you.

- We recognize that for our communities, the police or campus safety officers may bring more danger than safety. An understanding of these complexities is foundational to how we approached this safety plan focused on safety, autonomy, and care.
- For secure communications use phone or Signal. The team communication platform is not recommended.

Contact Information

Transgender Media Lab

Safety Working Group

Name: Email:
Mobile Phone:

Name: Email:
Mobile Phone:

Name: Email:
Mobile Phone:

Carleton

Office of Risk Management: Coordinates Carleton's Response

Name: Email:
Work Phone:

Campus Safety Services

Name: Email:
Work Phone:

Information Security

Name: Email:
Work Phone:

Access to Information and Privacy Manager

Name: Email:
Work Phone:

General Counsel

Name: Email:
Work Phone:

University Communications

Name: Email:
Work Phone:

Head of Film Studies

Name: Email:
Work Phone:

Chair of the School for Studies in Art and Culture
Name: Email:
Work Phone:

Dean of the Faculty of Arts and Social Sciences

Other

Introduction

"Safety in dominant culture terms has almost always meant protecting the interests of the powerful and maintaining the status quo. As we advocate for safety, we need to ask ourselves, safety for who? What does safety really look like? A vibrant, life-giving queer and trans rights movement must define safety not as the absence of discomfort or even the absence of risk, but as the presence of our social values. That is to say, safety as freedom. Safety as care. And safety as solidarity across difference.

The culture in which we live has taught us that in order to be safe, we must exert our will over others, that the problems of social conflict and risk can only be solved through social control, the rule of law and order, discipline and punishment. The end goal of this securitarian logic is that we become numb to violence, oppression, and even atrocities so long as they are carried out in the name of safety.

What is a vision of safety that is creative, rather than destructive? That encourages rather than strangles life? That grows out of a politic not of control and policing but rather freedom, care, and solidarity? Who do we need to become to bring that world into being?

> Safety as freedom – *the freedom to be who we are and express our truths without the fear of being punished for it.*
>
> Safety as care – *knowing that we can turn to the people around us for help when we are hurt, harmed, or in need.*
>
> Safety as solidarity – *responding to fear and scarcity by banding together rather than turning against one another.*

When I dream of a radically safe future for queer and trans people, I dream of a strong web of community that is intentionally and purposefully connected to the world around it. We bind ourselves to one another because we know we need each other not only to survive, but to thrive. We have freed ourselves from the illusion that safety is about locking people away and are grounded in the truth that safety comes from giving people what they need. All we need to do is start practicing – to start embodying safety in shapes of freedom, care, and solidarity, bound together by love."

- Kai Cheng Thom. "We Are Not Safe Till We Are Free: Redreaming Queer & Trans Safety." Substack newsletter. Kai Cheng Thom (blog), September 20, 2024. https://kaichengthom.substack.com/p/we-are-not-safe-till-we-are-free.

As Thom writes, the dominant culture assumes that we must exchange freedom for safety. We are told we must sacrifice our values for solidarity and care to be secure in our person. The rule of law demands order through discipline and punishment. This coercive, often violent, social control is a securitarian logic that requires that we become numb to violence, oppression, and even atrocities in exchange for safety. Bodily autonomy and personal freedom are expressions of truth. Creative expression in art, writing, and action is also an expression of freedom that can demand safety or celebrate it. Security is an expression of values. Communities we belong to can be overlapping, heterogeneous, and sometimes in conflict. We belong to nations, cities, and organizations that overlap systems of care that include and exclude, but we must be able to demand equity in care at all levels.

The Transgender Media Lab (TML) was founded by Dr. Laura Horak in 2020 to create an institutional home for students recruited to research trans media-making and build the Transgender Media Portal (TMP), a website and database of trans+ and Two Spirit filmmakers and their works. The purpose of the TMP is to make audiovisual work by trans+, Two Spirit, nonbinary, intersex, and gender-nonconforming people more available to artists, activists, festival programmers, researchers, instructors, and the public. We hope to promote the careers of today's trans+ and Two Spirit filmmakers, call attention to older works so they can be programmed and preserved, jumpstart research on these films, and provide artists and others with access to an innovative tradition of work.

Our lab's core values are:

- Radical Honesty & Listening
- Community-Oriented and BIPOC Trans Centred
- Challenging Hierarchies
- Care Ethics

To see more about how we determined these values and how they shape our actions in the lab, see the Transgender Media Lab Handbook on our Policies page.

We are also working to create networks with other researchers and organizers who share our values so that we can contribute to each others' collective survival.

Given these values, we embrace Kai Cheng Thom's concept of safety as freedom, care, and solidarity. We reject surveillance and colonial, carceral solutions. We commit to working with staff at Carleton University and our community partners to keep ourselves, the people we work with, and the filmmakers featured in our Portal as safe as possible, without mistaking control and policing for safety. We will undoubtedly make mistakes. We commit to growing and learning from these mistakes. This plan is a living document, and we welcome feedback at transgendermediaportal@gmail.com.

Organization and Decision-Making

Here is how our lab is structured (as of March 11, 2026): [redacted]

Image description: A diagram of the TML's organizational structure. The Community Advisory Board is at the top. Then there are four overlapping teams: the Operations Team; Community Accountability, Research & Data Wrangling (CARD) Team; Design, Infrastructure & Systems (DSI) Team, and Safety Working Group.

All safety-related incidents will be addressed by the lab's Safety Working Group (which includes the lab director) in collaboration with the person or people affected by the incident. In general, we will try to follow the lead of the affected people.

However, if the Safety Working Group judges that there is a continued threat to members or affiliates of our lab, they may choose to take additional action not directed by the affected people. We will do our best to avoid involving Campus Safety or police unless consented to by the affected people.

Likewise, if the affected person or the Safety Working Group contacts a Carleton staff member, that staff member and their team will work with us to decide on next steps together. However, you should know that if the staff member judges that that safety of the Carleton community is at risk (e.g. if there is an outstanding threat to Carleton students, weapons involved, or if you pose a risk to yourself or others), they may initiate additional action not directed by the affected people, such as contacting the police. We acknowledge that the police often pose more of a threat to our communities than anything else, and we have communicated this to the head of Carleton's Risk Management and Campus Safety Departments.

Confidentiality and Data Management

Investigation
During a Safety Incident investigation, members of the Safety Working Group may gather information from multiple computer systems and/or conduct interviews with relevant personnel. All information gathered or discovered during a Safety Incident will be **strictly confidential** throughout the investigative process. All members of the Safety Working Group are trained in information security and data privacy best practices. At the conclusion of the investigative process, the Director will brief the TML Operations Team on the relevant details of the incident and the investigation. A Post-Incident Review (PIR, see page 32 below) will be drafted by the Director and used to re-evaluate and revise this Integrated Safety Plan. During this phase, no confidential information will be shared unless it is strictly relevant to the investigation and/or the incident itself.

Affected Stakeholders
In the event the incident involves the unauthorized access or disclosure of confidential or sensitive information about lab members, affiliates, and/or filmmakers in the Portal, the Transgender Media Lab may communicate information relevant to the incident as well as any additional requested information to which they have a right (e.g. specific student records, staff records, etc.) to relevant Carleton University staff members. If the Transgender Media Lab is made aware of direct threats against lab members, affiliates, and/or filmmakers, the Director will inform those parties of the scope and substance of those threats through private communications, such as an email or telephone call. The Transgender Media Lab reserves the right to withhold certain information at the discretion of the Safety Working Group if that information may jeopardize current or future investigations or pose a security risk to the Transgender Media Lab or other entities.

In the event the incident is limited to Transgender Media Portal systems not containing confidential or sensitive information, it will be at the discretion of the Safety Working Group whether to share information related to the incident with outside stakeholders.

Communication Guidelines

Initial communication to any affected stakeholders should occur as expeditiously as possible upon the identification of the incident. This communication should be from official Transgender Media Lab or Carleton University communication channels. In some cases, this may include an initial communication (letter, email, phone call) that simply states that the Transgender Media Lab is aware of the issue and is addressing it, with the promise of a follow up.

Communication with news media will be initiated by Carleton University's Department of University Communications and/or the lab's director. Incoming news media calls and requests for information will be directed to the lab director or a designee. A communication response plan (talking points, interview refusal statement, etc.) will be formulated as needed.

How to De-Escalate

Because our communities can't count on Campus Safety or the police to keep us safe, we do our best to keep ourselves safe. One of our most important tools to accomplish this is de-escalation. The tools of de-escalation can serve us in matters small and large, from an internal disagreement to an uncomfortable confrontation with hostile members of the public. If you're on the spot, don't hesitate to grab a lab member for help. See Event Safety for how to plan in advance for these types of situations.

We are building on the teachings of a long line of social justice activists before us. This guide draws on Rebecca Godderis's training, Neighborhood Anarchist's Deescalation Skills & Mindset handout, and the Direct Action Movement's De-Escalation Skills and Tactics

Be aware of what things make you feel more stressed. If you find yourself in a situation where you don't feel comfortable, be quick to ask for help from someone else.

One of the best gifts you can give is to hold space for someone, to listen compassionately, and to bear witness. When someone shares with you something intense from their lives, validate their experience. You can say "That must have been really difficult for you" or "Thank you so much for telling me." People don't need solutions or answers as much as compassion.

Be sincere, respectful, and honest. Respect breeds respect.

Have confidence in yourself. You will not always say the "right" thing. People can feel if you are interacting with kindness and respect and their connection with you will grow. Rapport is organic and is nurtured in every moment. People are going to remember how you make them feel, not what you say. These are the principles of a community predicated on care:

- Be empathetic and non-judgemental.
- Respect personal space.
- Use non-threatening nonverbals (gestures, facial expressions, movements, and tone of voice).
- Remain calm, rational, and professional.
- Focus on feelings.
- Redirect confrontational messages.
- Set boundaries.
- Allow time for decisions.

The following strategies can be used when attending events or managing public confrontations:

- Practice with Role Play: Run a few test scenarios with event organizers to be prepared and resolve any issues in the protocol flow.
- Eye Contact: Maintain regular eye contact with event organizers or eyes on group messages to be aware of any potential situations arising.

- Pre-Established Signal: Establish a known non-verbal signal, spoken signal, and message signal that can be communicated to begin a protocol for de-escalation. For example, have a specific non-verbal signal to call for backup or support that will enter de-escalation if you are overwhelmed, and have another signal to begin emergency procedure to leave a bad situation.
- Rely on Code of Conduct: When speaking to a threat actor, calmly enforce event rules or code of conduct and ask them to leave if necessary.
- Attempt De-escalation: to have them lower their voice, stop disrupting, acknowledging concerns if appropriate.
- Offer Options to Threat Actor: participate in the event calmly, talk to event organizers calmly after the event, leave written feedback, or leave.
- Stay United: Maintain a unified and non confrontational approach, avoid overlapping speech at the disruptor.
- Divide Roles: One person leads communication with the disruptor(s), another monitors the physical safety, the crowd, etc.

After the incident is over:

- Document the situation. Capture the date and time and describe the facts of the incident in a digital document with a version history, such as iOS Notes, Google Docs, or similar. Have a witness corroborate your documentation, if speaking to the police might be necessary.
- It's normal to feel a lot of hard emotions and physical reactions after the incident is over, sometimes hours or days later. Check out Appendix C. Care Plan for strategies on how to respond to these reactions.

Procedures for Different Types of Attack

Attacks on Personal Safety

We recognize that trans artists, researchers, activists, and everyday trans people are too often subjected to harassment and attacks from individuals, politicians, police, and immigration enforcement officers.

This section outlines the kinds of attacks commonly leveled against trans people, how we try to prevent them, and what we do in case an attack occurs.

Introduction: Common Types of Attack

Attacks on personal safety can include threats to physical safety, mental health, reputation, and damage to places and things. According to the research, common incident types include:

1) Malicious Speech

- Disinformation from media and politicians
- Transphobic and sexist social media harassment
- Fraudulent Freedom of Information requests
- Complaints about the project to the school president and provost and to the project funder
- ate mail
- False claims about groups or individuals
- “Canceling” by starting mass public shaming campaigns directed at us as individuals or as a group
- Email and social media contact (team accounts, personal accounts): These may include threats, insults, or disturbing images.[1]
- Publishing names, faces, addresses on media without consent (“doxing”)
- Reporting us to police for "child grooming" or other bogus accusations
- Targeting team members' other projects
- Writing to institutions we’re affiliated with, defaming us[2]
- Threatening lawsuits against us
- Weaponizing social justice and anti-oppression movements to launch targeted attacks (i.e., targeting pro-Palestine team members with accusations of antisemitism)[3]

[1] Image-based sexual harassment and cyberflashing are frequently targeted at women online, often in response to their political advocacy surrounding gender, race, and queer identity (Center for Countering Digital Hate, 2022).

[2] In 2021, Cecelia Lewis was intensely harassed, often with racist and misogynistic false claims, for her diversity, equity, and inclusion (DEI) initiatives in the school board in which she was employed (Carr, 2022). Like numerous other black women targeted for their DEI work, Lewis was unsupported by her institution and eventually chased out of the school board (Carr, 2022).

[3] Canary Mission is one such example, known for naming, gathering the personal information of, and publicly targeting university students and faculty who publicly support Palestine or critique Israel

- Misrepresenting the site as “grooming” children into the “transgender lifestyle”[4]
- Pressuring SSHRC or other project funders to reduce funding for projects like these
- Wide-reaching Gamergate-style[5] attacks from people who might not have a strong ideological drive but want to cause chaos
- Revenge porn, sextortion, claiming to have accessed a target's web camera without their knowledge, threatening to release embarrassing images and personal information if instructions are not followed.

2) Threat of physical harm
- Doxing: tracking down and sharing private information, including phone numbers and home addresses
- Showing up at home, office, or places of work
    - stalking
    - yelling
    - threatening
    - injuring (ranges from pushing & punching to attacks with knives or guns)
- Bomb or Bomb threat
- Swatting and fake “wellness checks”: falsely reporting a threat such as a bomb threat, mass shooting, domestic violence, murder, hostage situation, or mental health situation to instigate a dangerous and potentially violent response from emergency services[6]
- Surveillance to stalk, follow, and/or monitor individuals.
- Spyware and stalkerware, including sophisticated programs like Pegasus
- Location tracking: AirTags, Find My, location tagged photos/videos, reverse image search, and Google Reviews are all capable of leaking your location in real-time or near real-time
- Unwanted touching, threats of sexual violence, and sexual harassment (eg. repeated and/or unwanted questions about genitals).

3) Destroying or stealing money, equipment, information
- Ransack lab office, director’s office, any other team members' offices
- Use HR info to steal our identities or to steal money from us

---

(Rothchild, 2020). Students targeted on the website have cited loss of opportunity and income, harassment, and threats of violence as harms done by the organization’s targeting (Rothschild, 2020).

[4] Abigail Shrier warns parents about trans influencers online brainwashing young women (Shrier, 2020). Also, in 2022, the American Academy of Pediatrics (AAP), American Medical Association (AMA) and Children’s Hospital Association (CHA) wrote a joint letter to the Attorney General and Department of Justice to investigate threats of violence targeted at children’s hospitals providing trans health care (Luneau, 2022).

[5] “Gamergate” was a hashtag movement in which women and feminists in game development, reporting, and analysis were systematically targeted, with the attacks tied to misogynistic conspiracy theories about women in a male-dominated industry (Massanari, 2017; Mortensen, 2016). During the harassment campaign, women, feminists, and their perceived allies were victimized with doxxing, threats of sexual violence, bomb threats targeted at public events, and more (Jankowicz, 2022).

[6] In 2023, Ontario transgender streamer Clara Sorrenti was arrested at gunpoint, misgendered, and deadnamed by London police after having her address leaked and police falsely called by online adversaries.

- Infiltrating our systems, collections, to cause chaos or gather intelligence for fascist groups
- Hack and leak our shared file storage and publish everything to defame us, the lab, & Carleton
- See cybersecurity policy for more on stealing passwords, data, etc.

4) Other
- Targeting by state-level threat actors (politicians, police, secret police, etc.)[7]
- State-level threat actors using information from the Portal to target trans people in their areas
- Infiltrating our networks and platforms to cause chaos, distrust, and discord within our community or gather intelligence for fascist groups[8]

These different categories are porous and can lead to each other. For example, malicious speech online can lead another person to publicize our addresses and yet another person showing up at our home or office and physically harming us. And threats of physical harm have mental health repercussions even if the threat is not carried out.

For more information on the types of attacks trans activists in Canada regularly experience, see JusticeTrans's "Understanding & Fighting Back against the Anti-Trans Movement in 'Canada'" in Appendix G.

Prevention

How to prevent attacks on personal safety? Being visible as a trans project is essential for achieving the project's goals–celebrating and circulating trans-made films. However, visibility also puts one at risk. In many cases, threat actors do not need to have any information beyond what is publicly available to carry out threats: e.g., the names of people in the lab, lab affiliates, and filmmakers in the Portal; our affiliated institution; the lab's email address and social media handles; and filmmakers' social media handles. Other threats require additional information such as team members' personal email addresses and social media handles.

Only a few threats require confidential information such as home and office addresses and passwords. While we try to keep confidential, sensitive, and internal data safe to prevent those types of threats, we cannot prevent the threats that only rely on public information. All we can do is prepare to respond quickly and effectively.

---

[7] Florida governor Ron DeSantis has banned textbooks, dictionaries, and lecture topics from Florida public schools and universities due to their content on race and gender. Provinces like Saskatchewan and Alberta have also introduced anti-trans policies over the past year (Long, 2024; Amnesty International, 2024).

[8] See, for example, Cervini, Eric. *Spying Before Stonewall: How the FBI Secretly Tracked Gay Activists in the 60s*. June 8, 2020. https://www.vice.com/en/article/the-fbi-secretly-tracked-gay-activists-in-the-60s/; 1. "Ghetto Informant Program," Wikipedia, July 5, 2025, https://en.wikipedia.org/w/index.php?title=Ghetto_Informant_Program&oldid=1298852561.

To prevent incidents, all members of the lab are required to follow the Zebra Crossing digital safety checklist Levels 1 and 2. Members will use multi-factor authentication (MFA) for all accounts, where available. See Attacks on Cybersecurity for more information on digital safety.

In our grants, we will budget for mental health support and adequate time off for researchers in the lab. We oppose casualization by creating jobs that pay fairly.

Before doing anything that we garner publicity for the project, we will:

- Brief our chair, dean, Coms, and the office of risk management to explain why we are at risk and to prepare them for any complaints.
- Notify our partner organizations and build a coalition of authoritative public facing institutions to build resiliency.
- Work with University Communications to prepare press statements designed to anticipate and counter disinformation. We will create a simple key message, written for those who care about the topic and are interested.
- Develop a response plan with pre-prepared press statements in the event of a hostile response that features disinformation, false claims, or defamation.

Detection

In many cases the threats will be easy to detect, such as if a person sends us an email or shows up at our door. However, sometimes the threats will not present themselves so blatantly.

How we identify more subtle threats:

- Use Google Alerts on the name of the lab, the portal, the names of the lab members, as well as “trans” + Ottawa and “trans” + Carleton.
- Before public events and launches, have lab members review rightwing forums looking for evidence that the lab/portal will be targeted. (See Event Planning protocol for more on this.)
- Stay up to date on anti-trans movements and movement actors in Ottawa, Ontario, Canada, and North America. Save documentation in a separate encrypted folder in our shared file storage. Print web pages to PDF to include date and time.
- Recommend that team members check bank accounts and credit card statements every month for unusual activity.

