

Facebook Expands Definition of Terrorist Organizations To Limit Extremism

(nytimes.com)



81



Posted by BeauHD on Tuesday September 17, 2019 @10:10PM from the what-to-expect dept.

Facebook on Tuesday [announced](#) a series of changes to limit hate speech and extremism on the social network, [expanding its definition of terrorist organizations](#) and planning to deploy artificial intelligence to better spot and block live videos of shooters. The company is also expanding a program that redirects users searching for extremism to resources intended to help them leave hate groups behind. The New York Times reports:

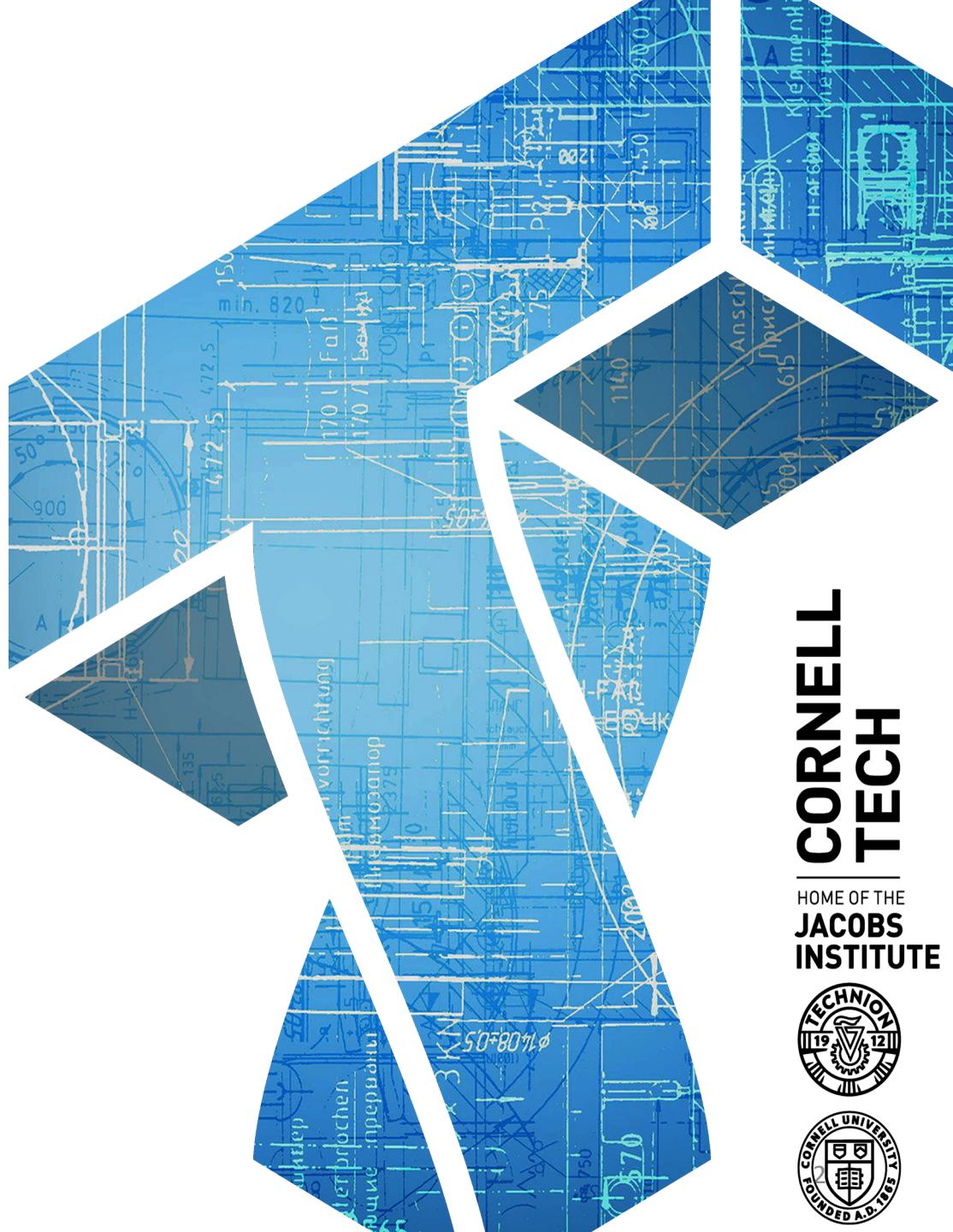
The announcement came the day before a hearing on Capitol Hill on how Facebook, Google and Twitter handle violent content. Lawmakers are expected to ask executives how they are handling posts from extremists. In its announcement post, Facebook said the Christchurch tragedy "strongly" influenced its updates. And the company said it had recently developed [an industry plan](#) with Microsoft, Twitter, Google and Amazon to address how technology is used to spread terrorist accounts.

Facebook said that it had mostly focused on identifying organizations like separatists, Islamist militants and white supremacists. The company said that it would now consider all people and organizations that proclaim or are engaged in violence leading to real-world harm. The team leading its efforts to counter extremism on its platform has grown to 350 people, Facebook said, and includes experts in law enforcement, national security, counterterrorism and academics studying radicalization. To detect more content relating to real-world harm, Facebook said it was updating its artificial intelligence to better catch first-person shooting videos. The company said it was working with American and British law enforcement officials to obtain camera footage from their firearms training programs to help its A.I. learn what real, first-person violent events look like.

CS 5435: Non-profit- motivated abuse and harassment

Instructor: Tom Ristenpart

<https://github.com/tomrist/cs5435-fall2019>



Announcements

- Homework 1 due in one week!
- Slight schedule change:
 - Mon/Wed lecture on web security (finishing abuse today)
 - Homework 2 will be released Thursday or Friday of next week
(originally scheduled for Wednesday)

Commercially-motivated abuse

- **Facebook:** spammer accounts, fake fraud accounts, ...
- **Twitter:** illicit promotional accounts, ...
- **Yelp:** fake reviews, fake restaurants, ...
- **AirBNB:** scam rental or experience ads
- **Lyft:** colluding drivers + riders
- **Google:** spammers using Gmail, advertisers violating terms of service, SEO, Play store bad apps, ...