More information about what to do if you have a compromised device or account can be found in the Care Plan.

Assessment

Once threatening activity has been detected, the lab’s Safety Working Group will work with the person affected by the threat to collaboratively decide on next steps.

The first step is to determine the **level of intervention** required.

Considerations

- Likelihood: What is the likelihood that the threat will take place?
    - Unlikely: little precedent and few favourable conditions to facilitate them
    - Likely: clear precedents and/or favourable conditions to facilitate them
    - Unclear: low information masks potential threat, but it remains important to err on the side of caution
- Impact: What is the potential impact of a harmful event?
    - How many people are affected?
    - How long-lasting is the effect?
- What other harmful situations does it enable?
    - Is there danger to others, who may not be directly targeted?
- Adversary: Identify the person/organization/entity behind the threat. Consider their capabilities, their limitations, and their history of past hostile actions.
- Target: identify all potential targets of the threat, including information, systems, and people. Consider physical, emotional, and financial harms as well as harms against reputations.
- Resources - What resources and information is needed to carry out an attack? Where might they get this information?
- Opportunity and ability - Where and when might the attack take place?

Response (See also Care Plan)

In the case of an incident, responses to many different aspects of the incident's impact will need to be considered. These include:

1. Physical safety
2. Mental health
3. Reputational harm
4. Damage to things
5. Accountability/restorative justice for the person doing the harm (when possible)
6. Prevention of further harm (when possible)

The Safety Working Group and affected person will work together to determine the most appropriate response. We will take care to ensure that mental health support is available to all lab members affected by the incident. (We recommend that the affected person review the Care Plan, which explains resources for trauma-informed support.) We will also determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so.

Initial Response

If there is an imminent physical threat, the affected person (or people) should call Campus Security (if on campus) or 911 (if off campus) or a trusted friend or family member.

If there is malicious speech addressed to an institutional or personal social media account, that account and all related accounts should immediately be made private. (See Appendix E)

Throughout this process, it will be critical to preserve all possible evidence and document all measures taken in detail. These reports should be saved in an encrypted file only accessible to the Safety Working Group.

Remediation and Recovery

Once the cause has been determined, the Safety Working Group will work to address harm caused and prevent future harm. (Again the affected individual should see the Care Plan for how to take care of themselves and heal from the incident.)

Potential actions include:

- Report incident to:
    - 9-1-1
    - Ottawa Police
    - Ontario Provincial Police
    - Federal Cyber Centre: https://www.cyber.gc.ca/en/incident-management
    - Carleton Campus Safety
    - Carleton Risk Management
    - Carleton ITS Security
    - Carleton Equity and Inclusive Communities
    - Carleton FASS Dean
    - Carleton's General Counsel and/or Access to Information and Privacy Manager
    - Social media platform (e.g. Facebook, Instagram, Bluesky)
- Track how the incident evolves.
- Set social media accounts to private (See Carleton's Guidelines to Social Media.)
- Block offending account(s).
- De-escalate. (See How to De-Escalate.)
- No response.
- Work with the Department of University Communication to:
    - Write up a statement and release it strategically on our social media and email listserv (e.g. on LinkedIn, not X).
    - Create a press release and send it to the media.
    - Monitor social media commentary.
    - Monitor email inboxes.
    - Remove contact information from all university websites.
    - Filter media requests.
- Work with University Safety to monitor on-campus offices around key dates.

Documentation

Regardless of whether it is determined there is a security threat, the Safety Working Group will accurately document the scenario in a Security Incident Log, which is saved in an encrypted file only accessible to the Safety Working Group. All Security Incident Logs will be stored in a single location so incident information may be reviewed in the future.

This report should contain information such as:

- Who reported the incident
- Characteristics of the activity
- Date and time the potential incident was detected
- Nature of the incident
- Potential scope of impact

See Appendices for Incident Log and Incident Report Templates.

Attacks on Cybersecurity

Cybersecurity is a team sport. We all have a role in maintaining the security of our research data, infrastructure, and associated information. As our lab's central project is a website and we host many of our lab's files online and on our personal computers, we are vulnerable to cybersecurity attacks.

Our Cybersecurity plan is based on the NIST Cybersecurity Framework (see Further Reading). Carleton University ITS has not given us permission to use their processes and forms directly. However, we have access via the AVRC CSU (computing services unit), so we are aligned and in liaison with Carleton ITS processes.

Introduction: Common Types of Attack

Types of cyber incidents that may threaten the organization are:

- Unauthorized attempts to gain access to a computer, system or the data within
- Service disruption, including Denial of Service (DoS) attack
- Unauthorized access to critical infrastructure such as servers, routers, firewalls, etc.
- Virus or worm infection, spyware, or other types of malware
- Non-compliance with security or privacy protocols
- Data theft, manipulation, alteration, or corruption (including misgendering and misnaming filmmakers in the Portal)
- Unauthorized distribution of data, including doxing attack
- Phishing, baiting, and other forms of social engineering attacks on users or participants
- Theft of passwords to break into team or personal accounts, enabling not just data theft but the potential to steal identities and funds

Prevention

To prevent incidents, all members of the lab are required to follow the Zebra Crossing digital safety checklist Levels 1 and 2. Members will pay special attention to the following requirements:

- All members will use multi-factor authentication (MFA) on all accounts, when available.
- All members will use unique passphrases for each account used in the course of research activities.[9]
- All lab passwords will be stored on the team's password manager.
- All lab members are *strongly* recommended to use password managers for their personal accounts as well, including their personal email accounts.
- Lab members will not use the communication platform desktop app, but instead access it on their web browser.
- Members will check https://haveibeenpwned.com once per semester to determine whether their accounts and/or passwords have appeared in data breaches.

[9] Communications Security Establishment Canada. "Best Practices for Passphrases and Passwords (ITSAP.30.032)." Canadian Centre for Cyber Security, September 17, 2019. https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032.

- Remote Desktop Protocol (Microsoft RDP) may never be used by members.

The team will decide on a pre-arranged code, signal, or phrase to communicate a compromised device or account without alerting the attacker. Examples of simple signal phrases could be "_____" or incorporating a specific emoji into a message.

Crossing Borders

When travelling to hostile legal jurisdictions such as the United States, members will limit access to research materials on digital devices. Because normal legal rights are suspended in border crossings, it is reasonable to expect search and seizure of mobile devices, laptop computers, and mobile devices. Research files and member contacts should not be stored on devices as static files during travel. Research materials should be accessed remotely during travel, using standard secure authentication methods. Border agents cannot compel individuals to log into services, so members must log out of all online services on a laptop. Removable media, such as a harddrive or flashdrive (USB key), should be encrypted or simply not taken on trips to hostile jurisdictions. Mobile devices should be in "lock down" mode and locked with bio-authentication systems. See the following documentation for locking down your devices for Android or iOS. Devices should remain password protected, encrypted, and in "lock down" for the duration of your visit.

Protecting the Server

Our service provider, _____, recommends enabling additional logging, automated server backups, and Fail2Ban, as well as setting up a firewall. Based on our project's specific needs, we have set up a firewall and also turned off password access to the server.

Detection and Assessment

All team members, regardless of their duties, should be on the lookout for the following symptoms on their personal computers and the lab's servers.

Signs a computer may have been compromised include:

- Abnormal response time or non-responsiveness
- Unexplained lockouts, content, or activity
- Locally hosted websites won't open or display inappropriate content or unauthorized changes
- Unexpected programs running
- Lack of disk space or memory
- Increased frequency of system crashes
- Settings changes
- Data appears missing or changed
- Unusual behavior or activity by staff, students, partners or other actors
- Unprompted authentication requests through MFA, either in app, text, or email notifications

Signs a cell phone may have been compromised include:

- An attacker's access to the device
- Strange activity on the device including a rapid change in battery life
- Consistently dropped calls
- The phone shutting down
- References to personal information like text messages, files, and photos

If you receive an email that seems to be from one of your own accounts, you can check whether it is real by clicking into your "Sent" and "Trash" email folders on the targeted account to determine whether the email was sent from your account. If the email is not in your folders, the attacker is likely not in your account but has instead mirrored the account to make it look like they are in your account. Do not click any links in the email or respond.

The project Web Developer will maintain current logs and backups of all server content and activity for one year at minimum. These logs and backups will be used to verify a breach, respond to an active attack, evict attackers, and restore damaged systems.

Once anomalous activity has been reported, it is incumbent upon the Safety Working Group to determine the level of intervention required. Other members of the Safety Working Group may be required to provide input during this phase to help determine if an actual security threat exists. If it is determined there is an active security threat or evidence of an earlier intrusion, the Director will alert the entire Safety Working Group immediately so that the situation may be dealt with as expeditiously as possible.

Security Incident Reporting

If you witness suspicious activity or behaviour on your personal or lab computer or software, please report a security incident to the Safety Working Group as soon as possible. In an email addressed to the SWG members, answer the following questions to the best of your ability:

- What are the symptoms?
    - Describe software behaviour and potential causes with screenshots, if possible.
- What is the time and date of the suspicious behaviour?
    - Providing specific dates and times will assist in assessing log data.
- What software is your computer running?
    - List your operating system, browser, browser extensions, and other software and settings. Please include software version numbers if possible.
    - What may be the cause?
- What project systems have been/are being/will be impacted?
    - Consider digital assets such as our shared file storage, our server, our Git repository, our listserv, and all associated hardware. How widespread is it?
- Which project stakeholders are affected?
    - Please include contact information, if possible.

Response

Upon determining that a significant incident or breach has occurred, the Safety Working Group will notify Carleton ITS Security and server provider immediately. As additional information is uncovered throughout the investigation, the Safety Working Group will brief Carleton ITS Security and server provider so appropriate decisions, such as allocating additional staff, hiring outside consultants, and involving law enforcement can be made. Additionally, based on the incident, it will be incumbent on Carleton ITS Security and Carleton's Access to Information and Privacy Manager to determine the appropriate stakeholders to notify of the incident and the appropriate medium to do so.

The Lab Director will document all interactions with internal and external partners to develop a timeline of events for the PIR process to follow.

Carleton staff should take into consideration the nature of the information or systems involved, the scope of the parties affected, timeliness, potential law enforcement interests, applicable laws and the communication requirements of all parties involved.

Compromised Personal Device

If you suspect one of your personal devices may have been compromised:

- Some steps taken to secure an account might notify an attacker that you have made changes to your account or device, such as removing a phone number or adding two-factor authentication to the compromised account/device. Before making changes, evaluate whether these changes might alert the attacker. If you anticipate retaliation, prioritize physical safety first and seek support.
- Use an alternate device, friend's phone, or a secure account to contact support, avoiding direct actions on compromised accounts.
- If you must use the compromised device, use a prearranged code, signal, phrase, or emoji to alert the Safety Working Group.
- Amnesty International offers tools and guides to determine whether your device has been compromised.
- The best way to preserve the phone as evidence is to put the device into airplane mode and keep it charged without using it.
- Going to the police can be challenging and is not the best option for every person being targeted. If you decide that this is not the best option, factory resetting the phone can remove some spyware.
- To replace the device – the safest option – contact your local Victim Services, Sexual Assault Centre, or another relevant social service agency to determine whether they have emergency device funds.

If you are concerned that stalkerware or another digital technology has been targeted at you as a form of intimate partner violence, stalking, or sexual harassment, please see the Coalition Against Cyberstalking's Resource List, the Clinic to End Tech Abuse's Get Help, and Lila.Help's list of resources for victims of domestic violence by region.

Initial Response

The first steps in any cyber incident response should be to determine the origin of the incident and isolate the issue. This may involve the immediate disconnection of workstations, servers, or network devices from the network to prevent additional loss. While this is occurring, it is necessary to examine firewall and system logs, as well as possibly perform vulnerability scans, to ensure the incident has not spread to other areas in order to define the entire scope of the incident.

The TML Web Developer will work to:

- gain immediate access to affected systems and force all authenticated accounts to perform a password reset, using passphrases and MFA procedures;
- gain immediate access to system logs and download them to an unaffected system;
- immediately ensure the safety of all system backups and ensure they are stored on an unaffected system.

Throughout this process, it will be critical to preserve all possible evidence and document all measures taken in detail. Thorough review and reporting on the incident will be required once the threat has been removed, the vulnerabilities have been removed and the systems have been restored.

Please note, if affected systems include typical communications channels like email, the Safety Working Group will update all team members on alternate, safe communications during this time. Upon resumption of normal activities, the Safety Working Group will provide guidance regarding secure communications.

Remediation and Recovery

Once the cause has been determined and appropriately isolated, an ad hoc **Remediation and Recovery Team** will need to remove the vulnerabilities leading to the incident. This team will likely consist of the TML Web Developer, members of the DSI Team, and members of Carleton's Information Technology Services team. The team's work may involve some or all of the following:

- Install patches and updates on systems, routers, and firewalls
- Infections cleaned and removed
- Re-image or re-install operating systems of infected machines
- Change appropriate passwords
- Conduct a vulnerability scan of any compromised machines before reconnecting them to the network
- Restore system backups where possible
- Document all recovery procedures performed and submit them to the Director
- Closely monitor the systems once reconnected to the network

Documentation

Regardless of whether it is determined there is a security threat, the Remediation and Recovery Team will accurately document the scenario in a Security Incident Log. All Security Incident Logs will be stored together, with separate backups, so incident information may be reviewed in the future.

This report should contain information such as:

- Names and contact information for all team members
- Security Incident Report (above)
- Detail all the remediation and recovery steps
- Incident Status (active, closed, monitoring)

See the Appendices for the Incident Log and Incident Report Templates.

Technical Incident Protocol

This Technical Incident Protocol gives the practical steps to follow the Cybersecurity Incident Response Plan as described earlier in this document: Identify > Detect > Respond > Report > Review.

1. Emergency Preparation
    a. Currently, the primary lead for technical incidents is the TML Web Developer.
    b. If the primary lead is not available, another primary lead will be arranged and notified.
    c. For secure communications use phone or Signal. The team communication platform is not recommended.
2. Emergency
    a. In the case of an active and ongoing emergency, contact the primary technical lead. Keep trying to contact members of the Safety Working Group until a response is received.
    b. If not already done, the lead notifies the DSI Team that an emergency is in progress.
    c. The lead deals with the emergency, getting help as needed including from Carleton ITS and the server service provider. The technical lead updates the Safety and DSI Teams as needed.
3. Logging
    a. Log the incident on ___.
    b. Create an entry in the Incident Log.
    c. If the incident needs to be tracked for follow up actions, then also create a related task in the tracking system, which is the Strategic Action Plans at the top of the Safety Working Group Agenda + Minutes.
    d. The Strategic Action Plans also contains the current list of all security tasks that require follow up.
4. Reporting

    a. If the incident requires a report, create an incident report document from the template. Use the same file name convention as other documents in the folder.
    b. Turn on document history to track changes in the document (auditing).
5. Review
    a. At every meeting of the Safety Working Group, all open incidents are reviewed as part of the standing agenda. This meeting must occur at least once every three months.

Event Safety

Unfortunately, anti-trans actors often use public events, both online and in person, to attack trans people and organizations. We prepare for these kinds of attacks in advance so that we know what to do if something happens. We can keep our lab members, invited guests, and attendees as safe as possible by following these guidelines.

Introduction: Common Types of Attack on Event Safety

Common types of incidents that threaten participant safety include:

At In-Person Events

- Filming/recording the event for public shaming
- Counter-demonstration: threats, physical violence, loud music, preventing people from entering/leaving
- Audience member(s) disrupting event: yelling, threatening, making a scene, offensive actions, harassing
- Bomb threats or attack, mass shooting
- Physical damage or threat to the event space
- Venue disruptions, fraudulent or real: canceling the event or changing location last minute to sabotage or prevent large attendance
- Intimidation: pressuring event partners/host/conference organizers to defame the TML and its members or remove TML or its members from event
- Someone is upset or triggered by the content
- Someone asks an inappropriate question in Q&A
- Escalated individuals who are not registered
- Escalated individuals in Q&A
- Sexual harassment

At Online Events

- Filming/recording the event for public shaming
- Recording attendees' names for malicious purposes
- Zoombombing: disrupting, yelling, threatening, offensive actions, harassing, broadcasting offensive images and videos
- Host disruptions, fraudulent or real: canceling or interrupting the event
- Intimidation: pressuring event partners/host/conference organizers to defame the TML and its members or remove TML or its members from event

- Someone is upset or triggered by the content
- Someone asking an inappropriate question in Q&A
- Escalated individuals who are not registered; yelling
- Escalated individuals in Q&A

Prevention (See also Event Planning Checklist)

To avoid incidents, safety planning is integrated in all steps of event planning from development to coordination to execution. We plan our events with attention to the following:

- Environmental Scanning:
    - Content: Are the guests or topic considered 'controversial'?
    - Location: Are there anti- rallies happening in the locale?
    - Environment: Have there been incidents at other similar events locally or currently? What safety lessons can we implement from them?
    - Overall: What is the level or perceived risk and concerns, and how can we increase safety?

- Selecting a Venue
    - Do you have the right to ask people to leave? Can anyone come in? Is there open access to the building or room?
    - Choose venues with multiple exit routes.
    - Be aware of their security options and connect with on-site security.
    - Choose spaces with accessible exit plans and safety plans.
    - Is it an evening or day event, and how far is parking/public transportation - considering safety of people arriving and leaving the event.

- Planning with Guest Speakers and Co-Organizers
    - Ask them about their security and safety concerns, needs, past experiences, and what we can generally do to make them feel safe.
    - Inform them of safety plans so they are not panicked or lost.
    - What is their comfort level in Q&A panels? Are there questions they will not respond to? Do they want a facilitator to respond to those questions and to disruptors?
    - Have your questions peer reviewed.

- Examining the Role of Law Enforcement Services
    - Have explicit discussions prior to an event on the role and need for law enforcement services: understand what actions various law enforcement services are authorized to take that the event organizers would be unable to act on their own (e.g. escorting people out of the venue).
        - If you decide that security/police have a role, have a clear plan to keep people who are typically targeted by security/police feeling safe and comfortable.

        - The event organizers should be knowledgeable on their rights as well as the rights and limits of law enforcement services they choose to include.
    - Identify the Emergency Contact Protocol of who will be called and when, by whom, and in what order. Prior to the event, assign day-of roles. Have this readily available and downloaded offline for the event organizers during events.
    - Options: Campus Security, Police/911, venue security, trained personnel, other backup contacts/ideas?

- Assigning Day of Roles to Organizers
    - Facilitator: Primary speaker who actively guides the audience through the event, mediating and engaging with both audience and special guests. They would maintain control of the event while de-escalation is taking place, or perform de-escalation techniques themselves.
    - Co-Host: Supporting the Facilitator, the Co-Host may also speak to, mediate and guide audiences and special guests, and support by beginning de-escalation or maintaining control of the room during de-escalation.
    - Security Monitor: A person who is positioned with a clear view of the activity in the event room and doorways, with easy access to act and signal other organizers. They would try de-escalation techniques off the stage, so that the Facilitator can focus on regaining control of the room.
    - Guest Liaison: The main point of contact for artists and special guests when they arrive at the venue. They will let guest speakers know where they need to be, where exit routes are, and will communicate directly with and escort guests during an emergency.
    - Peer Support: Someone available to provide help, guidance, and emotional support in the event of a crisis.
    - Medic/First Aid Liaison: Someone equipped for emergency physical care and/or the first person to contact ambulances and other emergency health services. This is important to assign to avoid multiple or delayed calls to emergency services in the event of a crisis.

- Special Considerations for In-Person Events
    - Create registration for the event.
    - Limit disclosure of the time and location of the event (registrants only, days before event, etc).
    - Screen audience questions and participation through mediation, submitted written questions/Slido/QR code, etc.
    - Take a headcount at the beginning and occasionally to be aware of changes. If there is a registration list can confirm with the number registered.
    - Maintain communications in event organizers group messaging so that the team is all aware of potential threats and we have documentation.

- Special Considerations for Online Events
    - Create registration for the event.

- Create a passcode, waiting room, or other form of authorization to control event access.
- Limit disclosure of the time and location of the event (registrants only, passcode day of event or days before event, etc).
- Limit video and audio controls for participants when appropriate.
- Turn off general chat.
- Screen audience questions and participation through mediation, submitted written questions/Slido/QR code, etc.
- Maintain communications in event organizers' group messaging so that the team is all aware of potential threats and we have documentation.

When to Cancel the Event
Throughout the event planning process, should the likelihood of threats to physical or emotional safety appear extremely high, cancel the event before an incident occurs. It is never too late to cancel or adjust logistics of an event in the interest of safety.

Detection and Assessment

All lab members involved in an event will be on the lookout for any possible incident. In addition, we may assign additional Safety Monitors to the job of keeping an eye out for safety incidents. In many cases, it will be obvious when an incident has started. Review the Common Types of Attacks to be aware of common suspicious behaviours.

Response

Our main priority with any incident is to de-escalate the situation and to keep organizers, guests, and attendees safe from harm. After the incident, we recommend that all affected people consult our Care Plan.

The first step is always to **assess the severity of the disruption/threat.**

For In-Person Events

If the incident is something that the event organizers can handle, we will proceed into the De-Escalation Protocol:

- Calmly announce we are going to use a security protocol and begin.
- Lock the venue so no new people can enter.
- Begin de-escalation:
    - Stage Area: If the disruption is near the stage, the Facilitator may initiate de-escalation.
    - Other Areas: In other cases, the Security Monitor will begin de-escalation. If backup is needed, Peer Support or another designated person will assist with de-escalation. The remaining event organizers should monitor the situation

without overlapping voices to avoid distracting the disruptor from the de-escalation process.
    - De-escalation: calmly enforce event rules and code of conduct (disruptors will be asked to leave).
        i. Security Monitor or Facilitator (whichever is not engaged), Co-Host, Peer Support and Medic on standby to engage Emergency Contact Protocol.
    - If a minor interruption, offer options to the disruptor(s): participate in the event calmly, talk to event organizers calmly after the event, leave written feedback, or leave peacefully.
    - If uncooperative, offer to escort disruptors out of the venue peacefully. Avoid touching to prioritize safety.
    - If a major interruption or situation becomes hostile, signal/announce and initiate Emergency Contact Protocol.
- Proceed to Remediation and Recovery Step 1.

If the incident is <u>beyond</u> what the event organizers can handle or regain control from, we will proceed to the Event Ending Protocol:

- Calmly announce the event will be ended to prioritize everyone's safety and comfort.
- Announce emergency protocols have been engaged: initiate Emergency Contact Protocol.
- Depending on the situation, Facilitator asks everyone to remain seated or guides attendees toward the exits in a safe and orderly fashion. Guest Liaison relays the emergency to guests and directs guests to remain seated or exit safely. Encourage everyone to remain calm and avoid rush or panic. Ensure vulnerable individuals are taken care of by the Co-Host, Security Monitor, or Peer Support.
- Take headcount before and after evacuating to see if everyone has been safely evacuated.
- Proceed to Remediation and Recovery Step 3.

For Online Events

If the incident is something that the event organizers <u>can</u> handle…

- Calmly announce we are going to use a security protocol and begin.
- Host/Co-host: Go to Host tools -> Suspend participant activities. This turns off and locks all mics & videos and also automatically locks the meeting so no new people can join.
- Begin De-escalation:
    - Calmly enforce event rules and code of conduct (disruptors will be asked to leave)..
    - If a minor interruption, offer options to the disruptor(s): participate in the event calmly, talk to event organizers calmly after the event, leave written feedback, or leave peacefully.
    - If a major interruption, remove/kick the disruptor(s).
- Proceed to Remediation and Recovery Step 1.

If the incident is beyond what the event organizers can handle or regain control from…

- Calmly announce the event will be shut down to prioritize everyone's safety and comfort and then end the meeting for all.
- Proceed to Remediation and Recovery Step 3.
- Lab director to formulate a plan to release an update on the situation, or respond accordingly.

For Online Lab Meetings

If the incident is beyond what the meeting facilitator can handle or regain control from…

- Immediately shut down the Zoom meeting and regroup on our communication platform.
- Proceed to Remediation and Recovery Step 1.

Emergency Contact Protocol

Establish clear procedures for determining who will contact emergency services, when to do so, who will make the call, and in what order.

For example:

Initiating Emergency Contact Protocol: Use a distinct non-verbal, verbal, or written signal to activate the emergency protocol, separate from regular incident procedures. The Facilitator will signal to the event organizers and announce the activation of emergency protocols. They should maintain a calm demeanor to help keep the room orderly, continuing to facilitate or act as a point of contact for questions.

Contacting Emergency Services

- If de-escalation by Facilitator or Security Monitor fails or the situation escalates into a greater safety threat, the Security Monitor (1), Co-Host (2), Peer Support (3), or First Aid/Medical Liaison (4) —whichever is least preoccupied, in the safest position, and least vulnerable to police violence—will contact the designated security contact or law enforcement and relay messages.
- For health emergencies, the Medic/First Aid Liaison will call 911 and relay messages. If no Medic/First Aid is available, the Peer Support, Security Monitor, or Co-Host —whichever is least preoccupied, in the safest position, and least vulnerable to police violence—will cover this role.
- For mental health emergencies, Peer Support will be on-site in a known location, clearly identified by a tag or sign. They will decide whether to call the appropriate emergency service or 911 and will have themselves or someone in the best position make the call and relay messages. If no Peer Support is available, the Medic, Security Monitor, or Co-Host —whichever is least preoccupied, in the safest position, and least vulnerable to police violence— will cover this role.

Communication: Always notify the group if someone has contacted emergency services, especially if the call was made by someone outside of the event organizers.

Remediation and Recovery

Once the incident has been de-escalated and order restored:

Step 1: Check in with the remaining participants and discuss whether the event can continue.

Step 2: Inform and direct participants to the appropriate channels if they need or want support following the incident.

Outcome #1: Continue the event.

Outcome #2: End the event in a calm and organized fashion.

Step 3: The event organizers regroup as soon and safely as possible in order to document the Incident Report accurately and to begin facilitating support for the team/affected individuals.

Step 4: Lab Director determines the appropriate public communication and formulates a plan to engage with University Communications, release an update on the situation, or respond accordingly.

Documentation

After the incident has been addressed and the event has concluded, the event organizers will gather all available information to create a comprehensive and accurate summary using the Incident Report Template. During this reporting process, we prioritize minimizing further harm and ensuring the care and wellbeing of those affected. This report serves as a record for the protection of those impacted, and we recommend including a witness to attest to the account.

Report Contents

The Incident Report Template will include all pertinent information to the incident, but at minimum we will document the following:

- Date, time, location of incident
- Description of the incident
- Description of actions taken
- Involved parties
- Witness information
- Reflection and follow up (to be completed in the next Review step)

Post-Incident Report and Review

Once the threat has been mitigated and normal operation is restored, the Safety Working Group will compile all available information to produce an accurate and in-depth summary of the incident in an **Incident Summary Report (ISR)**. Throughout the incident, the Safety Working

Group will have kept Incident Logs that contain detailed records wherever possible, and these shall serve as the basis of the report. Interviews will also be conducted with appropriate members of the Safety Working Group to obtain any additional information that may be available to augment the logs and records kept throughout the process.

Report Contents
The Incident Summary Report (ISR) will include all pertinent information to the incident, but at minimum:

- Dates and times of milestones throughout the process (e.g. incident detection, verification, notifications, remediation steps, completion, etc.)
- List of symptoms or events leading to discovery of the incident
- Scope of impact
- Mitigation and preventative measures
- Restoration logs
- Stakeholder communications (including copies of memos, emails, etc. where possible)

Timeframe
The ISR should be prepared as expeditiously as possible following the incident so future preventative measures may be taken as quickly as possible. Information to prepare the ISR and interviews with the Safety Working Group should be conducted immediately to ensure the greatest possible accuracy of information.

Post-Incident Review Meeting
After the conclusion of the incident, the Director and possibly select members from the Safety Working Group will meet with management to discuss the event in detail, review response procedures and construct a Process Improvement Plan (PIP) to prevent a recurrence of that or similar incidents. The compiled Incident Report constructed by the Director will serve as a guide for this meeting.

In the meeting, a full debrief of the incident will be presented and findings discussed. The Director will share the full scope of the breach (as comprehensively as possible), causes of the breach, how it was discovered, potential vulnerabilities that still exist, communication gaps, technical and procedural recommendations, and the overall effectiveness of the response plan. As a whole, the group will review the information presented and will determine any weakness in the process and determine all the appropriate actions moving forward to modify the plan, address any vulnerabilities and what communication is required to various stakeholders.

Process Improvement Plan
The Director will draft a **Process Improvement Plan (PIP)** based on the results of this meeting. The plan should discuss any applicable items necessary to prevent future incidents to the extent practicable, including cost and time frame requirements where possible. The PIP will also include a review strategy to ensure all recommendations made in the PIP are met in a timely fashion and functioning appropriately. Areas of focus may include, but are not limited to:

- New hardware or software required

- Patch or upgrade plans
- Training plans (Technical, end users, etc.)
- Policy or procedural change recommendations
- Recommendations for changes to the Incident Response Plan
- Regional communications recommendations

Additionally, the PIP must be kept strictly confidential for security purposes. Any communication required to clients or to the public must be drafted separately and include only information required to prevent future incidents.

Further Reading

Dunn, Suzie, Julia Falco, Chanel Grenaway, et al. Challenging Gendered Digital Harm: Research Report on Impacts and Solutions to Digital Harm Facing Women, Gender-Diverse People, and Gender Equality Organizations. Canadian Women's Foundation, 2025. https://canadianwomen.org/wp-content/uploads/2025/05/25-18_CWF_GenderedDigitalHarm_ENG_Mainreport_v14.pdf

Marwick, Alice, Dafna Kaufman, Jacob Smith, et al. *An AoIR Guide to Researcher Protection and Safety*. 2025. https://aoir.org/riskyresearchguide/.

National Institute of Standards and Technology. "Cybersecurity Framework," November 12, 2013. https://www.nist.gov/cyberframework.

National Institute of Standards and Technology. "CSF 2.0 Profiles," February 20, 2024. https://www.nist.gov/cyberframework/profiles.

National Institute of Standards and Technology. "The NIST Cybersecurity Framework (CSF) 2.0." Gaithersburg, MD: National Institute of Standards and Technology, February 26, 2024. https://doi.org/10.6028/NIST.CSWP.29.

References

Bhargava, Isha. 2023. “Trans Twitch Star Files Human Rights Complaint Against London, Ont., Police After Swatting Arrest.” CBC News, April 24, 2023. https://www.cbc.ca/news/canada/london/trans-twitch-star-files-human-rights-complaint-against-london-ont-police-after-swatting-arrest-1.6819941.

Communications Security Establishment Canada. “Best Practices for Passphrases and Passwords (ITSAP.30.032).” Canadian Centre for Cyber Security, September 17, 2019. https://www.cyber.gc.ca/en/guidance/best-practices-passphrases-and-passwords-itsap30032.

Cervini, Eric. Spying Before Stonewall: How the FBI Secretly Tracked Gay Activists in the 60s. June 8, 2020. https://www.vice.com/en/article/the-fbi-secretly-tracked-gay-activists-in-the-60s/.

Cineas, Fabiola. 2023. “Ron Desantis’s War on ‘Woke’ in Florida Schools, Explained.” Vox, February 15, 2023. https://www.vox.com/policy-and-politics/23593369/ron-desantis-florida-schools-higher-education-woke.

“Ghetto Informant Program,” Wikipedia, July 5, 2025, https://en.wikipedia.org/w/index.php?title=Ghetto_Informant_Program&oldid=1298852561.

Jankowicz, Nina. 2022. How to Be a Woman Online. New York: Bloomsbury Academic.

JusticeTrans. 2024. “Understanding & Fighting Back against the Anti-Trans Movement in ‘Canada.’” Toronto, ON: JusticeTrans and Women and Gender Equality Canada. https://justicetrans.org/wp-content/uploads/JT-REPORT-2024-FINAL-ENG.pdf.

Lang, Nolan. 2024. “Saskatchewan’s Pronoun Law and Canadian Anti-Trans Sentiment - Spring.” Spring: A Magazine of Socialist Ideas in Action, February 7, 2024. https://springmag.ca/saskatchewans-pronoun-law-and-canadian-anti-trans-sentiment.

Luneau, Delphine. 2022. “ICYMI: Leading Medical Organizations Call for Action to Counter Threats, Abusive Behavior Targeting Health Care Facilities, Workers and Families.” Human Rights Campaign. October 3, 2022. https://www.hrc.org/press-releases/icymi-leading-medical-organizations-call-for-action-to-counter-threats-abusive-behavior-targeting-health-care-facilities-workers-and-families.

Massanari, Adrienne. 2017. “#Gamergate and the Fappening: How Reddit’s Algorithm, Governance, and Culture Support Toxic Technocultures.” New Media & Society 19 (3): 329–46. https://doi.org/10.1177/1461444815608807.

Mortensen, Torill Elvira. 2018. “Anger, Fear, and Games: The Long Event of #GamerGate.” Games and Culture 13 (8): 787–806. https://doi.org/10.1177/1555412016640408.

Rothchild, Alice. 2020. “Cyber Bullies at Canary Mission Muzzle Free Speech.” Washington Report on Middle East Affairs, January/February, 12–13.

https://www.wrmea.org/2020-january-february/cyber-bullies-at-canary-mission-muzzle-free-speech.html.

Ruf, Cory. 2024. “Amnesty International Canada Condemns ‘Appalling’ Anti-Trans Policy Changes in Alberta.” Amnesty International Canada. February 2, 2024. https://amnesty.ca/human-rights-news/appalling-anti-trans-policy-changes-in-alberta/.

Shrier, Abigail. 2020. *Irreversible Damage: The Transgender Craze Seducing Our Daughters.* Washington, DC: Regnery Publishing.

Appendices

Appendix A. Incident Log Template

Column titles:

- # (ID number)
- TLP (Traffic Light Protocol): clear, green, yellow, or red
- Has Report: yes, no
- Date
- Status: new, open, closed
- Task # (NA, Planio #, GitHub #)
- Type: email, Bluesky, Facebook, Instagram, other online platform, physical, verbal, threats, theft, vandalism, medical, fire, hazard, other
- Reported By (reporter name)
- Username (of threat actor)
- Short Description
- Response
- Notes
- Screenshot File Name
- Link (to webpage with suspicious activity)

Appendix B. Incident Report Template (IRT)

Date and Time
Date of Incident:
Time and Duration of Incident:

Location
Venue Name and Address:
Specific Area of Incident:

Date and Time
People involved:
Contact info:

Description of Incident
Brief Summary:

Detailed Description of Incident and Actions Taken (Immediate response, Emergency services contacted, How was the incident resolved):

Description of Equipment, Property, Damage or Loss Incurred and Estimated Value:

Additional Info, Supporting Documentation:

Incident Type

- ☐ Physical
- ☐ Verbal
- ☐ Property Theft or Vandalism
- ☐ Medical Emergency
- ☐ Fire or Hazard
- ☐ Other:

Incident Severity

- ☐ Low
- ☐ Moderate
- ☐ High
- ☐ Critical

Involved Parties
Names and Roles of Individuals Involved:

Contact Info (optional based on safety and privacy concerns, useful for recordkeeping):

Witness Information
Name of Witness:
Contact Information:
Statement/Testimony:

Reflection and Follow-Up
Lessons Learned:

Preventive Measures Implemented:

Follow-up Tasks:

Reporter Information
Name:
Date:

Appendix C. Care Plan: A Victim-Centered and Trauma-Informed Guide to Evaluating Options in Times of Crisis

Immediate Actions

If you feel physically unsafe, remove yourself from the environment and contact emergency services or a trusted ally. Ensure you have access to basic necessities like water, food, and a safe space during the crisis. If you are concerned about being followed, watched, or stalked when removing yourself (e.g. someone is waiting outside), you might call a campus or community walk-and-talk service, contact a trusted ally, call a taxi, or have someone in the area escort you out. For immediate anxiety, grounding techniques, like deep breathing exercises, can help.

Introduction

It can be incredibly overwhelming and stressful to take action in a time of crisis. While it is important to centre the targets and/or victims of an incident, it can be painful and upsetting to be centred and to have to make big decisions in times of crisis. To even see yourself as the victim of a targeted attack can take a long and challenging process of reframing – for some, this just isn't a useful position.

In writing this policy, we want to recognize that the systems that exist to respond to these threats, attacks, and incidents are often not designed with the wellbeing of people targeted in mind. Often, when faced with potentially upsetting, stressful, and even traumatic incidents, we are left with what feels like no good options. This very real experience can be isolating and alienating. We hope that this plan will be one step toward a victim-centric safety planning process that does not rely on structures of securitization to make support and community accessible. We write this plan with an understanding that incidents are not always reported due to the same challenges that can also block access to community, support, and care.

This plan is written with two perspectives in mind: providing a basis and structure for community-based care and providing resources directly to victims of different types of attacks. A central point of focus is the options you have when dealing with an attack or crisis. We are often pressured to take immediate action and this plan aims to instead provide an overview of what each option provides and might look like.

Dealing with Shame and Blame

Above all else, we want to stress that a personal or cybersecurity incident is not your fault. As many steps as we take to protect ourselves, we can still become victimized or harmed by an incident out of our control. Sometimes this is a result of a direct, targeted attack and other times you may be collateral damage. Challenges faced by victims of a personal or cybersecurity incident include emotional stresses such as guilt, shame, embarrassment, or fear. Compromising a shared computer system can result in guilt and shame that will silence timely reporting. Professional embarrassment or fear of career consequences may hinder the project

safety. Personal, often physical, challenges associated with public scholarship and activism may require rapid responses such as calling the police or security, which may also be a source of risk and further stress.

Challenging Decisions
As we are faced with challenging decisions to protect ourselves and others, we do not become responsible for the harm that is done to us. The challenges associated with the experience do not become less real as a result of our planning processes. Planning does not make us responsible for the everyday violences and sources of harm that come out of repressive political-economic structures, nor the actions of individuals who want to cause us harm. Whether you have a minimal online presence or a large public following, you are not to blame for the harm that is directed at you. The standard, and often systemic, response to these kinds of incidents often falls back on victim blaming: you were “too loud,” “too public,” “too private,” and even “too trans” to be protected. Regardless of your actions, you can be the target of cyber- and personal security threats and we are here to support you through it.