How to prevent fraudulent actions?

- **Content analysis**
 - Spam filters
- **Identify bad accounts**
 - Correlate bad actions with accounts, try to detect bots
 - Sock-puppet accounts (many controlled by one person)
- **Identify bad devices**
 - Device cookies to correlate different account accesses
 - IP blacklists, ISP blacklists
- **Target fraud-support infrastructure**
 - Botnet takedowns, bank accounts, civil/criminal legal actions

Examples of other forms of abuse

- Online harassment and bullying
 - Coordinated campaigns
 - Doxxing, raiding (other websites), ...
- Misinformation campaigns
- Targeted attacks and RATs (remote access trojans)
- Tech abuse in intimate partner violence

Coordinated harassment campaigns

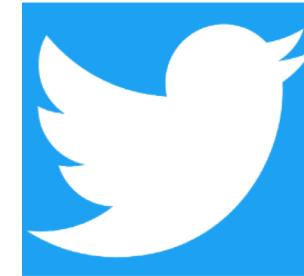


- Anonymous bulletin board
- Generated lots of memes, known to host some child porn (though technically against site policy)
- Associated with Anonymous hacker group
- Used to coordinate harassment, bullying, hacking
- Associated with alt-right groups
- Involved in Gamergate, banned Gamergate discussion



- Similar to 4chan (different site operator)
- No longer available due to CloudFlare and other providers dropping it

Coordinated harassment campaigns: Gamergate



- Sustained harassment campaign against female gaming developers and others
 - Rape threats, murder threats, doxing (home address, other personal information disclosed)
 - Astroturfing, sock-puppet campaigns on Twitter
- Organized on 4chan & (after banning on 4chan) 8chan, most harassment played out on twitter (#gamergate)
- Why? Ex-boyfriend of initial victim posted false claims about victim
 - “Right-wing backlash against progressivism” (in gaming)

Mininformation campaigns



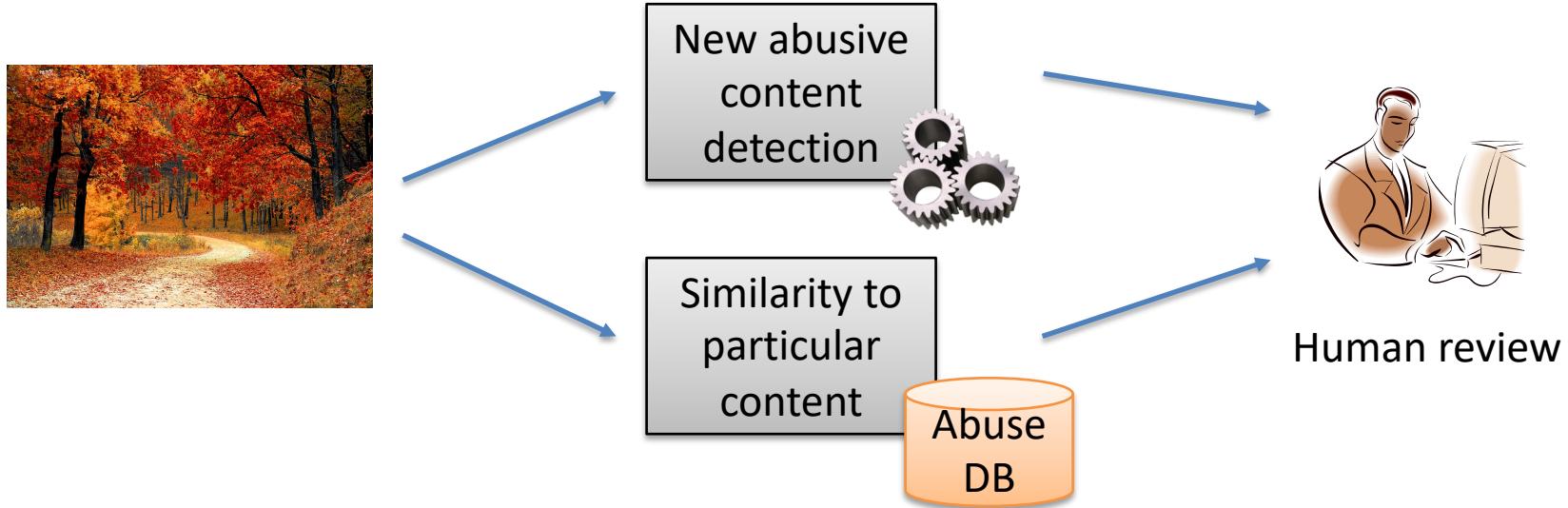
4chan



- Pizzagate conspiracy
- QAnon conspiracy
- 2016 election interference
 - Cambridge Analytica
 - Russian influence operations
- Research studies indicate falsehoods spreads faster than truth on social media

“there is a worldwide cabal of Satan-worshipping pedophiles who rule the world, essentially, and they control everything. They control politicians, and they control the media. They control Hollywood, and they cover up their existence, essentially. And they would have continued ruling the world, were it not for the election of President Donald Trump,”
-Travis View

Identifying abuse content



- Use locality-sensitive hashing to check if similar to known bad content
 - H such that $|H(\text{image}) - H(\text{image}')| < \text{threshold}$ if image, image' very similar
- Use machine learning to try to identify patterns indicative of abusive content
 - Is image a picture of a naked child?
- Refer out to human for review (Facebook has 10,000s of moderators)
- Content flagged by users also sent through reviewing pipelines
 - Flagging mechanisms also subject to abuse (illicit takedowns)

Targeted attacks

- Dissidents, journalists, activists targeted by nation-states
 - Phishing attacks, botnet-style C&C servers to collect data
 - Remote Access Trojans (RATs)
- Small industry of companies providing “lawful access” tools

From: Melissa Chan <melissa.aljazeera@gmail.com>
To:
Sent: Tuesday, 8 May 2012, 8:52
Subject: Torture reports on Nabeel Rajab
Acting president Zainab Al Khawaja for Human Rights Bahrain reports of torture on Mr. Nabeel Rajab after his recent arrest.
Please check the attached detailed report along with torture images.