While disclosing that you have been targeted can help us to support you through an incident, it can also present additional threats to personal and social safety, especially when an incident involves the weaponization of personal information and/or false accusations. We want to have open conversations about what disclosure means to you, what kind of and how much information is shared, and how documentation is stored. We must be ready to identify an incident and determine our safety both in person and online. We view this process as complex, imperfect, and nonlinear and are ready to support your process of responding to and recovering from an incident.

Finding support and self care during distressing times

Fear, anxiety, and depressive symptoms are common responses to cyberstalking and online attacks (Worsley et al. 2017). Victims report feeling helpless and feeling that the support available to them, particularly from police, is inadequate (Worsley et al. 2017). Being stalked, attacked, and/or threatened can feel embarrassing and isolating – often by design. Whether personalized or politicized, shame is a key part of violence.

It is important that you access networks of support to whatever extent you are comfortable. Share your experiences with friends, colleagues, family, join online or in person support groups, reach out to professionals and survivors. Share as little or as much as you are ready to. Take your time to layer coping strategies and responses that feel right for you and your situation whilst prioritizing your safety.

We want to ensure that you have options in this process of personal safety planning and, above all, that you are not dealing with it alone. If it is overwhelming to document an incident, make space for yourself to feel that and find support around it. The following strategies can provide support during difficult times:

Practice Self-Compassion: Remind yourself that being targeted is not your fault, and you are not alone in this experience.

Acknowledge Your Feelings: It's normal to feel anger, fear, or helplessness. Allow yourself to process the impact of the crisis and your emotions without judgement.

Lean on Trusted People: Reach out to friends, family, or colleagues who can offer emotional and practical support.

Focus on What You Can Control: Prioritize actions that help you feel safer, such as enhancing digital security or temporarily stepping away from online platforms.

Delegate tasks: Ask trusted allies to help with monitoring online activity, reporting abuse, or managing your social media accounts.

Professional Help: Consider consulting a therapist, counselor, or support group experienced in handling harassment-related stress.

Advocate for Yourself: Clearly express what type of support or assistance you need from your network. Block or mute harassers and adjust privacy settings to protect yourself.

Engage in Calming Activities: Practice mindfulness, breathing exercises, or activities that help you ground in the present moment.

Stick to a Routine: Re-establishing daily habits can create a sense of stability and normalcy.

Digital Detox: Limit screen time and social media exposure to avoid retraumatization from online interactions.

Stay Connected and Combat Isolation: Reach out to others, even if it's just to vent how you're feeling. Staying connected can reduce overwhelming feelings and loneliness.

We also recommend this advice from psychologist Lisa Feldman Barrett (*How Emotions Are Made: The Secret Life of the Brain*) on dealing with online harassment and distressing times.

Evaluating Options: Reporting & Documenting an Incident

Document the Incident:
Alongside the direct experience of the incident and decision-making, the process of capturing, documenting, and storing information about an incident can bring on complex and potentially mixed emotions. In some cases, it can be easy, cathartic, and relieving to document an incident. In other cases, it can be upsetting, triggering, and overwhelming to do so. It is normal to move through these emotions whilst processing the incident. Neither response speaks to the nature or the severity of the incident nor to you as a person.

Documenting an incident is often associated with potentially exposing or arresting its persecutor. Sometimes this will be and immediately feel like the best option. Sometimes you might feel

confused or unsure. Sometimes you will be completely opposed to this approach. For this reason, it can help to focus on this particular task at a speed and at times that make sense for you. You do not have to make a police report, go to security with, publicize, or even review this documentation. However, it is often useful to ensure that you have it prepared so you can put it away and revisit when you have a better sense of what your next steps might be. It can take some of the pressure off of a decision when its immediacy is stripped away.

Types of Evidence:
Document evidence such as screenshots, emails, or messages to use if you decide to report the harassment. Keep a record of the incident in a place where it is secure but out of sight in everyday life. Store screenshots out of your main camera roll on your cell phone and in a private, password protected Drive or Locker. The idea is to have these files safe, secure, and available to you when you might need them, without turning them into a trigger or a disruption. If documenting feels overwhelming, ask a trusted friend or ally to assist.

Reporting the Incident:
See the Contact Info section for who to contact to first report an incident. For more information about reporting, see the relevant section, either Personal Safety, Cybersecurity, or Event Safety.

If you immediately know that you need support or need help finding support, you can bring this up while reporting. If you do not immediately know, that is perfectly normal and okay. The door to support will not close. You can let us know when reporting if you need someone to check in with you regularly, how, when and how long you might need this.

If you decide to report a potentially compromised phone to police, it is likely that they will take your phone for a period of time to scan or evaluate its contents. For example, they can retrieve messages, locate spyware or stalkerware, and gather other kinds of evidence against your attacker. While this may preserve evidence, giving your phone to police can be uncomfortable and even risky. If this is a concern, you may be able to get help from your local victim service program or from a free legal clinic. If you need help finding these services, reach out to a contact on the safety team or trusted friend.

Resources and tools

For Carleton Students

Health and Counselling Services

https://wellness.carleton.ca/health/

Equity and Inclusive Communities

https://carleton.ca/equity/

For all Lab Employees

Employee & Family Assistance Program: Carleton's Employee & Family Assistance Program (EFAP) is a free comprehensive program that is available to support faculty, staff and their families.

https://carleton.ca/healthy-workplace/employee-family-assistance-program/

Ottawa and Canada-based Resources and Tools

Ottawa Victim Services (OVS) is a not-for-profit organization based in Ottawa, ON, Canada. Since 1998, OVS hasbeen providing emotional and practical support to people in our community who've been affected by crime or tragedy Ottawa Victim Services

The Crisis Line's professionally trained volunteer crisis line specialists are there to answer your call 24 hours a day, seven days a week. They will provide you support in a crisis and can transfer your call to the Local Crisis Team if needed. Crisis Line

Good2Talk is a free, confidential and anonymous helpline providing professional counselling and information and referrals for mental health, addictions and well-being to post-secondary students (18-30) in Ontario, 24/7/365. Good2Talk

Free walk-in counselling: no referral is required for the Walk-In Counselling Clinic. You will be assisted, with no appointment, on a first-come, first-serve basis during our Walk-In Counselling Clinic hours. The Walk-In Counselling Clinic is open to Ontario residents within the greater Champlain region. The Walk-in Counselling Clinic offers counselling services in English, French, Arabic, Somali, Spanish, Cantonese and Mandarin at a variety of different locations. Walk-In Counselling Clinic

VictimLink BC (1-800-563-0808) is a 24-hour, B.C. toll-free information, support and referral service for victims. You will find a safe and confidential service where you can discuss your experience and decide what you want to do. They will not discuss your situation with anyone else without your knowledge and permission, except as required by law (such as in cases of child abuse or neglect or a crime that is about to be committed).

Free Legal Clinics of Ottawa, with three locations across the city, can give you legal advice, help you fill out forms related to your case, represent you at some tribunals and courts, refer you to other agencies when they can't help

Canada-Wide Resources and Tools

Canadian Centre for Occupational Health and Safety offers a guide for dealing with internet harassment in the workplace.

eMentalHealth.ca: a community navigation tool concentrated on resources in Eastern Ontario, organized according to catchment area and type of service. This searchable online tool makes community resources and referral information accessible.

NeedHelpNow.ca offers support to minors affected by online sextortion and online sexual violence.

Techsafety.ca compiles a list of Canada-wide and provincially-specific resources for victims of online harassment, abuse, and stalking.

Victim Services Directory can be used to locate and connect to local victim service providers.

International Resources and Tools

Coalition Against Stalkerware – resources and tools for detecting and removing spyware.

Access Now: if you're an activist, a journalist, a human rights defender, or a member of a civil society group currently experiencing an urgent digital security incident, you can contact Access Now, a nonprofit organization that can provide emergency assistance, recommendations and referrals, technical support, and educational resources through its Digital Security Helpline.

Crash Override Network operates a crisis phone line and online resources for people who are experiencing online abuse.

Dangerous Speech Project's guide on counterspeech.

CCRI Crisis Helpline: if you are a victim of nonconsensual pornography, defined as the distribution of sexually graphic images without your consent, and you are living in the U.S., contact the Cyber Civil Rights Initiative, a nonprofit organization combating online abuse. It offers resources, legal referrals, and a 24/7 Crisis Helpline.

Vita Activa: If you are a Spanish speaker, Vita Activa has a helpline providing online support for women, LGBTIQ+ people, journalists and activists experiencing stress, trauma, gender violence or other crises.

Coalition Against Stalkerware can help you find support through a resource list it maintains if you are concerned about potential spying, monitoring, or stalking.

Online Harassment Field Manual, by the nonprofit organization PEN America, offers strategies and resources for those facing online abuse.

Tall Poppy helps organizations protect their employees against online harassment and abuse. They offer an online digital safety management platform which helps people lock down their accounts and protect their privacy. Should an employee come under attack, their expert incident response team provides compassionate support to reduce the harm of harassment.

Emotionally Demanding Research Network Scotland is a group of researchers (including students, research support staff, and practitioners involved in research) with experience of conducting emotionally demanding/challenging research. Our aim is to connect people involved in this kind of work in order to better support each other in doing this research.

Right To Be provides resources for self-care for victims of cyber harassment. Their guide is available in English, French, Arabic, Burmese, Indonesian, and Spanish.

References

Barrett, Lisa Feldman. “Advice from a Psychologist.” Online Harassment Field Manual, PEN America, April 9, 2018. https://onlineharassmentfieldmanual.pen.org/advice-from-a-psychologist/.

Cofense. n.d. “Sextortion | Is Your Business Exposed? Find Out Here.” Cofense. Accessed January 31, 2025. https://cofense.com/sextortion/.

Pearce, R. (2020) A methodology for the marginalised: Surviving oppression and traumatic fieldwork in the neoliberal academy. Sociology, 54(4), 806-824.

“Technology Safety Quick Tips – BC Society of Transition Houses.” n.d. BC Society of Transition Houses (blog). Accessed January 31, 2025. https://bcsth.ca/techsafetytoolkit/technology-safety-quick-tips/.

Worsley, Joanne D., Jacqueline M. Wheatcroft, Emma Short, and Rhiannon Corcoran. 2017. “Victims’ Voices: Understanding the Emotional Impact of Cyberstalking and Individuals’ Coping Responses.” Sage Open 7 (2): 2158244017710292. https://doi.org/10.1177/2158244017710292.

Appendix D. Event Planning Checklist

In Advance of Event:

What is the level or perceived risk and concern, and how can you increase safety accordingly?

- ☐ Content: Are the guests or topic considered ‘controversial’?
- ☐ Location: Are there anti- rallies happening in the locale?
- ☐ Environment: Have there been incidents at other similar events locally or currently? What safety lessons can we implement from them?
- ☐ Have explicit discussions prior to an event on the role and need for law enforcement services: understand what actions various law enforcement services are authorized to take that the event organizers would be unable to act on their own (e.g. escorting people out of the venue)
    - ☐ If you decide that security/police have a role, have a clear plan to keep people who are typically targeted by security/police feeling safe and comfortable.
    - ☐ Familiarize yourself with your rights as well as the rights and limits of law enforcement services chosen (Campus Security, Police/911, venue security, trained personnel).
- ☐ If the event is expected to garner publicity for the project, brief the chair, dean, Coms, and the office of risk management to explain why we are at risk and to prepare them for any complaints.
    - ☐ Work with University Communications to prepare press statements designed to counter disinformation. Create a simple key message, written for those who care about the topic and are interested.

Venue, Date and Time Selection:

- ☐ Choose venues with multiple exit routes and accessible exit plans and safety plans.
- ☐ Confirm if you have the right to ask people to leave. Can anyone come in? Is there open access to the building or room?
- ☐ Is there service or wifi? How will the event organizers communicate on the day of?
- ☐ Consider the safety of people arriving and leaving the event, whether it is an evening or day and how far is parking/public transportation.

Planning with Guest Speakers and Co-Organizers:

- ☐ Ask guests about their security and safety concerns, needs, past experiences, and what we can generally do to make them feel safe.
- ☐ What are the guests’ comfort levels in Q&A panels? Are there questions they will not respond to? Do they want a facilitator to respond to those questions and to disruptors?
- ☐ Have your questions, speeches, or facilitation notes peer-reviewed.

Leading Up to Event:

- ☐ Create registration for the event.

- ☐ Limit disclosure of the time and location of the event (registrants only, days before event, etc)
- ☐ For online events: Create a passcode, waiting room, or other form of authorization to control event access

Day of Event:

- ☐ Identify security options and introduce yourselves to on-site security.
- ☐ Go over your Emergency Contact procedure, assign and review roles:
    - ☐ Know what authorities or support will be called and when, by whom, and in what order, to avoid multiple calls or confusion.
    - ☐ Identify people with de-escalation training, First Aid, knowledge of local mental health resources.
    - ☐ Roles: Facilitator/Host, Co-Host, Guest Liaison, Security Monitor, Medic, Peer support
- ☐ Inform co-presenters and guests of safety plans, exit routes and points of contact so they are not panicked or lost if an incident occurs.
- ☐ Take a headcount at the beginning and occasionally to be aware of changes. If there is a registration list, confirm with the number registered.
- ☐ Screen audience questions and participation through mediation, submitted written questions/Slido/QR code/etc.
- ☐ Maintain communications in a group chat so that the team is all aware of potential threats or actions taken and so that you have documentation.

For Online Events:

- ☐ Limit video and audio controls for participants when appropriate.
- ☐ Turn off general chat.
- ☐ Assign trusted co-hosts.

Appendix E. Carleton's Social Media Privacy and Security Guidelines

The Transgender Media Lab's Social Media Policy is available on our public website. This policy helps ensure our social media content reflects our lab's values. This policy also describes the actions we will take to ensure that people commenting on our social media posts are not causing harm to BIPOC and disabled trans people.

Below are the guidelines that Carleton University Communications has shared with us:

Basic Security

- Consider having a professional and personal profile. Your personal profile should be used for close friends and family, while you share your professional profile on your website, employment bio, etc. This allows you to continue using social media on your personal account without having to interact with distractions or harassment that may come to your professional account. Personal accounts have limited connections (only people you know), are listed as private, and do not have identifiers to your real name or profession. This allows you to have a safe space to interact with friends on social, should your professional account come under any issues.

- Link a private phone number and email address to your accounts, separate from your normal or everyday email account. You may consider using an email address created specifically for social media management. If your account is accessed or your email is viewable from the social profile, you can ensure that your normal private email is not visible to the public.

- Regularly check the security settings on your profiles (ex. quarterly). Platforms often change features and settings, and you may have your settings overridden or new settings enabled as default.
- Narrow your connections on your personal profiles. Be wary of the types of entities and individuals who you connect with and do not know on a personal level.

Usernames, Biographies, Profile Pictures

- It is strongly recommended that you avoid using a profile or username which indicates or relates to your real name.
- Avoid profile pictures which can indicate your location (street signs, home number, license plates, etc). When possible, choose photos with a neutral background and show limited objects.
- Keep personal information off the platform. Birthdates, addresses, additional modes of contact, these are items that do not need to be shared on social media.

Passwords and Logins

- When possible, you should always use multi-factor-authentication (MFA).
- Do not reuse passwords between sites.
- Do not use departmental or shared mailbox accounts, only use work emails to manage CU owned accounts (exampledepartment@carleton.ca vs janesmith@carleton.ca)

Managing X (Twitter)

Restricting Commentary

- Click on your post
- Click "..." in the upper right of the post
- Click "Change who can reply"
- Click "Only accounts you mention"

Privacy Settings

- To find your privacy settings click the "..." icon; sometimes labelled as "More".
    - Click "Privacy and Safety".
    - From this area you can determine the information you share, who can see what you share, along with what you can see.
- To prevent others from accessing your Tweets, click "Audience and tagging".
    - Click "Protect your Posts". This makes it so individuals who follow you are the only ones who can see your posts.
    - Change 'Photo tagging' from "anyone can tag you" to "only people you follow can tag you".
- Turn off your location by Clicking "Your posts".
    - Click "add location information to your posts".
    - Deselect "Add location information to your posts".
- To mute or block individuals click on "Mute and Block"
    - You can mute notifications from people you don't follow or don't follow you, as well as new accounts/accounts with default profile pictures/accounts with unverified emails and phones numbers – this is recommended as these accounts are most likely to be troll accounts.
    - o mute or block individuals you must do so from one of their posts or profile pages. Navigate to a post or profile page and click "...". From that menu select mute or block.
- To control direct messages, return to "Privacy and safety," click "Direct Messages"
    - Click "Allow messages only from people you follow". This will prevent strangers from DMing you.
    - Disable read receipts.
- Turn off "Spaces" listening activity under the Spaces section.

- Discoverability, consider disabling letting people find you with your email or phone number, especially if your account is created with a publicly available email or phone number (e.g. your Carleton University account).

Managing Instagram

Restricting Commentary

- Click “More” or the icon.
- Click “Settings”.
- Scroll to “How others can interact with you”
- Click “Hidden Words”
    - Click “Manage custom words and phrases”
    - Enter the words that are causing issues. All words entered will automatically trigger comments to be hidden should they contain them. (ex: murder, terrorism, etc.)
- To restrict users, and automatically hide all their previous commentary on your account and posts:
    - Click the username on the comment o Click the ‘...’ on the user profile
    - Click ‘restrict’
- On an individual post:
    - Click on your post
    - Click “...” in the upper right of the post o Click “Turn off commenting”

Privacy Settings

- Click “More” or the icon.
- Click “Settings”.
- You will be taken to the embedded Meta Accounts Center. You can choose to edit your information in the Instagram version or go directly to the Meta Account Center. Both options have similar tools sets, but the Meta Accounts Center will allow you to view all your Meta profiles at the same time.
- Click “Who can see your content”
    - Click “Private Account”. Now people need to request access to see your content.
- • Click “How others can interact with you”
    - Disable “Show Activity Status”
    - Change “Allow @mentions from” from ‘everyone’ to ‘people you follow’ o Disable “Allow others to use your posts”
    - Change “who can tag you” from ‘everyone’ to ‘people you follow’
    - Consider the “Hidden Words” section of the settings.
- You may choose to add advanced filtering to hide comments with key words you find offensive or triggering
- Enable “hide message requests” which will take the keyword filter and apply it to DM’s.
    - Click “Comments”
- Change “allow comments from” ‘everyone’ to ‘people you follow and your followers’

- Consider adding keyword filters which will automatically hide any comments you don't appreciate.

Managing Facebook

Restricting Commentary

- Click Settings
- Click "Followers and public content"
- Click 'Hide posts with profanity'
- Click 'Hide Comments containing certain words'
    - Enter the words, separated by commas, that you wish to be comments and posts to have to be automatically hidden.