►  1 attachment: Rajab.rar 1.4 MB  Save

Figure 1: E-mail containing FinSpy.

<https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-blond.pdf>

<https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-marczak.pdf>

<https://www.usenix.org/system/files/conference/usenixsecurity14/sec14-paper-hardy.pdf>

Targeted personal attacks

25% of women suffered **rape, physical violence, and/or stalking**
11% of men **by an intimate partner**

[National Intimate Partner and Sexual Violence Survey 2010-2012]

Intimate partner violence (IPV) abusers exploit technology:

- Harassing texts/messages
- GPS devices & spyware apps
- Victim accounts being “hacked”
- Physical device access
- ...

Research at Cornell Tech



Qualitative studies of IPV ecosystem in NYC

Freed, Palmer, Minchala, Levy, R., Dell. *Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders*, CSCW 2017

Freed, Palmer, Minchala, Levy, R., Dell. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology, CHI 2018

IPV spyware & anti-spyware measurement studies

Chatterjee, Doerfler, Orgad, Havron, Freed, Levy, Dell, McCoy, R. *The Spyware Used in Intimate Partner Violence*, Oakland 2018

Clinical computer security models and tools

Havron, Freed, Chatterjee, McCoy, Dell, R. *Clinical Computer Security for Victims of Intimate Partner Violence*, USENIX Security 2019

Freed, Havron, Chatterjee, McCoy, R., Dell. "Is my phone hacked?" Analyzing Clinical Computer Security Interventions with Survivors of Intimate Partner Violence, CSCW 2019

New York City Family Justice Centers



**Mayor's Office to
End Domestic and
Gender-Based Violence**

Range of services for domestic violence, sex trafficking, and elder abuse victims:

- Civil / legal services
- Counseling & safety planning
- New York Police Department (NYPD)
- District Attorney's offices
- Access to emergency shelter
- Non-profit organizations

ENDGBV runs ***Family Justice Centers***
One in each neighborhood of NYC



Year-long qualitative study: methods

Clients
(Survivors /
Victims)

11 focus groups with 39 women (English & Spanish)
ages 18-65 (average 42)
from 15 different countries
with range of education levels
most no longer living with abusive partner

Professionals

Semi-structured interviews with 50 professionals
female (45) and male (5)
case managers, social workers,
attorneys/paralegals, & police officers

Largest and most demographically diverse study to date

Client Story #1

"I was raised in a country in which women are trained to serve men. I'll say that he never hit me, basically, but he did the worst thing ever. Honestly, I would probably rather that he hit me instead of the things that he did to me.

Use shared ownership to install spyware

So he put a spyware in [our] computer. Obviously, I didn't know because he studied computer programming, so he was very savvy about it. ...

Non-consensual intimate images

Account compromise

So he went into my computer, he got my Facebook password, email password, and he shared naked pictures of me. He sent them from his Facebook to my bosses. He took my phone and he sent them through private messages to several friends, but also through my email and my Facebook because he had the password.

Device compromise

Impersonate victim

The embarrassment that I went through, the public humiliation, it... beat me to the ground"

Four categories of common attacks

Ownership-based

- Abuser owns device/account
- Shared account/device
- Buying children device
- Prevent use / destroy device
- Digitally control access
- Track location, monitor usage

Account/device compromise

- Physical access to unlocked device
- Force password / pin revelation
- Remotely “hack” via security questions / passwords
- Install spyware / “dual-use” app
- Track location, monitor victim
- Steal or delete info
- Lock victim out of account
- Impersonate victim

Harmful messages or posts

- Call/text/message victim (from spoofed account)
- Post harmful content (e.g., threaten violence)
- Harass victim’s friends/family
- Proxy harassment

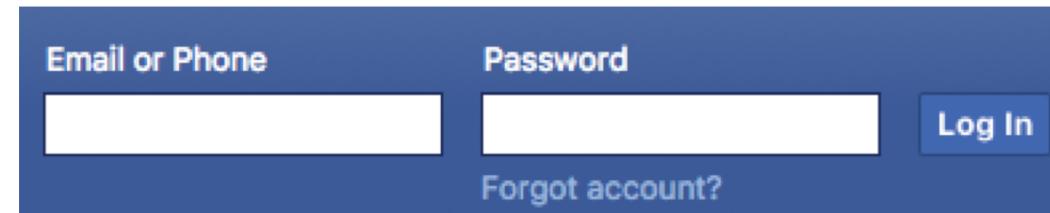
Exposure of private information

- Blackmail by threat of exposure
- “Doxxing” victim
- Non-consensual intimate images
- Fake profiles/advertisements of sexual services

Attacks not technically sophisticated, but succeed because threat models don't match threats

Threat models specify:

- (1) Who are Attacker and Victim
- (2) Attacker's capabilities & goals



Account login – IPV threats

Threat	Description	Defense?
Abuser knows password (different location)	Abuser knows password and logs in from different location	Two-factor authentication; device authentication
Abuser knows password (same location)	Abuser knows password and logs in from same household or even device	Change password; use two-factor authentication
Abuser compels password disclosure	Abuser forces password disclosure (emotional or physical coercion)	Decoy passwords?
Abuser uses device to gain access	Session cookies allow abuser to login from device without auth checks	Delete session cookies

“[The abuser] stole her computer and was able to access all this information . . . her school applications, her bank accounts, all sorts of things, and gain access and control of these things. That . . . had a totally traumatizing effect.”
- Case manager

The spyware problem

“An abusive partner kicked in our front door and wound up in the lobby of our building by tracking her phone . . . it was some secondary application that the abuser had put on it and knew exactly where she was. He literally kicked our front door open. We called the police ... it was scary.” – Case manager



Spy On Your Girlfriend's Cell Phone Without Touching It

A promotional image for Spy Master Pro. On the left, a man in a suit looks thoughtful with his hand to his chin. On the right, a woman with glasses and a smile is talking on a phone. Between them is the text: "Cheating Partner?", "Spy on their phone secretly!", and the Spy Master Pro logo, which includes a stylized eye icon and the text "SPYMASTER PRO".

Cheating Partner?

Spy on their phone secretly!

 SPYMASTER
PRO

<https://www.spymasterpro.com/>

A typical off-store spyware app



All-Inclusive Mobile Phone Spy

- ✓ Spy on all iOS and Android devices
- ✓ Track SMS, Call logs, App chats, GPS etc.
- ✓ No Rooting or Jailbreaking required
- ✓ Invisible mode, monitor the activity remotely

Covert

Remotely record audio,
video, and alter settings

Real-time + historical



Smooth (ab)user experience with off-store spyware

Installing is easy
Whole process takes ~5 min

On victim's device:
No app icon, no notification

On abuser end:
Fancy web UI or apps



The image displays two screenshots of the Spyzie mobile application. The left screenshot shows a dark-themed dashboard with a sidebar menu containing options such as Dashboard, Calls, Contacts, Messages, Social Apps (labeled HOT), Locations, Geofences (labeled HOT), Capture Screenshots, Browser History, Photos, Video Preview, Calendars, Keylogger (labeled HOT), and App Relevant Info. The right screenshot shows a light-themed dashboard with tabs for Android Demo and iOS Demo, and sections for Calls (5 notifications), Messages (10 notifications), Locations (3 notifications), Facebook (15 notifications), Snapchat (20 notifications), WhatsApp (5 notifications), Browser History (27 notifications), Contacts (1 notification), Photos (3 notifications), Video Preview (1 notification), Capture Screenshots (2 notifications), and Keylogger (54 notifications).

How do abusers find spyware apps?

Need large number of query terms that an abuser might use

→ How to spy on my husband

All Videos Shopping News Images More Settings Tools

About 11,700,000 results (0.44 seconds)

How to Spy on My Husband's Cell Phone Without Touching It?
<https://besttrackingapps.com/spy-on-your-spouse/> ▾
Dec 15, 2017 - Hundreds of people wonder "how to spy on my husbands cell ... How Can I Track My Husbands Cell Phone Without Him Knowing and for Free?
So, How to Spy on My ... · How to Catch a Cheating ... · How Can I Track My ...

How to Spy on My Husband's Phone Without Him Knowing! - YouTube
 <https://www.youtube.com/watch?v=LBTf2jEEdCo> ▾
Aug 18, 2016 - Uploaded by Richard Smith
Cell Phone **Spying** Software - Track Anyone Via Phone With Ease .This is the BEST Monitoring Software and ...

How can i spy on my husband cell phone without touching his cell ...
[smstrackers.com](#) › Tracking My Partner ▾
The popularity of mobile **spy** software is increasing every passing day as worried wifes want to confirm that their **husbands** are absolutely honest with them at all ...

How can I spy on my husband cell phone without touching ... - Guestspy
guestspy.com/can-spy-husband-cell-phone-without-touching-cell/ ▾
Jan 10, 2017 - How can I **spy on my husband** cell phone without touching his cell. GuestSpy is a strong tracking tool with a few attributes that are truly ...

Blogposts comparing spy apps

Video how-to guides

Ad funnels for spy apps

Spy app websites

Search engines give query suggestions

how to spy on my

how to spy on my **husband**

how to spy on my **boyfriends phone**

how to spy on my **boyfriends iphone**

how to spy on my **girlfriends iphone**

how to spy on my **husband iphone**

how to spy on my **boyfriends facebook messages**

how to spy on my **husband phone**

how to spy on my **son's iphone**

how to spy on my **bf phone**

how to spy on my **wifi network**

Searches related to how to spy on my husband

[track my husbands phone for free](#)

[track my husbands phone without him knowing](#)

[how can i find out who my husband is texting for free](#)

[cheaters spy app free](#)

[how can i track my husbands cell phone without him knowing and for free](#)

[how to hack my husbands whatsapp](#)

[how can i track my husbands phone location](#)

[spy on cell phone without touching target phone](#)

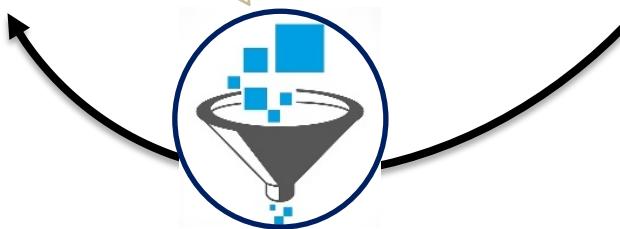
“Snowball” searching

how to spy on my girlfriend,
track my girlfriend android,
how to spy on my husband

...