Managing LinkedIn

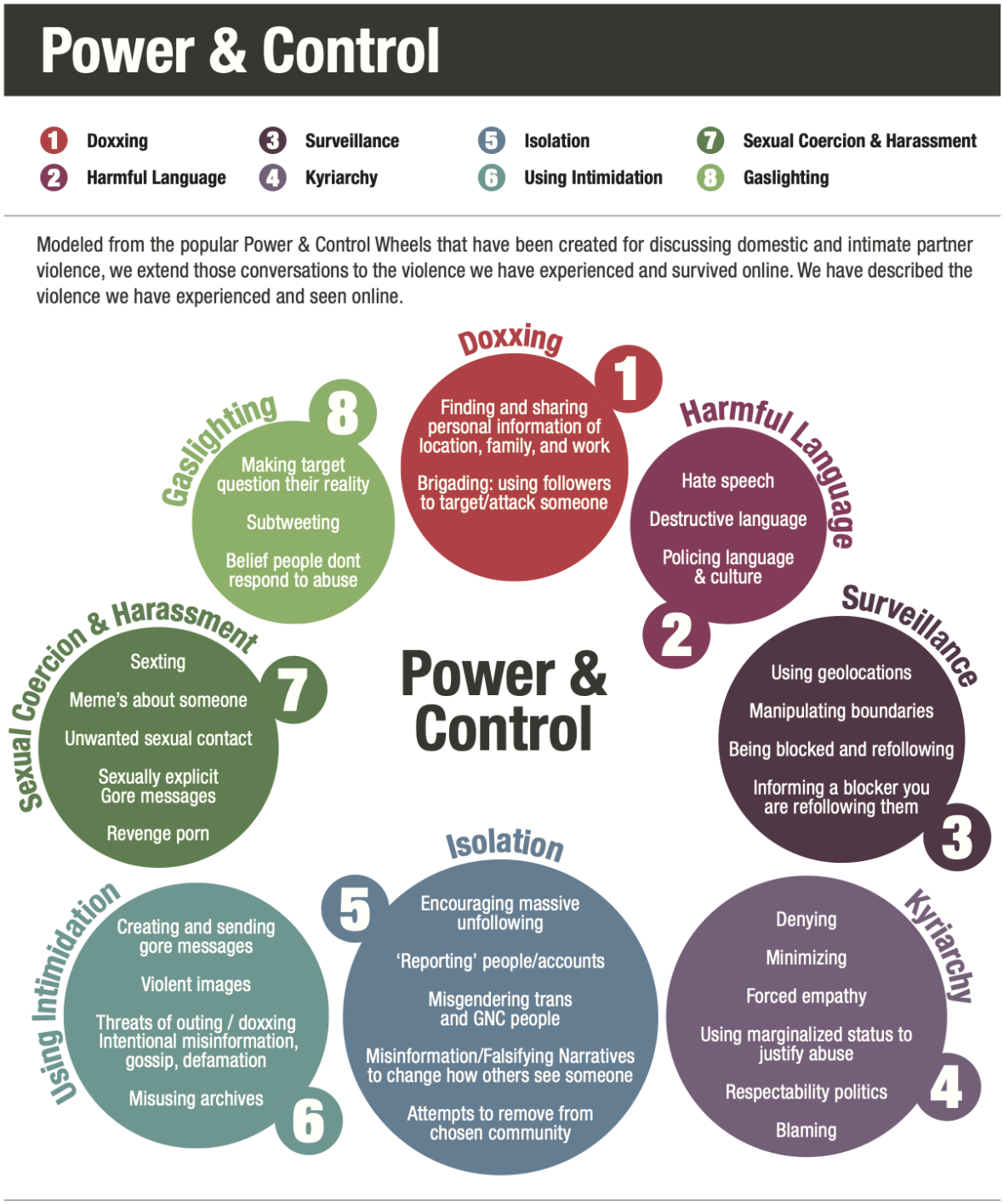
Restricting Commentary

- Click on your post
- Click "..." in the upper right of the post
- Click "who can comment on this post"
- Click "no one"

Privacy Settings

- Click "Me" on the top right of the LinkedIn menu
- Click "Setting & Privacy" Under "Account"
- On the next page, the right-hand menu will have a tab "Visibility".
- Click the "Visibility" tab
    - Under 'profile discoverability using email', change from anyone to connections
    - Under 'profile discoverability using phone number', change from anyone to connections
    - Click "Who can see your last name", change to connections
    - Click "Notify connections when you are in the news" – turn to off.

Appendix F. Power & Control Online



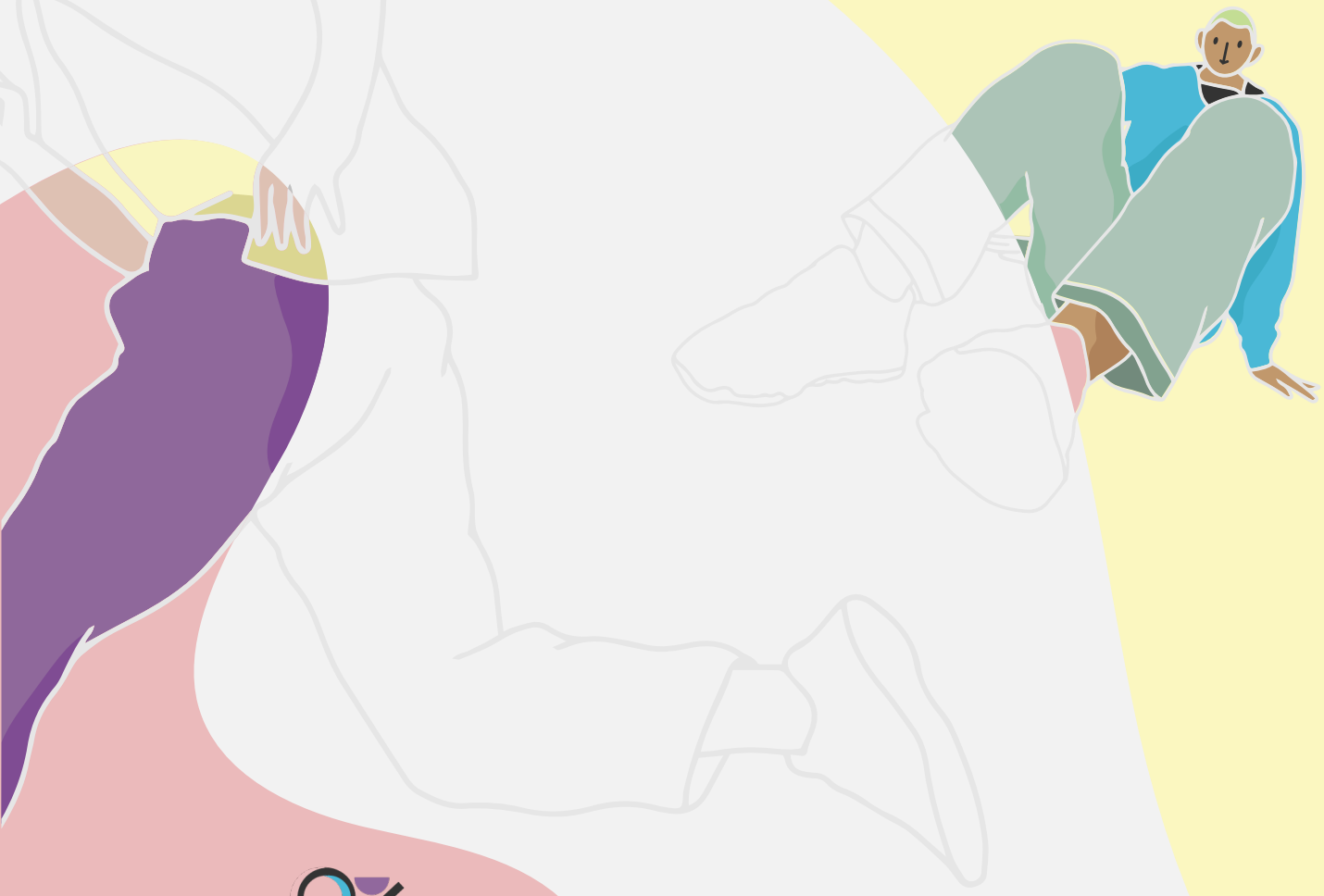
Appendix G. Understanding & Fighting Back against the Anti-Trans Movement in ‘Canada.’

PDF available here:
https://justicetrans.org/wp-content/uploads/JT-REPORT-2024-FINAL-ENG.pdf

JusticeTrans, 2024

Understanding & Fighting Back against the Anti-Trans Movement in “Canada”

A Guide for Trans Communities & our Allies



JUSTICE TRANS

Women and Gender Equality Canada

Femmes et Égalité des genres Canada

Acknowledgements & accountability

JusticeTrans was founded in Tkaronto, now known as Toronto, on Treaty 13 and Williams Treaty territory. Tkaronto means "where there are trees standing in the water" in Kanien'Kéha. This is the traditional territory of many nations, including the Mississaugas of the Credit, the Anishnaabeg, the Chippewa, the Haudenosaunee, and the Wendat peoples. We acknowledge these nations as the stewards of these lands and waters and thank them for their care. As a national organization, our staff and board lives, works, and plays across Turtle Island in what is colonially known as Canada. We recognize that over 600 Indigenous nations have tended to these lands and waters as their home fires and their traditional territories. These nations have made it possible for us to do our work, and they deserve our respect. At JusticeTrans, we are committed to having a collaborative and empowering relationship with the 2Spirit and Indigenous trans, non-binary and gender diverse communities we serve. We also commit to dismantling the forms that settler colonialism inherently takes in our work.

We stand in solidarity with Indigenous nations across Turtle Island, and we bear witness and hold ourselves and others accountable to the atrocities of the past and the ongoing violence and oppression that are inherent to settler colonial systems, socialization, and practices.

For more interactive maps of Indigenous territories and data visit:

native-land.ca
The Map Room
The Geo Viewer
Residential Schools

Acknowledgements & accountability

This research would not have been possible without the participants who trusted us with their experiences and stories. Thank you!

The research team was comprised of six trans, non-binary, and gender diverse people. Due to safety concerns in the current context, we have chosen to remain anonymous. All of us are queer and university-educated, most are disabled and four are racialized. These intersections affect the ways we experience the world and how we did this work. Additionally, the project was developed and led by white settlers.

The project also operated within two frameworks that are rooted in white supremacy and colonialism: research and the non-profit sector. Although this team did radical work in many respects, we could have gone further to subvert oppressive systems. We have learned from this and intend to adapt future projects!

This work was possible thanks to the support of JusticeTrans staff, and our advisory committee, which comprised seven 2Spirit, trans, non-binary, and gender diverse individuals from coast to coast. We would like to acknowledge our community partners on this project:

- Hamilton Trans Health Coalition
- Community-Based Research Centre
- Egale Canada
- Community members with experience as practitioners, researchers, and activists involved in Indigenous, anti-racist, disabled, youth-led, and feminist movements

JusticeTrans would also like to acknowledge the support of Women and Gender Equality Canada, whose generous funding has made this project possible.

Ethics clearance ID:
Carleton University Research Ethics Board-A, Project # 119828

How to cite:
JusticeTrans. (2024). Understanding & Fighting Back Against the Anti-Trans Movement in "Canada": A Guide for Trans Communities and our Allies. "Canada".

Table of Contents

Introduction

In recent years, there has been a noticeable increase in anti-trans organizing worldwide and in the country colonially known as Canada. This has especially been the case since 2023. Egale Canada identified "nearly 6,500 instances of online hate and protests against the 2S/LGBTQIA+ community in Canada within the first three months of 2023"[1]. The purpose of this project was to study this worrying trend so trans communities and our allies may better understand the anti-trans movement and fight back more effectively.

What do we mean by trans?

"Trans" is used here to include many distinct identities including 2Spirit as well as trans, non-binary, and gender diverse identities. This usage does not indicate that 2Spirit peoples are defined as part of the trans umbrella: these Indigenous identities are beyond the scope of non-Indigenous understandings of sexuality and gender. Nor does it aim to conflate these identities as one.

This guide uses the word "trans" throughout instead of 2S/TNBGD because that makes text more accessible, especially since this acronym is not well known. Please note we still think intentional language is important.

We also use trans instead of 2S/TNBGD because, unfortunately, the anti-trans movement is targeting anyone and anything it perceives as trans or trans-affirming.

Please be advised that the topic covered in this guide is violent and may be triggering. Many participants described their experiences as traumatic. Please prepare yourself mentally and think of self-care you can do while during and after you read.

Methodology: How we got to these results

Reading tip:
Explaining how we got results is part of good science. However, feel free to skip this section and go straight to results!

These results come from JusticeTrans' project, Tracking Transphobia: Identifying and Countering Anti-Trans Organizing in Canada. The project goals were to:

1. Define what the anti-trans movement is
2. Identify the rhetoric and tactics used by the anti-trans movement to attack trans activists and trans-affirming organizations
3. Identify the effects of anti-trans attacks on organizations and individuals and how they reacted and protected themselves
4. Develop a guide to help organizations and individuals respond to anti-trans attacks

To achieve these goals, we conducted a review of the literature, a media scan, and research interviews

Our approach to science

This project is firmly trans-for-trans (t4t). This means that, as an all-trans research team, supported by an all-trans staff and project committee, we tried to create a safer space for trans participants to "express the full complexities of their realities"[2]. A lot of care was put into helping interviewees feel as safe as possible.

We also took measures to create a safer space for the research team because doing this kind of research while also experiencing the same types of marginalization and violence is extremely emotionally demanding[3]. However, the project's time constraints made it impossible to spread out the work, which is essential when doing emotionally demanding research[3]. As a result, some team members are feeling the devastating impacts of vicarious trauma. This is the specific trauma that comes from long-term exposure to traumatic materials at work[3].

Research that is done by and for marginalized communities is often perceived as driven by a social justice agenda and as subjective instead of good, objective science[3]. We believe that leaning into our subjectivity as researchers, and into our participants' subjectivity, is a resource for objectivity because we are upfront about our biases.

Yes, this research is absolutely driven by a social justice agenda: fighting back against the anti-trans movement.

Literature review & media scan

The literature review and media scan used a bilingual search strategy with keywords for identity, actions, groups, and organizations. The literature review included academic databases and Google Scholar and had no time limit. We identified 32 relevant documents through this search and our networks. The media scan relied on the Eurêka.cc database, using the search strategy in Table 1.

Table 1.
Media scan search strategy

LEAD= ("anti-trans " | "anti trans " | "anti-transgender*" | "pronoun*" | "drag queen" | pronom*)& LEAD= (protest* | demonstration* | boycott* | manifestation* | lobby* | lobbies | policy | policies "gender critical" | TERF* | "trans-exclusionary radical feminis*" | "trans* exclusionary radical feminis*")

Filters: Canada (ENG + FR), January 1st 2023 – November 8th 2023

Results: 1134

PDFs we extracted: 926 pages (we tried not to extract duplicates, but the database made it difficult)

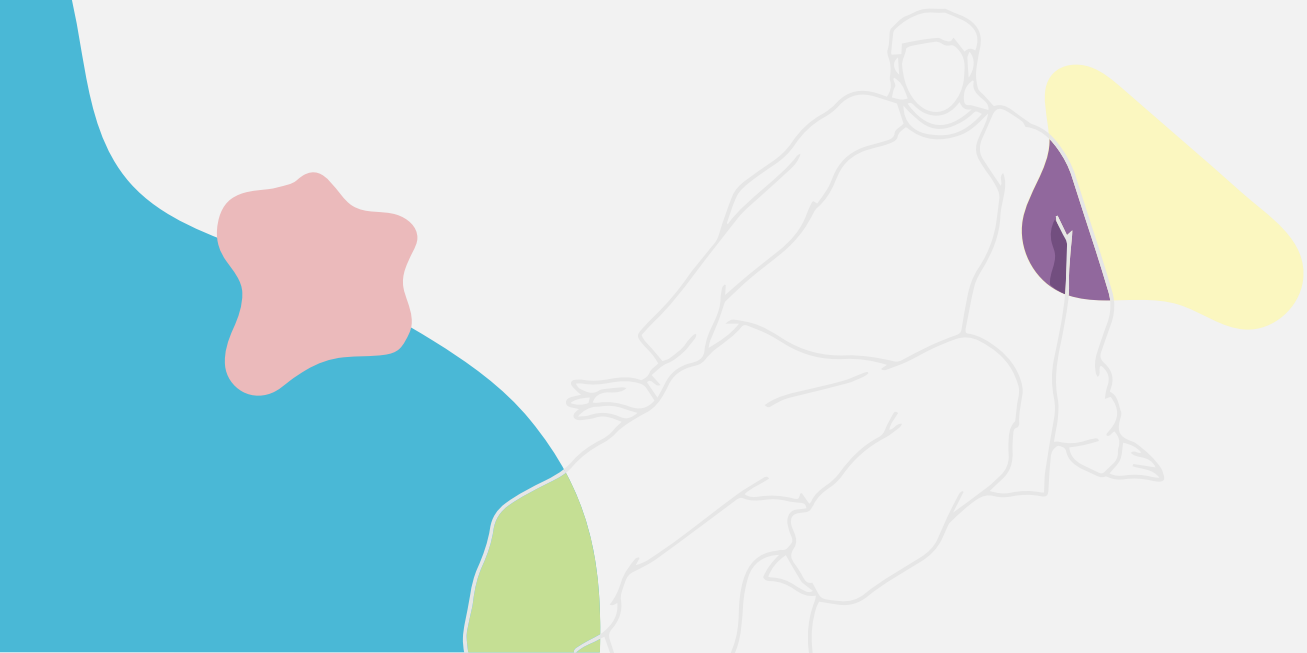
Research interviews

Participant recruitment began mid-November 2023. We were looking for two groups:

1. 2Spirit and trans, non-binary, gender diverse adults who were targeted by anti-trans attacks in so-called Canada

2. Adults who worked at women's organizations, queer organizations, schoolboards, or trans-affirming service providers that were targeted in so- called Canada.

We prioritized racialized applicants, people from the four organization types, and applicants outside of Ontario. We conducted one-on-one, semi-structured interviews with 22 people between November 2023 and February 2024. The research director conducted thematic analysis of the interview transcripts from January to February.



Results: our participants

Participant demographics are summarized in Table 2.