Query set

Regex-based
filter to remove
unrelated terms



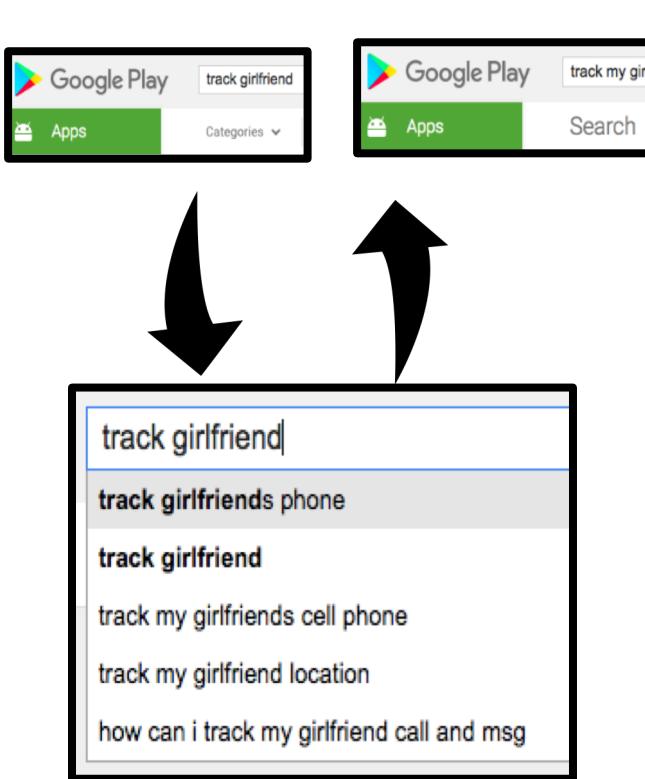
how to spy on my
how to spy on my **husband**
how to spy on my **boyfriends phone**
how to spy on my **boyfriends iphone**
how to spy on my **girlfriends iphone**
how to spy on my **husband iphone**
how to spy on my **boyfriends facebook messages**

Searches related to how to spy on my husband

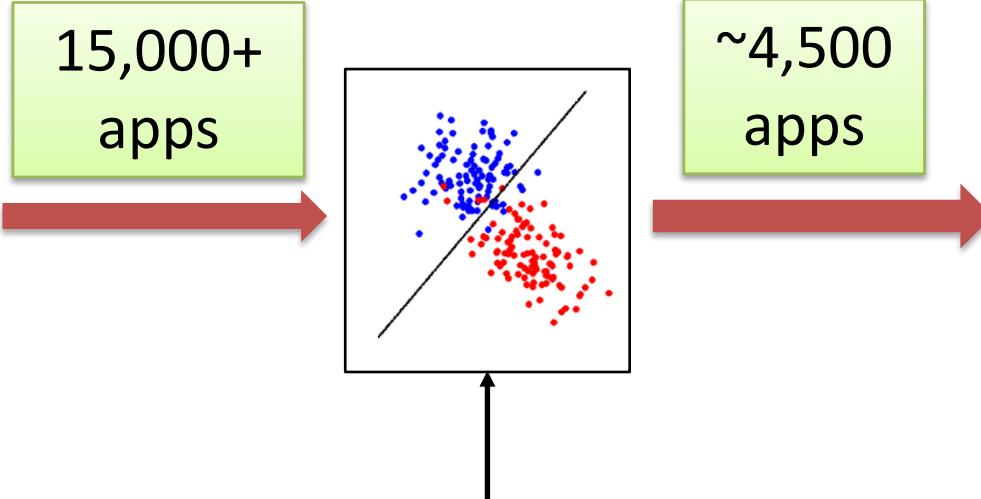
track my **husbands phone for free**
track my **husbands phone without him knowing**
how can i find out who my husband is texting for free
cheaters spy app free
how can i track my husbands cell phone without him know

Finding IPV-relevant apps in official app stores

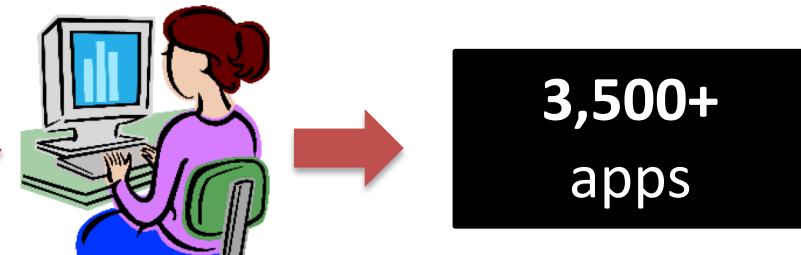
Snowball searching over
3 months on Play Store



Prune using
ML classifier



Filter using
human verifier



Looks at app title, description,
permissions, and genre as
reported in Play Store

Smaller study (2 weeks) on
iTunes App Store: 451

Taxonomy of on-store apps

Personal tracking

- Find my phone or Anti-theft
- Automatic call recorder
- Automatic data/SMS syncing
- Phone control
- Personal safety



Mutual tracking

- Find-my-family / friend
- Couple tracking



Subordinate tracking

- Employee tracking
- Parental control

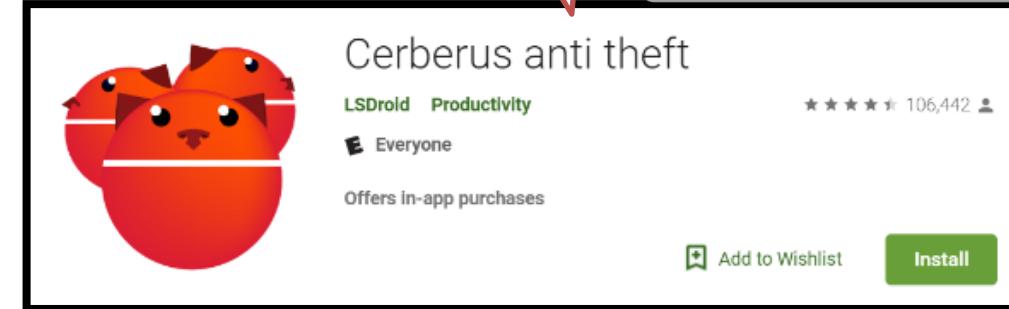


Seemingly innocuous apps used as spyware

*"I'm looking for an app I can install on my wife's phone that is **hidden** so that I can see **where she is or has been** via cell towers or gps."*