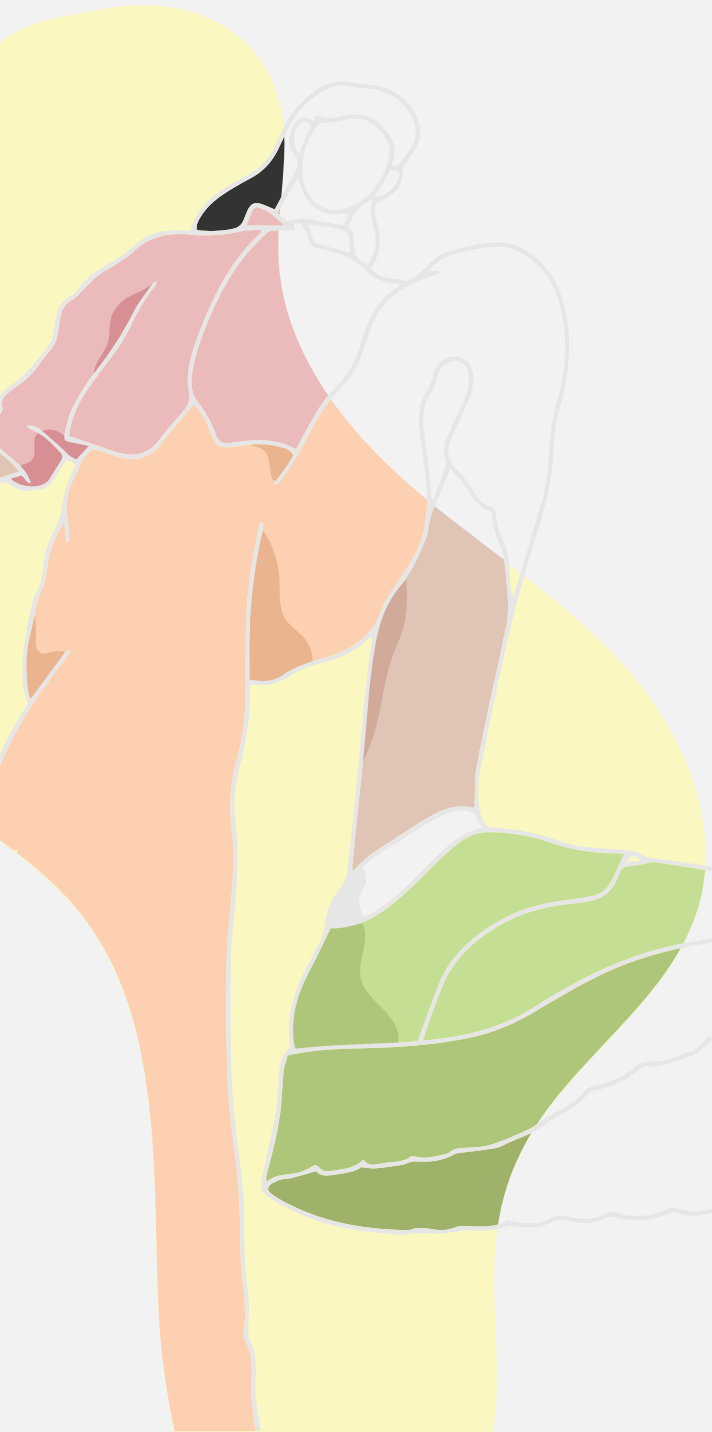


Table 2
Participant demographics (n=22)

Characteristic	Details	Number	%
Gender	Non-binary	6	27.3
	Trans woman or transfeminine	4	18.2
	Trans man or transmasculine	5	22.7
	Culturally specific identity	1	4.5
	Trans, unspecified	2	9.1
	Cis woman	4	18.2
Race	Racialized (details in text)	5	22.7
	White	17	77.3
Social Class	Working class	10	47.6
	Middle class	9	42.9
	Upper class	2	9.5
Education	High school	1	4.5
	College	3	13.6
	Undergraduate	5	22.7
	Graduate	13	59.1
Disabled		18	81.8
Queer		20	90.9
Parent		6	27.3
Affiliation	Activist	5	22.7
	Schoolboard	2	9.1
	Queer organization	8	36.4
	Service provider	5	22.7
	Women's organization	2	9.1
Location	Prairies	3	13.6
	Québec	1	4.5
	Territory	1	4.5
	British-Columbia	5	22.7
	Maritimes	2	9.1
	Ontario	10	45.5
Setting	Urban	14	63.6
	Suburban	4	18.2
	Rural	3	13.6
	Northern	1	4.5
Targeted as	Individual	5	22.7
	Organization	7	31.8
	Both	10	45.5

Most participants were disabled, queer, very educated, and white. Ontarians are also overrepresented in the sample. As in JusticeTrans' previous project[2], we struggled with recruiting and retaining participants from Québec (despite community ties within the team and bilingual recruitment efforts) and from Northern territories.

Participants were aged 22 to 51, with an average age of 32.7 years old. The standard deviation was 8.8, meaning most participants were aged 23.9 to 41.5. Almost half of participants had been targeted both as individuals and at their organization. Participants started experiencing anti-trans attacks between 2011 and 2023, and over 50% were first attacked in 2022 (median). We asked participants when anti-trans attacks ended for them. 81% of participants stopped being attacked in 2023 or were still experiencing attacks as of the interview.

Major limitation: racial diversity among participants

The majority (77%) of participants were white. Racialized participants disclosed they were: Chinese; Indian immigrant; South Asian and Southwest Asian North African mixed; mixed race Persian and white, second-generation immigrant; and a Person of Colour. None of the participants were Black nor Indigenous.

This is a major limitation of this project because as the following pages will show, racialized people get targeted differently by the anti-trans movement and have different safety concerns. Although racialized applicants to the project were prioritized, we struggled with retaining those who were eligible to participate. We suspect this may be due to:

- Very short timelines for this project, as there was no time to continue recruitment
- Exhaustion in populations that are under attack on multiple fronts
- Added safety concerns compared to white participants
- Fatigue among small, overly-researched populations[4]
- Distrust of JusticeTrans as a historically predominantly white organization
- Format of this research being rooted in white ways of doing things (ex. one-on-one interviews instead of community-driven focus groups)
- Hiring patterns in organizations in general, where racialized workers are often frontline or contractual workers rather than core staff
- Insufficient honorarium amount offered ($100) given the emotional labor involved

Understanding the anti-trans movement in Canada

What it is

The anti-trans movement relies on a set of diverse tactics that seek to restrict the rights of trans people, including those related to bodily autonomy and participation in public life[5]. This movement exists within a political and media culture that promotes transphobia, which may refer both to individual and systemic discrimination and oppression of trans people[6,7]. Rather than focusing on an anti-trans movement, existing research often focuses on anti-trans hate, a vague term which includes hate crimes. However, as this guide will show, the anti-trans movement is about much more than hate.

The anti-trans movement targets trans people and other people who transgress the gender binary, like drag artists[5]. The anti-trans movement does not include research on detransition[8].

Who is involved

This research revealed that people involved in the anti-trans movement have a broad range of affiliations and form an unstable coalition with important ideological divides[9-10-11]. Although their attackers' affiliations were not always obvious to interviewees, in other cases these were quite clear. Additionally, an unpublished report[10] identified 250 actors including individuals, organizations, and media sharing over 650 relationships. This guide identifies three main categories of anti-trans actors: trans-exclusionary radical feminists, religious groups, and right to far-right groups.

Trans-exclusionary radical feminists (TERFs), or gender-critical groups as they like to be named, are part of this movement under the pretense of protecting cis women and girls. Some examples include Vancouver Rape Relief and Pour les droits des femmes du Québec[6,12]. Eight interviewees identified TERFs as involved in what they experienced. Importantly, although feminism is often framed as a leftist movement, prior research identified a strong overlap between TERFs and right-wing media[10].

Religious public figures, people, and organizations were also identified as part of the anti-trans movement[10]. Some Christian nationalist and Muslim community members formed Hands Off Our Kids and instigated the 1 Million March 4 Children[11], while Christian groups like Save Canada and some chapters of the Salvation Army were also identified by interviewees.

The third category includes right-wing, far-right and alt-right activists, groups, and politicians, as discussed by half (11) of the interviewees and as shown in the media scan. The media scan showed that right-wing political parties in New-Brunswick, Saskatchewan, Alberta, Manitoba, Québec, and federally have latched onto the anti-trans movement. They do this to promote their platform and introduce anti-trans legislation and policy. These parties' electoral bases are also involved by voting to introduce anti-trans elements to their parties' platforms. American neoliberal and conservative groups also provide strategy, resources, and infrastructure to Canadian groups[10].

According to interviewees and prior research[10,13], far-right groups involved in anti-trans organizing include:

- Libertarians
- White supremacists
- Men's rights activists
- Conspiracy theorists such as QAnon followers, anti-mask and anti-vaxxers, sovereign citizens, and freedom convoy supporters.

Why this movement has risen

Factors explaining the anti-trans movement's rise include an international backlash against increased trans visibility and recognition[1]. Researchers[14] found that between 2011 and 2019, Canadian media coverage of trans youth has become "increasingly affirming of transgender identities, experiences, and needs". Additionally, over the past decade or so, more human rights and legal protections have been secured for trans Canadians. Unfortunately, increased trans visibility and recognition go hand in hand with increased violence towards the trans community[15]. As an example, the banning of trans conversion therapy could have redirected the anti-trans movement towards a backlash against schools[16].

The anti-trans backlash is part of a broader, international anti-gender conservative backlash which targets feminism, women's rights, and queer rights[17]. The anti-gender backlash emerged in Europe in the mid-2000s, only to expand to other parts of the world and to increasingly target trans rights in recent years[17].

What is a moral panic?:

A moral panic happens when a group of people gets identified as a threat to society. It comes from widespread and exaggerated fear.

A convergence of moral panics has also been observed since 2018 and has contributed to the anti-trans movement[13]. By analyzing 231 instances of hate mail they received, one researcher[13] identified three converging moral panics. These moral panics are the fear that transness is contagious; of pedophilia and child abuse; and of educators and other professionals who have access to children and youth. All three moral panics tap into anxieties around protecting children and youth.

The last factor potentially explaining the rising anti-trans movement is an emboldened right wing. This right wing has been emboldened by Donald Trump's election and has seeped beyond U.S. borders to target everything accused of being woke, from critical race theory to trans rights[1,9,10,13]. As Sarah notes, "I've been in this role for 10 years. This did not happen before the rise of the alt right machine."

What this movement is saying

Just as there are many types of people involved in the anti-trans movement, these people have many talking points (rhetoric) about trans people, about why they're involved in this movement, and to justify anti-trans tactics.

To some, trans folks are unnatural, less than human, deceptive, shameful, or mentally ill[13,18,19,20]. The biggest talking point, however, is the idea that trans people are dangerous sexual predators[5,12,13]. Transfeminine folks are discussed as if they were violent men who want to invade women's spaces and hurt cis women and girls. Similarly, trans folks and drag artists are presented as groomers or pedophiles who want to harm children.

Nearly half (10) of our interviewees spoke to this second theme, especially as they or their organization had been accused of grooming children. One states:

"It was just your typical kind of vitriol. Calling me a groomer and things like that." - Joe

This comment shows just how normal this accusation has become. A recent decision by the Ontario Superior Court of Justice even addressed the use of groomer as an anti-queer slur[21]. For Levi, this rhetoric is connected to a broader distrust of queer folks who were assigned male at birth. This shows that the moral panic which was directed towards gay men a few decades ago has been reimagined, with trans folks as the main villains[13].

A key justification used by the anti-trans movement is that they are simply protecting children and youth, which [13] interviewees brought up and which was shown to be quite influential in prior research[10]. According to three interviewees, the anti-trans movement claims to protect children from gender-affirming care. This care is presented as harmful as it would supposedly confuse kids and lead to permanent mutilation.

This movement claims to protect children from groomers and pedophiles, but also from indoctrination into "gender ideology", "radical leftism", and "wokeism" as we learned from the media scan. One third of interviewees (eight) discussed this concern over indoctrination. The anti-trans movement believes indoctrination happens through primary, secondary, and university curricula covering topics like gender identity and sexual education. It also believes trans-affirming professionals and organizations are trying to indoctrinate children and youth[10]. Indoctrination is connected to the broader claim of social contagion[10,13], or as Juno puts it "the idea that one transgender youth [...] is going to infect all these other children by their mere existence".

Due to these concerns, the anti-trans movement emphasizes parental rights to protect their children from sexualization, indoctrination, gender-affirming care, and social contagion. Parents claim to have a right to be informed by schools when children question their identity or use a new name or pronoun; they also want to have a say in what their kids are taught (media scan and five interviews). The underlying assumption is that children are their parents' property and have no rights of their own. Other legal rhetoric was also identified. The protection of religious freedoms to raise children as they see fit came up in the media scan. Cis women's right to not be victimized also came up.

Prior research[13] and five interviewees mentioned moral rhetoric such a being told they were going to hell. This comes from the idea that transness is sinful or wrong. This also came through in the media scan, in claims that society is experiencing a moral slippery slope and that drag story hours are destructive to children, families, and the nation as they normalize transness. These ideas come from social conservatism[22].

Lastly, two interviewees brought up economic rhetoric. Indeed, some people associated with the anti-trans movement ask how the "transgender agenda" is funded or claim public funds are misspent when Pride crosswalks are painted.

What this movement is doing

Across affiliations and rhetoric, the anti-trans movement relies on a diversity of tactics deployed on- and offline. As JoJo put it, "That's a lot of work. To Hate." A general tactic used by the anti-trans movement is to select and attack visible targets, which 16 interviewees spoke to. Visible targets include:

- visible individuals, to which transfeminine activists, racialized trans activists, and drag artists are especially vulnerable
- visible queer or trans-affirming organizations, especially in smaller towns
- visible locations, such as trans-affirming organizations' buildings and spaces with Pride-themed decorations;
- visible trans-affirming events.

Relatedly, invading safer spaces such as on- and offline events and attempting to cancel trans-affirming events came up as tactics in six interviews.

“A lot of it is less of actual logic and more of taking these [...] like spark words like these scary words that make people go like, ‘Oh. Oh no, they’re bad! I don’t need to know why they just said groomer, pedophile or whatever.’ And that’s bad. They’re keying in on the paying attention to those words that spark fear and anger.” -Levi

Nine interviewees also spoke to a tactic of stoking division by radicalizing the public, especially through fearmongering[5]. As one participant explains:

“There was again so many children [at the anti-trans protest] that were also verbalizing these things and that was, you know, I find that to be a little bit extra hard.” -Anric

Sarah was worried about how susceptible people were to this radicalization, especially in her small town. Especially concerning is the radicalization of children and youth by the anti-trans movement. Three interviewees had specifically been targeted by teenagers and young adults in offline settings.

These examples of radicalization fit within “culture warfare” [9].
Culture warfare includes:

- Polarization, which means groups are built up and pitted against other groups
- Framing issues in a moral way to then argue that one side is right and the other is wrong
- Using an us versus them mentality, where the other side is demonized
- Using emotionally charged symbols and issues to represent broader ideological conflicts.

Media & information

The anti-trans movement leverages media and communications in a variety of ways to wage cultural warfare[9]. The anti-trans movement uses social media to achieve its goals through coordinated and uncoordinated attacks[9]. The majority (19) of our interviewees reported on this, and we identified more cases in the media scan. Some specific tactics include:

- Maliciously reporting social media content (related or unrelated to trans issues) or attempting to get a trans-affirming social media account shut down
- Dogpiling, which means flooding social media with critical or hateful comments
- Doxing, which is exposing identifying information about an activist or trans affirming professional
- Malicious cross-posting, for example sharing trans-affirming TikTok videos to Twitter with the intention to engage in hate
- Bigger accounts riling up their social media followers
- Phishing, so attempting to deceive people and organizations into revealing sensitive information.

The anti-trans movement also uses traditional media, as reported by nine interviewees and prior research[9,10]. This includes articles, opinion pieces, and news broadcasts appearing in right-wing media spaces such as Rebel News, True North, and Fox News. However, this also includes pushing anti-trans rhetoric, misinformation, and disinformation in more mainstream media outlets, such as click-bait investigations into detransition or sensationalist op-eds about trans women incarcerated in women's prisons.

Misinformation: spreading wrong information

Disinformation: intentionally spreading wrong information

Ten interviewees discussed the spreading of misinformation and disinformation. Coordinated disinformation campaigns rely on algorithms to spread through social media, print media, online forums, and news broadcasts[6]. Popular topics include disinformation about trans identities, rights, and healthcare[6]. Also, "propagandists use grains of truth and polarization to manipulate public opinion"[9]. Two interviewees identified specific cases of disinformation through flyers, such as one promoting a fake BDSM story hour for children. Service Provider F was targeted under the pretense that they sold sex toys to children. The media scan also revealed that a right-wing outlet repeatedly misrepresented results from a poll to legitimize its stance.

Unfortunately, disinformation has real consequences: it increases distrust of traditional sources of information while also helping anti-trans individuals feel a sense of community towards each other[9]. As interviewees pointed out, misinformation and disinformation are also changing laws and affecting sexual health education in schools.

A tactic related to disinformation is to limit accurate information on queer and trans issues, like banning books from schools and libraries or limiting gender and sexual education in schools[5]. For example, third-party sexual education providers like Planned Parenthood were banned from schools in Saskatchewan in 2023. From now on, only teachers can provide education on these topics.

Institutional tactics

A range of institutional tactics were identified by half (11) the interviewees and in the media scan. The first type is regular people using institutional channels. For example, a flood of grievances was filed against the New Brunswick Ministry of Education over Policy 713. A journalistic investigation identified over 600 pages of letters, phone recordings, and emails filed against the Ministry; only four of these pages were filed before this policy sparked widespread outrage[23].

Other ways regular people use institutional channels as part of the anti-trans movement is by writing to their elected officials and petitioning[22]. In Quebec, one petition against public funds going towards drag story hours got over 23,000 signatures. Four interviewees also spoke of citizens co-opting assemblies like schoolboard meetings, parent-teacher events, and townhalls to bring up anti-trans talking points, and even running for a schoolboard position by using an anti-trans platform. Some complaints were also filed directly against five interviewees for their activism or work. Some anti-trans activists also contacted a funding agency to try to cancel an organization's funding.

Some of these tactics fall under anti-trans lobbying, which means trying to change public policy to reduce trans people's rights[6]. For example, lobbying against anti-discrimination legislation, against legislation that provides healthcare to trans youth, or against legislation that protects trans folks who wish to participate in sports in a way that matches their identity[24].

Another type of tactic is professionals using their institutions to harm trans people. Because her organization advocated for trans-affirming policy changes at her university, Hale was repeatedly targeted by professionals within the university setting. These professionals retaliated against her activism by using institutional means: she was sent a formal warning letter, was investigated, and was even discriminated against while applying for a paid position. Hiring anti-trans academics for speaking engagements or long term positions[12] is another way this tactic is deployed.

The last type of institutional tactic is big and small institutions pulling their weight to support of the anti-trans movement. On a small scale, it can be an organization writing an anti-trans public statement:

"And then [local church] put out a huge statement. Like saying like they do not support the trans community, don't support the 2S/LGBT none of it." -Mia

What is Policy 713?

Policy 713 set out standards over how schools would create a safer environment for 2S/LGBTQIA students in New-Brunswick. It was adopted in 2020. However, in May 2023, an ad promoting this policy caught the public's attention and sparked outrage.

This backlash led to the policy being changed in August 2023, in a way that compromises trans youths' safety and autonomy. Now, schools will seek parental consent before respecting youth's new name or pronouns, if they are younger than 16 [23].

What is the notwithstanding clause?

In Canada, federal and provincial governments have a responsibility to uphold human rights. However, they can sometimes override this responsibility by using the "notwithstanding clause". This clause allows governments to do things that violate human rights, for up to five years, without getting challenged in court [33].

Another example is schools obtaining "Family Friendly" certification to state they are anti-choice and protecting children from indoctrination[22].

On a big scale, governments have been pulling their weight in support of the anti-trans movement. For example, the Quebec government has been funding a known TERF organization since 2019, to the tune of $143,000 in 2022-2023 alone[25]. In December 2023, the same government allocated $800,000 to a "wise persons committee" tasked with reflecting on gender identity. The three wise persons are cis people, some with TERF ties[26].

Another example is governments changing policy and laws in ways that expose trans people to harm, for example with bathroom bills[7]. Unfortunately, the backlash against and change to Policy 713 inspired provincial governments across the country to follow suit. Similar changes became an election issue in Manitoba in September; Saskatchewan passed its Parents Bill of Rights in October; while Alberta announced upcoming policy changes in January 2024. The use of the notwithstanding clause is an especially harmful way the Saskatchewan government pulled its weight in support of the anti-trans movement.

Protests

Protests are a common tactic used by the anti-trans movement, as discussed by almost two thirds (14) of our participants. These protests range from a handful of anti-trans protestors to thousands, the most notable being the nation-wide 1 Million March 4 Children which happened in Fall 2023.