*[Install] **Cerberus** from the market. Once installed and configured, can be **set to be invisible in the app drawer**. You can also **record audio** and **take pictures remotely** with it! Be sure to **silence the camera first** though!"*

Dual-use app



Abundant resources for spying on victims

- Crawled **Google** and  (and **iTunes**) using snowball search
- We found:

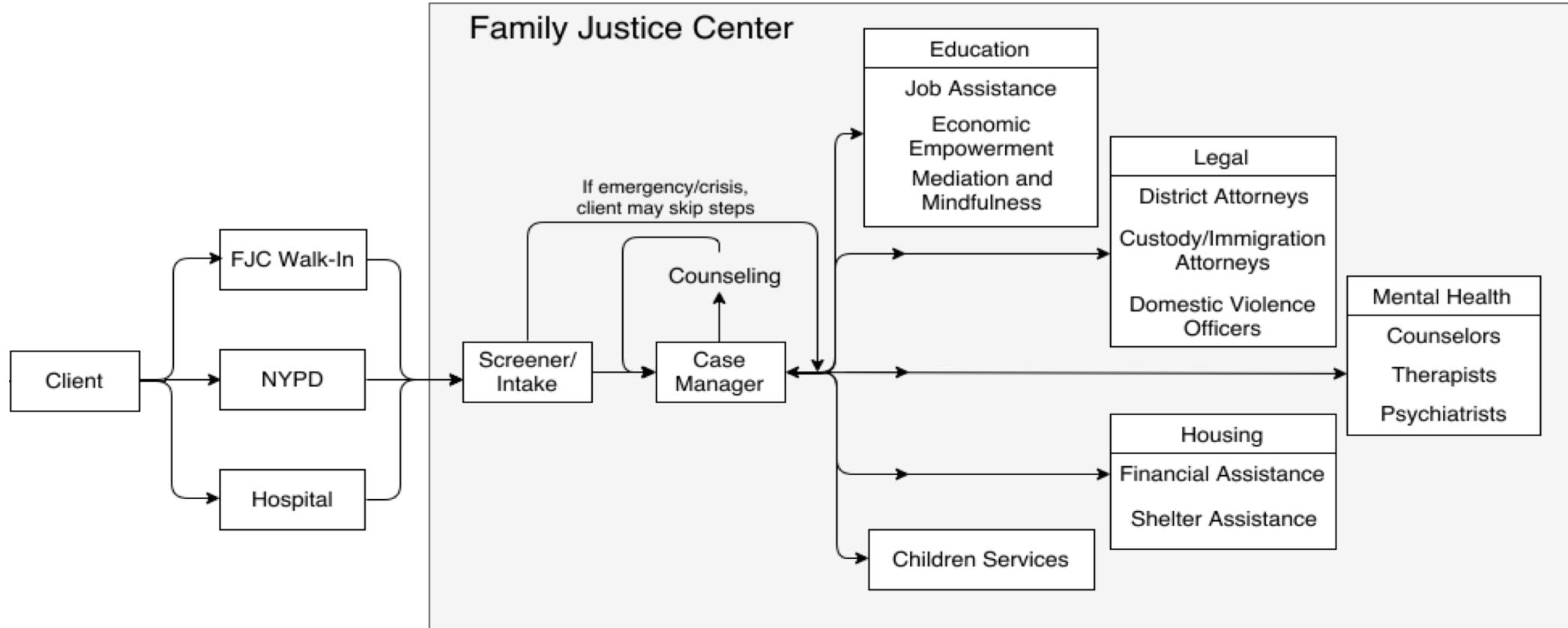
23 off-store apps
(most *overt spyware*)



3,500+ apps on 
451 apps on 
(most *dual-use apps*)



How are victims obtaining help?



Victims, professionals feel they lack needed technology expertise

Victims overwhelmingly report having insufficient technology understanding to deal with tech abuse

“[The victim is] absolutely not savvy on technology.”
– Case manager

Abusers usually considered to be “more tech-savvy” than victims

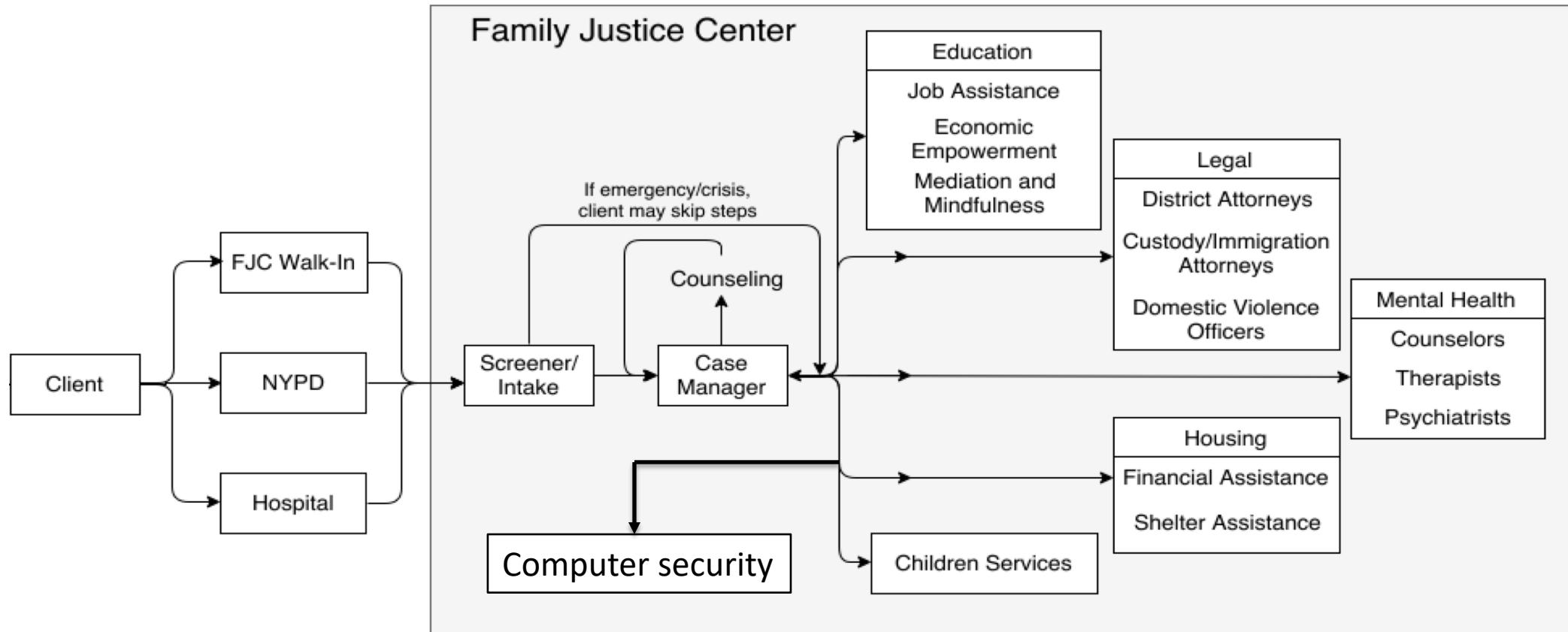
Professionals overwhelmingly report having insufficient technology understanding to help with tech abuse

“I end up Googling it. And then I’ll deal with [the client]. But I think... I don’t know how to do it so we’ll just Google it together.” – Case manager

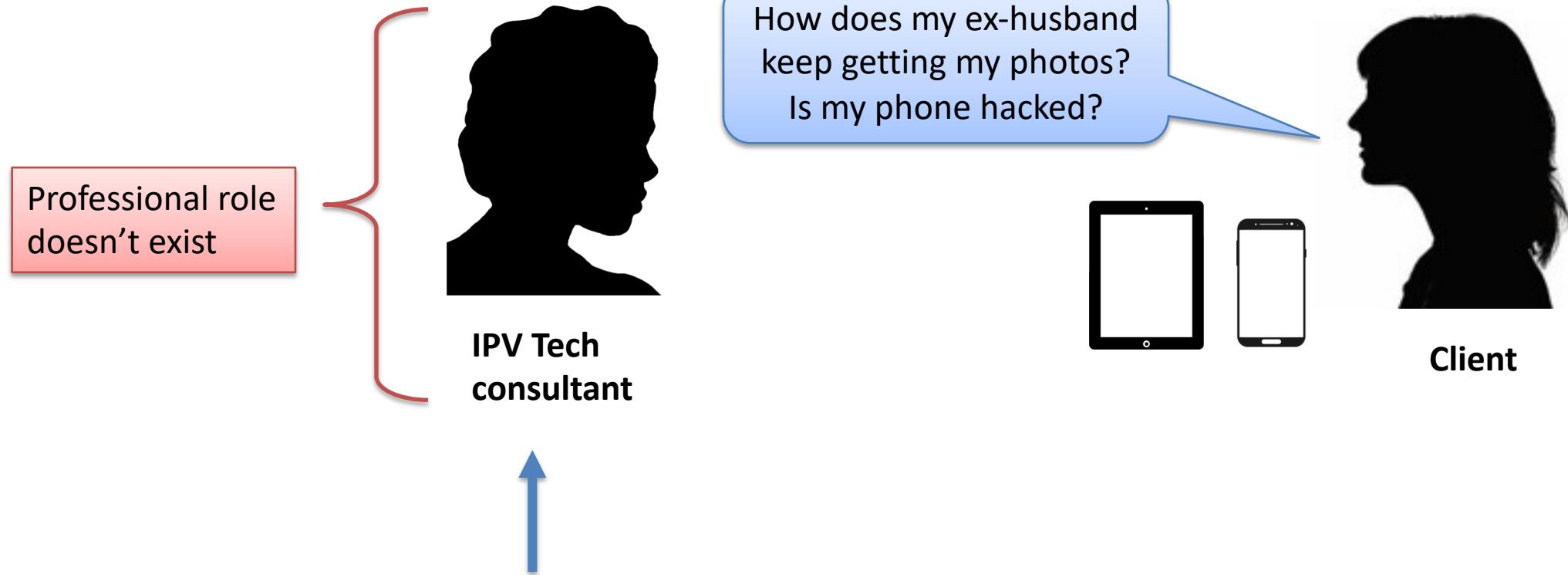


“Google-as-they-go”