Participants identified several rallying points for anti-trans protestors:

- Against Pride and Pride events
- Against the inclusion of trans women and transfeminine people in gendered spaces
- Against drag story hours
- Against professionals supporting trans youth
- Against teaching or sharing information about gender or sexuality
- In support of school policies protecting parental rights.

Anti-trans protests discussed by participants happened in many locations, including:

- Schools and schoolboards
- Government buildings like city hall and the provincial legislature
- Elected officials' houses
- Highway overpasses
- Public libraries
- Civic centers and sports events
- Galas
- Queer-owned businesses
- In theirs or their organization's neighborhood, including queer neighborhoods

Specific tactics are used during anti-trans protests. These include interfering with people's access to trans- or queer-affirming events; promoting hateful messages; and filming themselves as propaganda[27].

Anti-trans protestors will also specifically use intimidation tactics, like trying to scare people into not attending a trans- or queer-affirming event, filming interactions with pro-trans protestors, and trying to provoke attendees into confrontation[27]. Three participants identified additional intimidation tactics like "shouting obscenities" and slurs, getting "in your face very close, a lot of screaming, like a lot of anger" and forming groups to follow counter-protestors as they leave (Ken, Anric, and Z).

Violence

The anti-trans movement also relies on violence, which more than half (13) of our interviewees reported. It would make sense that the anti-trans movement would use violence against trans people and trans-affirming organizations to advance their own goals.

Vandalism targeting their organizations, local trans-affirming businesses, Pride crosswalks, and individuals' own homes came up in 5 interviews. This included hateful graffiti, wrecking Pride decorations, breaking windows, and in two cases leaving dead animals' remains.

Trans people are especially at risk of harassment. In the Trans PULSE study[28], 34% of participants reported having been verbally threatened or harassed (n=433). The majority (19) of our interviewees experienced at least one form of hateful communication and half (11) reported verbal harassment: Hateful communication and verbal harassment include:

- Malicious questions and debating transness
- Hateful messages, emails, letters, phone calls, and face-to-face rants or even yelling
- Use of slurs and hate speech[13]
- Invalidating trans people's gender, including through misgendering
- Weaponizing people's image by filming them or taking their picture without consent
- Sharing videos of gore
- Encouraging individuals to commit suicide[13]

Threats were made against ten participants, their children, and their organizations, including:

- Death threats
- Invitations to put their kids up for adoption and threats to call in child protective services
- Rape threats
- Gun threats

Vaguer threats also came up in the media scan, such as anti-trans attackers stating they know where the person lives and when they're home.

Five participants also reported physical harassment like getting followed or street harassed by anti-trans individuals (experienced by two), trans students getting harassed at school (reported by two), and protestors showing up at an elected official's house (reported by one). Street harassment also came up in the media scan.

Assault is unfortunately used as a tactic by the anti-trans movement. In the Trans PULSE project, 20% of participants reported being physically or sexually assaulted for being trans[28]. Four of our participants reported experiencing or witnessing assault especially at protests, such as grabbing, punching, pushing, or hitting. Assault, armed assault, and assault against police officers in the context of protests were also reported in the media scan. The most brutal case of assault we identified was the stabbing of a gender studies professor and two students at the University of Waterloo in June 2023.

Lastly, murder of trans people may be used as an anti-trans tactic. One recent study[5] investigated patterns of anti-trans rhetoric, anti-trans legislation, and fatal violence against trans people in the United States, from 2015 to 2022. The authors found that all three aspects increased over this period and were correlated with each other. This means we can't (yet) prove that anti-trans rhetoric and laws cause anti-trans people to murder trans folks, but there is highly concerning evidence.

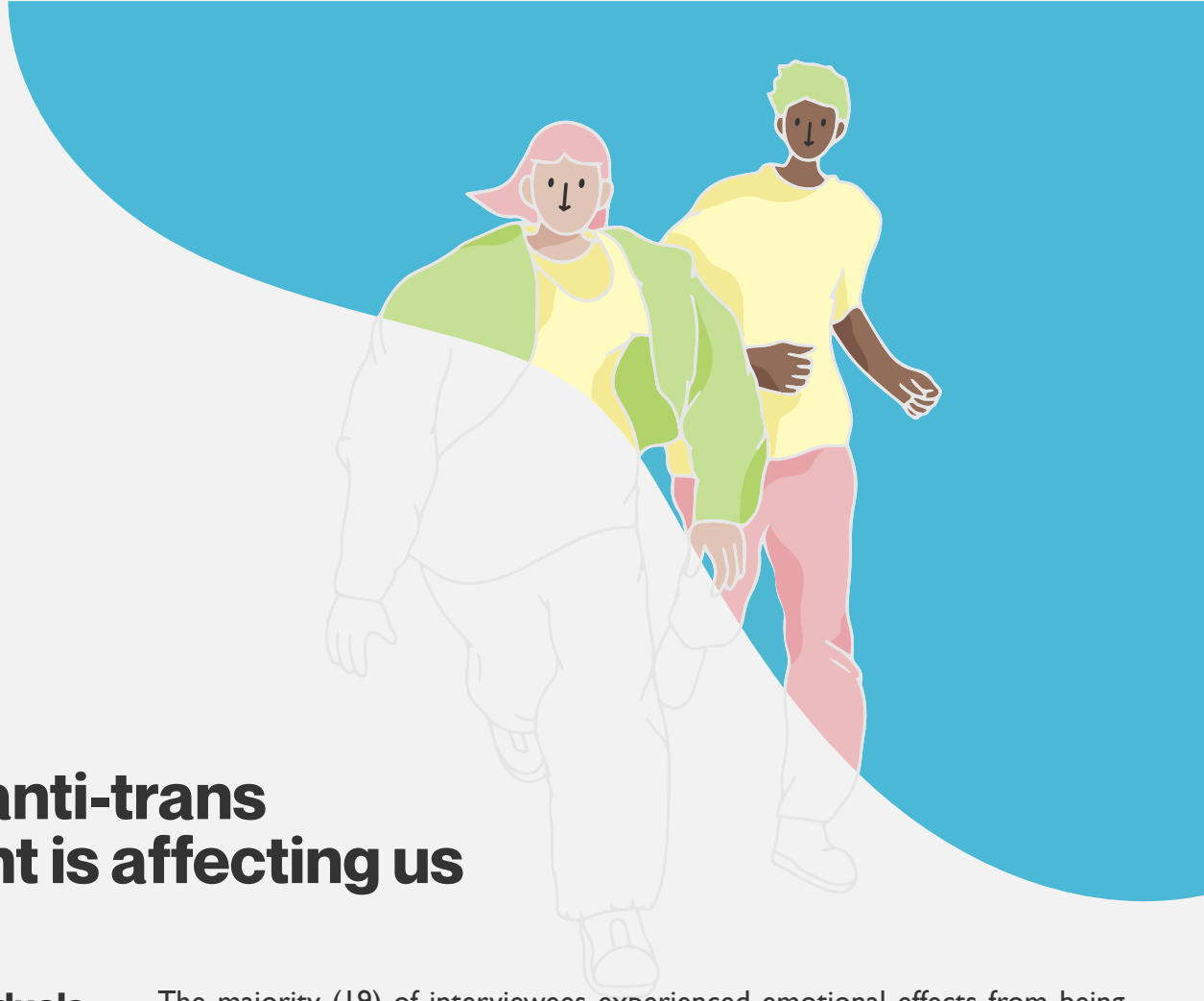
Intersectional tactics

The anti-trans movement relies on other forms of hate to inform its tactics. One way is by using transmisogyny. For example, deliberately excluding trans women and transfeminine people from women-only spaces[29]. Another example is last year's boycott of Hershey chocolate bars, after a Canadian trans woman was featured in the campaign[30].

The intersection between transphobia and racism also came up in seven interviews. Four participants reported that anti-trans attackers had used Nazi language and imagery. Racist and antisemitic slurs and language were also used against or witnessed by two participants, as well as one researcher[13]. Three racialized trans activists suspected they were specifically targeted based on the intersection of transphobia and racism:

"I was being harassed as a trans woman, I was being harassed as a person of color, like, you know." -Hale

The above quote from Hale also highlights the intersection of transmisogyny and racism. This is unfortunately unsurprising as one study[31] found that 45.8% of trans women reported having experienced transphobic hate crimes, and participants' race or ethnicity affected the type of hate crime experienced (n=629). In that study, Black and Latina trans women were at the highest risk of experiencing battery with a weapon.

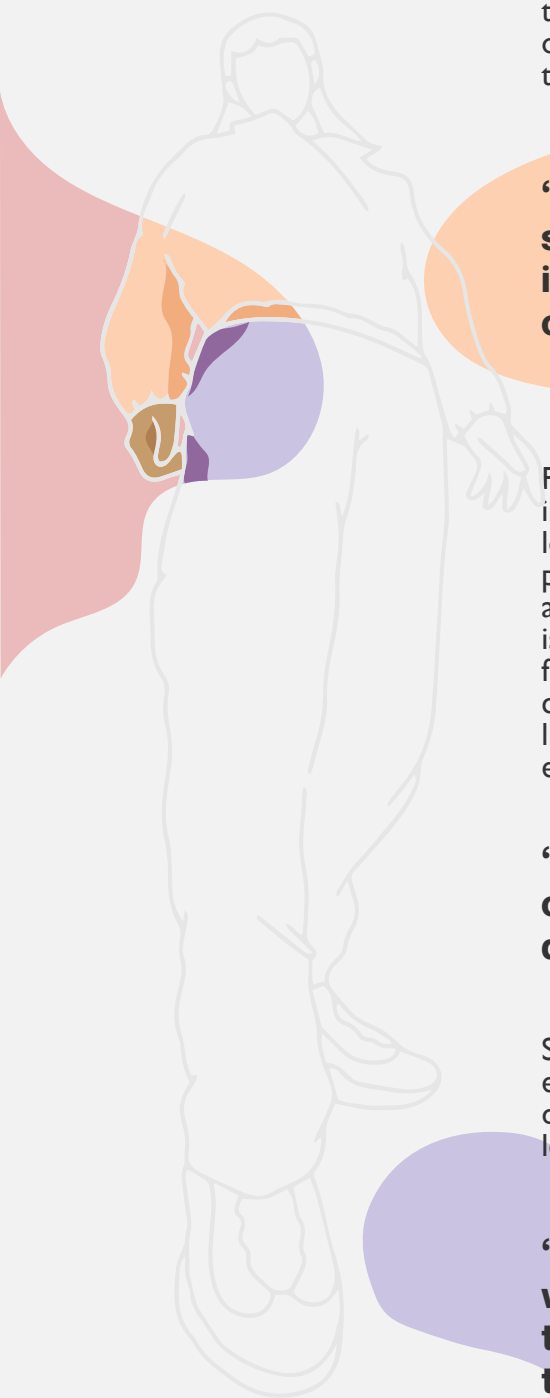


How the anti-trans movement is affecting us

Effects on individuals

The majority (19) of interviewees experienced emotional effects from being targeted by the anti-trans movement, either as individuals or as members of trans-affirming organizations. The most common emotional effect was fear (nine). This included the fear of losing their job and of child protective services intervening. One in three participants (eight) also reported PTSD-like symptoms like feeling traumatized, triggered, hypervigilant, and agoraphobic. Five participants felt angry or frustrated. Four participants reported anxiety and panic attacks, while four felt discouraged or disappointed. These experiences also made four participants either feel a sense a responsibility towards the trans community or question the responsibility they'd taken on. Other emotions that came up in three interviews or less were: complicated emotions, feeling upset and unsafe, distrust, guilt, helplessness, hurt, and worry. These negative experiences also increased one participant's internalized transphobia:

"I would say it definitely impacted me a lot on my mental health and like the saddest thing I feel about it is the internalized transphobia, just because all people reacted to trans people and how they, they are treating trans people, then like I intentionally I felt like if I come out as trans I would be perceived as othered and I would never be loved. [...] It's definitely, it made it worse. Like how yeah, just because the environment is like that. So. How I see myself and my self-worth and my, my confidence has definitely been impacted because of how the world is treating trans people." -JoJo



Some (six) participants experienced physical and material effects of anti-trans organizing. Two participants became a lot more visible suddenly. Two racialized trans activists experienced blowback at their job or while seeking employment, compromising their material safety. One participant's insomnia got bad enough that they sought out medication. It also made access to healthcare harder for one disabled racialized trans participant and their trans child, especially since they got harassed and assaulted in the context of seeking gender-affirming care:

"A lot of this anti-trans organizing and the rise of anti-trans sentiment is like it's really hard to know how far your doctor is going to go for you. You know, it's things like the gender clinic, even at [hospital] being absolute shit." -Natasha

Five participants also identified effects on their relationships and community. This included negative impacts on relationships with romantic partners and family, loosing friends, and isolation from community. As a Chinese transmasculine person, JoJo felt isolated from the Chinese community where some anti-trans attacks they experienced originated, as well as from the trans community which is predominantly white. As a Christian non-binary person, Mia felt isolated both from the religious community which is often anti-queer and from the queer community which is often suspicious of organized religion. One participant felt like the community at large was betraying trans folks, children, and teachers by engaging in the anti-trans movement:

"This is the community betraying the service providers, the children in the community, teachers in the schools... gender diverse people are everywhere." -Juno

Some racialized and disabled trans participants experienced intersectional effects, which were discussed in previous paragraphs. Two participants also discussed how navigating the anti-trans movement as someone with more or less privilege had vastly different consequences:

"The way in which we're antagonized, the way in which advocating as like a POC trans person and as a transfeminine person. It's like, significantly more dangerous than for folks with like, fewer intersections." -Hale

Pugicorn also discussed her family's economic and educational privilege in navigating the effects of the anti-trans movement. She added that her two trans children have vastly different experiences of transness and of the anti-trans movement because one passes as cis, while the other does not.

Effects on organizations

Most participants (17) were affiliated with trans-affirming organizations that had been targeted by the anti-trans movement, and 14 participants identified effects on their organizations.

Five participants reported effects on populations served by these trans-affirming organizations. Women's Organization A and Schoolboard A identified reduced reach on social media and reduced attendance at their events. Service Provider F's educational events were canceled by their local schoolboard. On a more positive note, Service Provider D and Queer Organization A noticed a growth in people using their services, to the tune of 400 new people for the latter. However, Wren noted frustration among clients of Service Provider D as a growth in demand for trans-affirming mental health services created longer waitlists.

There were also effects on staff. Twelve participants discussed emotional effects specific to staff like struggling to do their work and to remain professional towards attackers. As Norah noted, "it's hard because not only is it your identity, it's what you do for work, you know, like this means so much to me." Four participants also noted physical and emotional effects on staff, who are drowning and exhausted. As one person put it:

"Every time I sit down to read about the [anti-trans] bill in order to best speak about it. It feels like it takes like a year off my life. It is exhausting. To have to be the expert on transphobia because you are a trans person." -Levi

These effects were so detrimental that Alex resigned from Schoolboard A, while board members resigned from Queer Organization A.

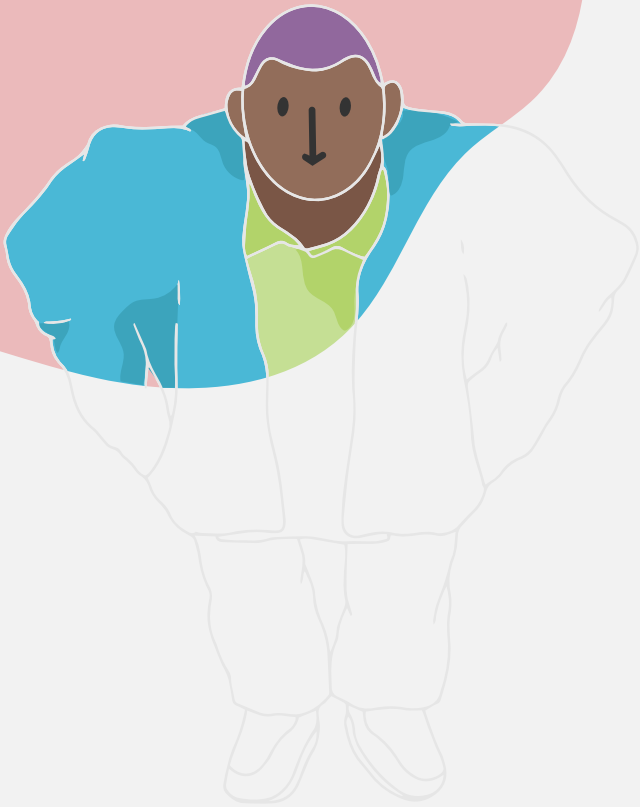
Anti-trans attacks also affected organizational capacity due to resignations, and because experiencing and responding to these attacks pulled significant time and energy away from regular tasks.

Effects on the broader community

Anti-trans attacks affected the broader community including trans people, students, and teachers, as ten participants discussed. Eight participants reported emotional effects on community: fear (six), frustration (one), and hypervigilance (one). Emotional effects on community also came up in the media scan and prior research, particularly how constant discrimination and dehumanization may be particularly detrimental to trans youth and lead to suicidal thoughts and behaviors[28].

Two participants discussed effects on accurate knowledge development and transmission within the community such as poor sexual education. Joe also discussed the risks of doing trans-affirming research and learning more about the trans community's needs, when researchers and practitioners are getting attacked for doing this work.

However, Bryn did identify a positive effect, as she had noticed a growth in organizing in her network, including teachers, educators, and parents getting more involved.



Responding to the anti-trans movement & fighting back

Keep fighting the good fight

Most participants (17) highlighted how they, their organization, and their community responded to anti-trans attacks by keeping up the good fight. Individuals responded by:

- Self-advocating and pushing back against complaints that were made against them
- Building up other people's hope
- Staying visible
- Coping through humor
- Experiencing growth in the way they responded to attacks

Organizations kept up the good fight in many ways:

- Maintaining and expanding services and events
- Using existing policy and reviewing policy
- Becoming more explicitly political

Five participants noted that trans staff at organizations often led the fight against and response to anti-trans attacks. However, this often involved taking on extra and even unpaid labor, like waking up early to handle social media before events. Alex and their trans colleagues were at the forefront and had to ask Schoolboard A, "Hey you know, what is this organization going to do about this to keep us safe, to keep trans people attending safe?"

Communities kept up the good fight by organizing, which half (11) of our participants discussed. This included restoring vandalized Pride crosswalks, fundraising to restore organization buildings, and canvassing campus to get people involved in mobilizations. One group of children and their parents even covered a local skating rink in chalk drawings and affirming messages the night before a counter-protest. One queer neighborhood created an art installation made from anti-drag posters to show support for drag artists.