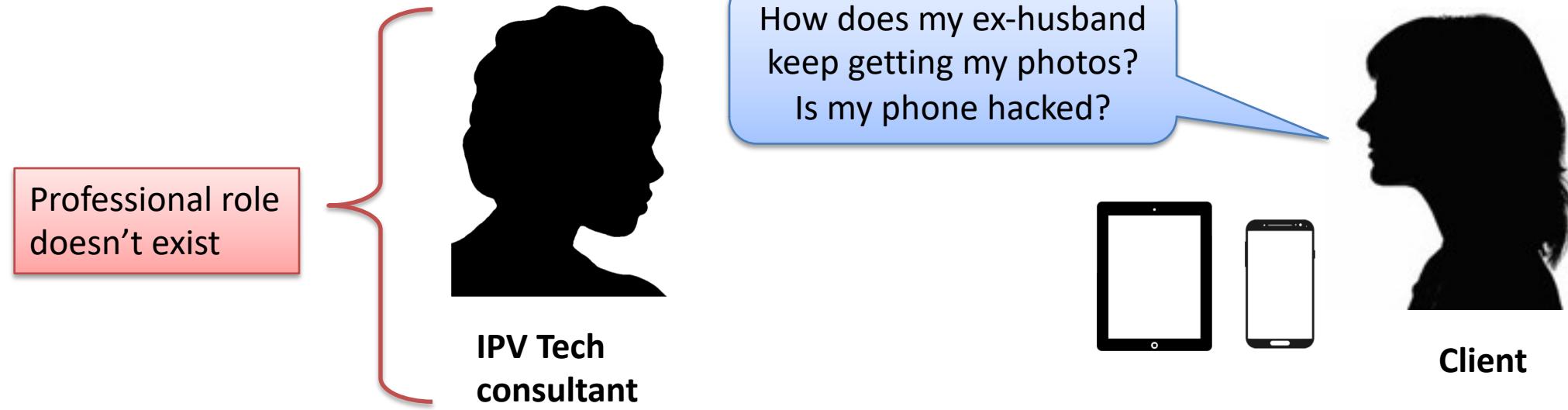
Our idea: clinical computer security



Our idea: clinical computer security



Our idea: clinical computer security



How to recruit, screen, & train volunteers?

How do we evaluate outcomes?

What type of clinical models do we want (referrals vs. walk-in)?

What legal protections are needed?

What tools are needed to perform investigations?

How should consultations work?

Prototyping clinical services in New York City at FJCs

Case manager,
lawyer, etc.



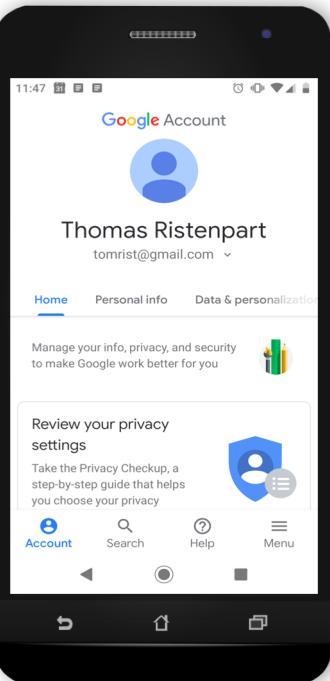
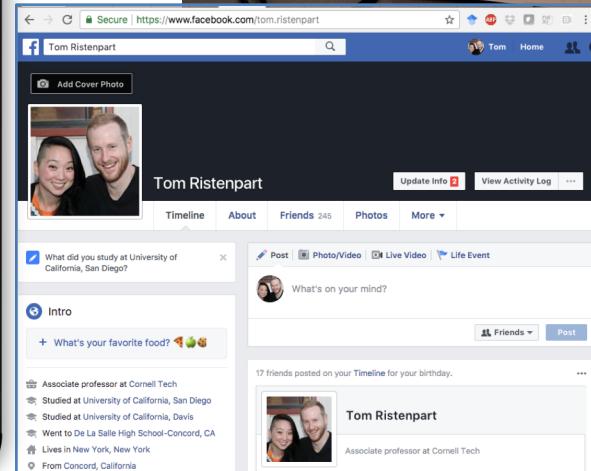
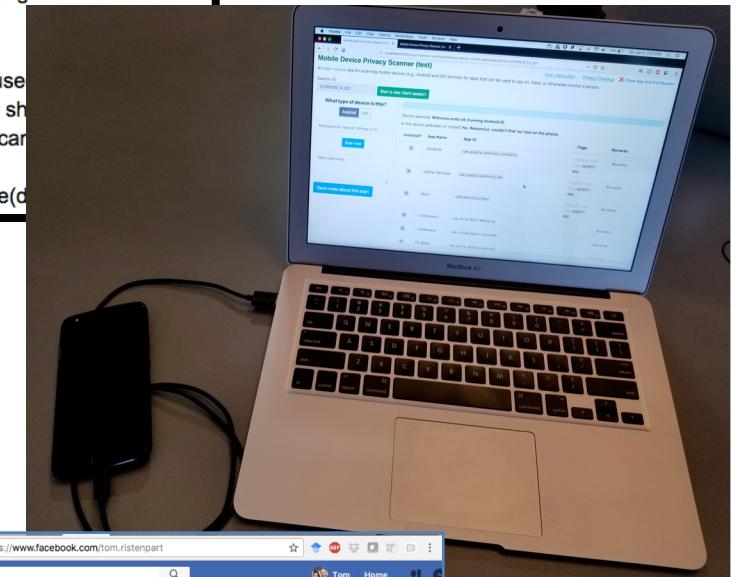
- Referral from FJC professional
 1. *Understand*
 2. *Investigate*
 3. *Advise*
- Safety-planning hand-offs

Case manager,
lawyer, etc.



Technology Assessment Questionnaire (TAQ10)
I am going to ask questions that might be helpful if you think your abuser your phone, or have access to information on your phone or other technol knowledge. This is technology abuse. Today we are going to be asking y this topic. Do you have any questions for me? Let's get started.

1. Do you worry that your device(s) is being used without your permission? (e.g., show up unexpectedly or know things they shouldn't know about you)
2. What devices do you use in your home or car? (e.g., smartphone, desktop, laptop, etc.)
3. Do you currently (or have in the past) share(d) your device with anyone else?



Field study in New York City

Summer, Fall 2018:

focus groups with dozens of professionals
protocol & instrument refinements
ENDGBV approval to meet with clients

Iterative design
with stakeholders

Nov 2018 – August 2019:

- 81 clients
- scanned 132 devices
- (potential) spyware apps or browser extensions on devices of 3 clients
- many account compromises
- reassured many clients about lack of tech problems

Clients and ENDGBV professionals
really positive about the approach

Clinic is ongoing

Dealing with abuse huge part of tech

- **Abuse vs. computer security**
 - Abuse: using system's functionality
 - Computer security: exploiting “unintended” functionality
 - Not a clear dividing line, and fascinating interplay
- **Real harms to people**
 - Commercial scamming, fiscal harm
 - Debilitating personal attacks
- **Need socio-technical approaches**
 - Ex: IPV safety review legal restitution, policy, clinical computer security,
...