Mirroring anti-trans tactics

The media scan and participants highlighted fighting back against anti-trans attacks by mirroring their tactics. For example, 13 participants reported countering disinformation on an individual level, at an organization, and in the community. This tactic also came up in the media scan. This included:

- Holding a teach-in
- Developing infographics, social media content, and campaigns backed by science
- Unpacking misinformation and disinformation in conversations
- Educating students and teachers about anti-trans laws, policies, and loopholes
- Using pre-existing guides and tools
- Getting interviewed in traditional media and publishing op-eds

Eight participants also reported using institutional tactics, which also came up in the media scan. Some individual and grassroots institutional tactics were:

- Filing complaints
- Showing up to assemblies and meetings
- Engaging in letter-writing campaigns and petitions

Institutional tactics used by trans-affirming and ally organizations were:

- Issuing public statements, such as 200 women's organizations affirming their solidarity with trans women
- Challenging anti-trans policy and law through court proceedings
- Local schoolboards creating their own policy to resist anti-trans directives coming from the Ministry of Education
- Ombudspeople submitting reports condemning anti-trans policies

Institutional tactics used by governments were:

- Issuing motions condemning the anti-trans movement
- Elected officials voting against their own party to protest anti-trans decisions

Individuals and organizations were involved in planning, amplifying information about, and attending pro-trans counter-protests. This tactic came up in ten interviews and in the media scan. In some cases, there were more counter protesters than anti-trans protesters:

"What was reported in the media then was that about 200 people showed up to counter protest. In comparison to maybe like 20-25 protesters. So they were vastly outnumbered by supporters." -Ken

Some tactics used by pro-trans counter-protesters included:

- Making noise to drown out anti-trans chants and speeches, ex. using instruments, pots and pans, and speaker systems
- Blocking hateful signs and creating blockades with huge fabric panels
- Having some physical altercations with protesters

Allies showing up

Allies fighting back against anti-trans attacks came up in six interviews. This included cis queer community members, parents, town members, religious figures, youth and labor organizations, and elected officials. This also included a city council refusing to change policy when anti-trans people invaded a meeting. One participant also reported that their white woman boss used her privilege to get legal and financial support for their Indigenous coworker who got assaulted by police at a counter-protest. Even within the trans community, people with more privilege showed up for a trans woman participant:

"I had like a bunch of trans men standing around the rest of the day just like making sure nobody was coming back and if they did, they were gonna be mobbed by a bunch of people."
-Charlotte

Levi also reported some frustration over misguided allyship. Sometimes school employees came to them to ask for guidance in responding to parents who were concerned about protecting their children. And other times, school employees came to Levi to commiserate over complaints that had been made about Levi. They concluded that allies needed to put in the work to learn some of these things on their own.

Four participants also reported ways allies failed them. For example, schoolboards and teacher unions stating they were pro-trans in private, yet never physically showing up or publicly stating this support. Another example is universities and social media platforms either not showing up, or actively harming trans people and trans-affirming organizations.

Ensuring safety and wellbeing

Divesting from police

Eight participants reported that they or trans-affirming organizations they'd been involved with had sought out police as a response to anti-trans attacks. Four reported police had made arrests, and in one case the attacker was even convicted of a hate crime. However, nine participants discussed how police were unhelpful in responding to anti-trans protests and violence, and this also came up in the media scan. The media scan indicated that police made arrests at protests for assault, armed assault, assault on police officers, mischief, disturbing the peace, and hateful materials. However, some of these interventions may have been aimed at pro-trans counter-protesters. Indeed, one participant noted that police response in their area was to ban both protests and counter-protests, while another reported at least one of three arrests at a recent event was against a pro-trans counter-protestor. It is especially telling that the only participant who mentioned police response in an overall positive way was a cis, straight ally whose organization did not primarily work with trans people.

In addition to being unhelpful, police are unsafe to trans communities. In the Trans Access to Justice project[2], over one in five respondents experienced police harassment and violence (n=703), while this statistic came up to one in four in the Trans PULSE project[28] (24%). Racialized trans people and sex workers are at even higher risk of experiencing police violence. Almost half (46%) of the sex workers in the Access to Justice project had experienced police violence, as opposed to 16% among non-sex workers (19% of participants were sex workers). More than one in three (35%) Indigenous participants had experienced police violence and harassment, as opposed to 22% of non-Indigenous participants (8.7% of participants were Indigenous)[2].

In the current study, six participants indicated police are unsafe to trans communities. Two participants reported witnessing police use force on pro-trans counter-protestors. One participant's Indigenous coworker, who showed up in support of a drag story time, was physically assaulted by the police. Two participants viewed the police as affiliated with the anti-trans movement. One of these expressed how unsafe that made police to racialized trans folks:

"And there's nothing you can do here in [city] really, if you're racialized, and like calling the cops when you know that the cops are also in the [freedom] convoy's pocket. And especially with a trans child in the house, like that's just not going to happen." -Natasha

Because police are unsafe to trans people, Queer Organizations E and F had policies to avoid seeking out police, including by not inviting them to Pride events. Alex pushed for similar changes at Schoolboard A. At Queer Organization F, police were a last resort in pre-determined situations like gun threats, and otherwise were contacted through the non-emergency line for example when Pride crosswalks got vandalized.

Six participants instead emphasized alternatives to involving police which were used within organizations and the community:

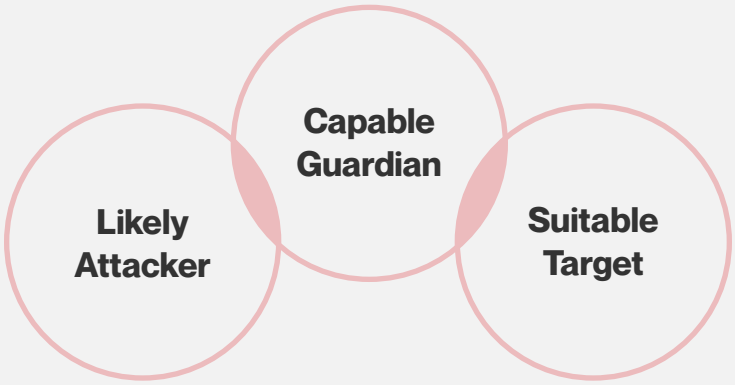
- Having people trained in de-escalation tactics circulate
- Having community members screen a building before an event
- Having more privileged people use their bodies as buffers at counter-protests
- Implementing a neighborhood watch and cop watch
- Documenting and tracking bad actors
- Advocating for the reallocation of police funds to social services
- Engaging in mutual aid and community care

Implementing safety measures

Participants reported many means of situational prevention to ensure the safety of individuals, organizations, and the broader community.

What is situational prevention?

Situational prevention is a concept that comes from criminology. It means states that opportunities for crimes happen in an environment where a likely attacker and a suitable target come together, in the absence of a capable guardian[32].



Based on this concept, opportunities for anti-trans attacks can be reduced by changing parameters in the environment:

- Making potential targets less visible or attractive to attackers
- Discouraging potential attackers
- Having capable guardians, which often means having potential witnesses around[32]

Situational prevention can come across as victim-blaming when people are expected to take on the responsibility of protecting themselves from crimes and other attacks. To be clear, being attacked is never a victim's fault. However, using prevention measures can help community members feel a lot safer and reduce the harms they experience if attacked.

As part of situational prevention, activists, organizations, and the broader community made potential targets less attractive to attackers by being strategic about visibility. Half (11) of our participants reported ways they were intentional about visibility, for example:

- Avoiding public transit
- Pulling their trans kid out of school
- Censoring theirs or their kid's online presence
- Limiting their organization's visibility on social media
- Having boundaries around privacy
- Removing themselves from harmful situations

Four participants reported implementing measures to protect staff's identity and personal information at their organizations. Two participants also discussed the importance of protecting theirs and their peers' identities at counter-protests.

Similarly, participants made themselves into unattractive targets by being strategic about language. Individuals and organizations were very strategic about the terminology they used to make sure they weren't attracting unwanted attention. For example, Queer Organization E pushed to remove the mention of vaginal dilators from a health insurance policy change. Women's Organization A also chose to be strategic about language by saying "Pride" instead of 2S/LGBTQIA because this term is less politically charged.

Others means of situational prevention are summarized in table 3.

Table 3
Ways to improve safety through situational prevention

Where	Reported by	How
At home	4	• Adopting a big dog • Using a home camera • Carrying non-lethal weapons for self-defence • No longer hosting events
At the organization	12	• Controlling access to services, staff, events, and social media - Letting calls go to voicemail - Being an appointment-only service - Being strategic about publicizing events - Having a receptionist - Registering and screening attendees or members • Improving tech - Improving cybersecurity and the security system - Installing a video-recording doorbell - Staff having work phones • In buildings - Installing a shatterproof window - Entering through the back entrance - Using the buddy system - Keeping the door locked - Removing anti-trans people from the premises - Strategically choosing organization and event locations • Being prepared - Doing safety planning before events - Following safety training - Designating someone to get children away from harmful situations
In the community	8	• At counter-protests - Having safety teams - Using the buddy system • In general - Cancelling their own events when the risk is too high - Removing anti-trans people from protests and pushing them out of town

Outside of situational prevention, two in three participants (15) discussed the importance of being strategic about engaging with anti-trans individuals.This was the case in person but especially online, both for individuals and organizations. Participants agreed that engaging was only worthwhile when questions or comments that seemed inappropriate or offensive at first glance were made in good faith. Otherwise, they reported and screenshotted comments and blocked attackers on social media; hung up the phone; and ignored hate mail. One reason for this was to not give legitimacy to harmful rhetoric, but also to protect community members who might see hateful comments online.

Care and support

Half (11) of our participants responded to anti-trans attacks by practicing self-care and leaning on community. This included taking breaks, remembering these attacks are not our fault, and knowing and setting boundaries. Self-care includes leaning on others such as seeking support from friends, loved ones, and mental health professionals. As the single employee at her organization, Sarah also sought support from colleagues in other organizations.

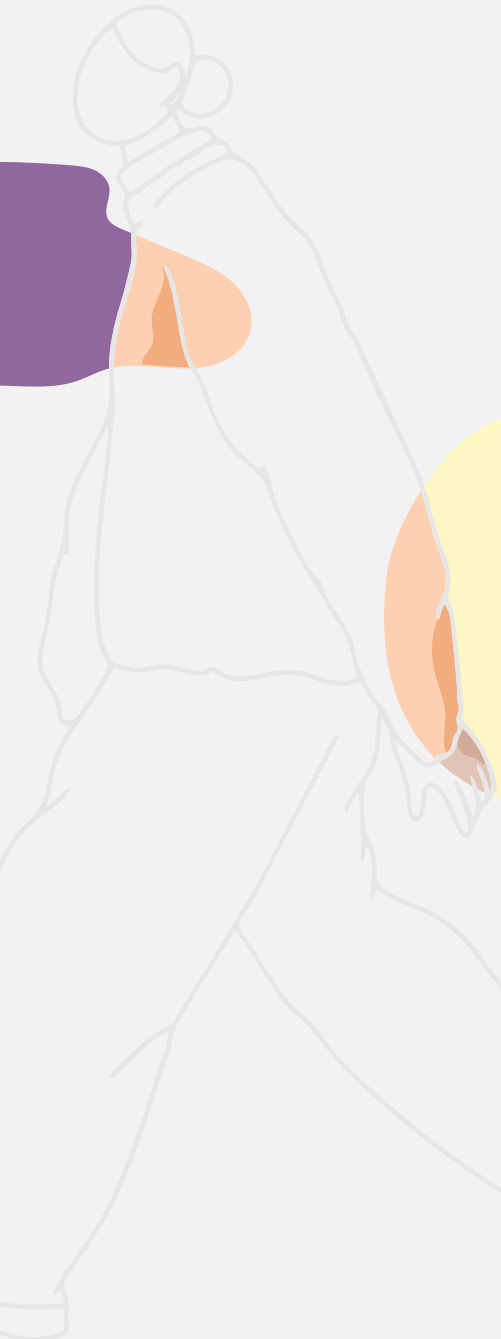
Twelve participants discussed how their organizations implemented ways to ensure staff safety and support. This included:

- Removing staff from harmful situations
- Allowing for flexibility and improving benefits
- Removing ineffective board members
- Setting clear work/life boundaries
- Giving the impression there is more staff
- Making space for emotional processing, care, and support
- Leadership protecting other staff from complaints

Unfortunately, Norah and Levi were not supported by their trans-affirming organizations and this lack of support severely affected them.

Ten participants also reported ways their organizations ensure the wellbeing of the population they served; these were covered in the previous section.

One last way community ensured wellbeing was to engage in community debriefing after counter-protests:



“Situations where we got together and talked about things and while that doesn’t necessarily make you feel safe in the moment, once you’re together and you are all talking about it, I did feel a sense of safety there. Knowing that you know we’re all experiencing it and like oh like what did you do, this is what I did, and I didn’t find it helpful you know. And then just knowing that people were wanting to follow up. I found to make me feel a little bit safer.” -Anric

Recommendations

1. Participants emphasized the importance of keeping up the good fight and not backing down. They also highlighted the importance of allies and ally organizations joining the fight.

a. We ask systems and institutions to join us as allies in this fight, and to obtain meaningful and ongoing training to ensure accountability in interactions with our community.

2. As a research team, we wish to reiterate the importance of divesting from police in responding to anti-trans attacks. Police are unsafe to trans people, especially to those of us who experience multiple intersections. We strongly encourage trans-affirming organizations to review their policies accordingly.

a. We recommend that governments intentionally (re)direct meaningful funding to community organizations that work with 2Spirit, trans, non-binary, and gender diverse communities, including organizations that provide mental health services and material support.

3. All would benefit from implementing prevention measures to protect themselves and others against anti-trans attacks. By being prepared, we can minimize the consequences of these attacks on people, organizations, and community members.

4. Organizations need to step up to protect staff who are targeted.

5. We encourage relying on a diversity of tactics to effectively fight back against the anti-trans movement.

6. Future research on the anti-trans movement needs to focus on the experiences of 2Spirit and trans, non-binary, gender diverse folks who are Black, Indigenous, and People of Color (BIPOC). This research should be developed and conducted by trans BIPOC, according to decolonial and anti-racist research methodologies and principles.

"I've actually also been [...] deeply moved by both how much people have come together and I think the creativity and the breadth of strategies I think has been yeah, really moving but also really inspiring and that I think that's one thing maybe I haven't seen in other forms of activism that I've been a part of before." - Bryn

As final thoughts, we'd like to remind trans people and our allies that **the anti-trans movement is an unstable coalition.** Its factions have incompatible values, which is likely to lead to in-fighting and ultimately, to this coalition's collapse.

Similarly, we need to keep **building our own coalitions** with leftist, anti-racist, and intersectional feminist groups. These groups make us stronger as we have compatible ideologies: we all aim to improve the material conditions of oppressed groups.

Together, we are stronger than the anti-trans movement.

Endnotes

1 Leitao, R. 2SLGBTQIA+ organizations rally for more funding, support amidst growing anti-gender movement | Future of Good. Future of Good (2023).

2 JusticeTrans. 2STNBGN Perspectives on Access to Justice: A Legal Needs Assessment. https://justicetrans.org/wp-content/uploads/2023/09/2STNBGN_Perspectives_on_Access_to_Justice-Report.pdf (2022).

3 Marcoux Rouleau, A. Lessons from insiders: Embracing subjectivity as objectivity in victimology. International Review of Victimology 1–23 (2023) doi:10.1177/02697580231179489.

4 Ashley, F. Accounting for research fatigue in research ethics. Bioethics 35, 270–276 (2021).

5 Brightman, S., Lenning, E., Lurie, K. J. & DeJong, C. Anti-Transgender Ideology, Laws, and Homicide: An Analysis of the Trifecta of Violence. Homicide Studies 0, 1–19 (2023).

6 Billard, T. J. "Gender-Critical" Discourse as Disinformation: Unpacking TERF Strategies of Political Communication. Women's Studies in Communication (2023).

7 Vipond, E. Trans Rights Will Not Protect Us: the Limits of Equal Rights Discourse, Antidiscrimination Laws, and Hate Crime Legislation. Western Journal of Legal Studies 6, (2015).

8 Pearce, R., Erikainen, S. & Vincent, B. TERF wars: An introduction. The Sociological Review 68, 677–698 (2020).

9 Action Canada for sexual health and rights. Campaigning to Win in a Time of Populist Politics. (n.d.).

10 Egale. Anti-Gender Politics in Post-Secondary Education in Canada. (2023).

11 Important Context About the "1 Million March 4 Children". Canadian Anti-Hate Network https://www.antihate.ca/1_million_march_4_children (2023).

12 House, C. C. A. 'I'm Real, Not You': Roles and Discourses of Trans Exclusionary Women's and Feminist Movements in Anti-gender and Right-wing Populist Politics. DiGeSt - Journal of Diversity and Gender Studies 10, (2023).

13 Walker, A. Transphobic discourse and moral panic convergence: A content analysis of my hate mail. Criminology 61, 994–1021 (2023).

14 Dyer, J. et al. Media discourse in Canada on trans youth and parent advocacy. Feminist Media Studies 0, 1–17 (2023).

15 Koch-Rein, A., Haschemi Yekani, E. & Verlinden, J. J. Representing trans: visibility and its discontents. European Journal of English Studies 24, 1–12 (2020).

16 Adam Hunter. Civil liberties association calls Sask. government school naming and pronoun policy discriminatory. CBC Saskatchewan (web site) (2023).

17 Corrêa, S., Paternotte, D. & House, C. Contours, meanings and effects of anti-gender politics. in Routledge Handbook of Sexuality, Gender, Health and Rights (eds. Aggleton, P., Cover, R., Logie, C. H., Newman, C. E. & Parker, R.) 484–493 (Routledge, 2024).

18 Williams, C. The ontological woman: A history of deauthentication, dehumanization, and violence. The Sociological Review 68, 718–734 (2020).

19 Hines, S. Sex wars and (trans) gender panics: Identity and body politics in contemporary UK feminism. The Sociological Review 68, 699–717 (2020).

20 Ozten Shebahkeget. Manitoba library, drag queens deliver story time event as protesters gather outside. CBC Manitoba (web site) (2023).

21 Egale. Court decision finds use of "groomer" slur against drag performers to be rhetoric based on hurtful and hateful myths and stereotypes. Egale https://egale.ca/egale-in-action/rad-v-webster/ (2023).

22 Graff, A. & Korolczuk, E. Anti-Gender Politics in the Populist Moment. (Routledge, London, 2022). doi:10.4324/9781003133520.

23 Alam, H. New Brunswick's Pride in Education day in May mobilized opposition to Policy 713. St. Albert Gazette (2023).

24 Crasnow, S. J. The Legacy of 'Gender Ideology': Anti-Trans Legislation and Conservative Christianity's Ongoing Influence on U.S. Law. Religion and Gender 11, 67–71 (2021).

25 Morris, E. Critics call on Quebec to cut funding to 'overtly transphobic' women's group. CBC News (2023).

26 Lefebvre, J. La filière PDF Québec frappe encore. Pivot (2023).

27 Canadian Anti-Hate Network. Guide for Pride Defenders. (2023).

28 Bauer, G. & Scheim, A. Transgender People in Ontario, Canada: Statistics from the Trans PULSE Project to Inform Human Rights Policy. (2015).

29 Baril, A. Francophone Trans/Feminisms. TSQ: Transgender Studies Quarterly 3, 40–47 (2016).

30 Brend, Y. Supporters rally around trans activist in Hershey's Women's Day campaign | CBC News. CBC https://www.cbc.ca/news/canada/hershey-fae-johnstone-transgender-1.6765214 (2023).

31 Gyamerah, A. O. et al. Experiences and factors associated with transphobic hate crimes among transgender women in the San Francisco Bay Area: comparisons across race. BMC Public Health 21, 1053 (2021).

32 Felson, M. Crime & Everyday Life. (Pine Forge Press, 1998).

33 Government of Canada, D. of J. Canadian Charter of Rights and Freedoms. Notwithstanding Clause vol. Section 33 (1999).