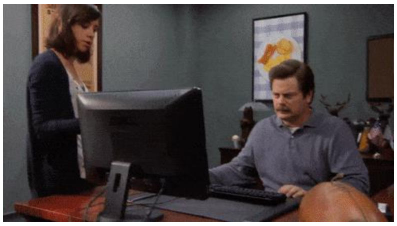
Navigating Safety:

The Use and Misuse of Technology and Intimate Partner Violence

1

Your Use of Tech?

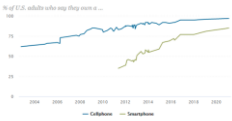


2

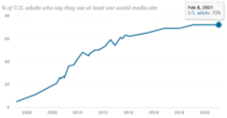
The Use and Misuse of Technology

3

Tech Use in the United States



Note: Respondents who did not give an answer are not shown.
Source: Surveys of U.S. adults conducted 2002-2021.
PEW RESEARCH CENTER



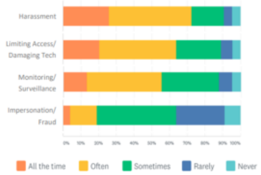
Note: Respondents who did not give an answer are not shown.
Source: Surveys of U.S. adults conducted 2005-2021.
PEW RESEARCH CENTER

Source: Pew Research Center's factsheets from 2021: Mobile and Social Media

4

Prevalence of Misuse

What kinds of tech misuse are survivors experiencing (not just during the pandemic?)

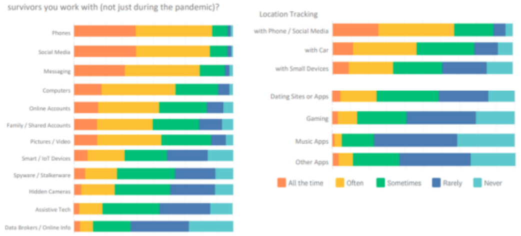


Source: *Tech Abuse in the Pandemic & Beyond: Reflections from the Field*, National Network to End Domestic Violence (2021).

5

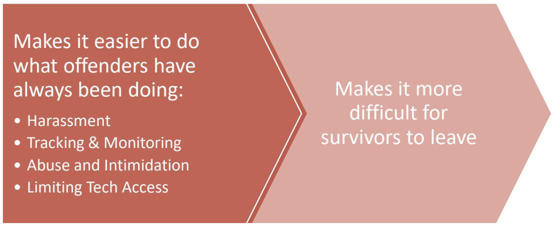
Prevalence Continued

How often are these kinds of technology misused against survivors you work with (not just during the pandemic)?



6

How Technology is Used: The Bad News



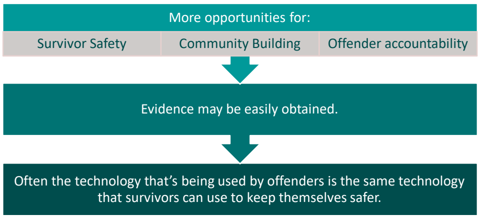
Makes it easier to do what offenders have always been doing:

- Harassment
- Tracking & Monitoring
- Abuse and Intimidation
- Limiting Tech Access

Makes it more difficult for survivors to leave

7

How Technology is Used: The Good News



More opportunities for:

Survivor Safety | Community Building | Offender accountability

Evidence may be easily obtained.

Often the technology that's being used by offenders is the same technology that survivors can use to keep themselves safer.

8

Keep in Mind…

Technology is generally a *neutral* tool used by perpetrators to abuse, stalk, harass etc.

Survivors have the right to technology and tech access and while used as described above it is also a powerful connector and safety tool as well.

9

Digital Hygiene:

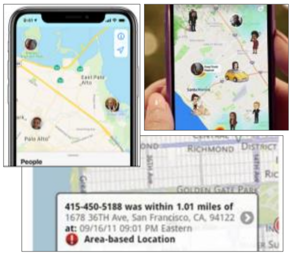
What Does it Mean to You??

10

Tech Use

11

GPS Technology and Cell Phone Locator Services



415-450-5188 was within 1.01 miles of
1678 36TH Ave, San Francisco, CA, 94122
at: 09/16/11 09:01 PM Eastern
Area-based Location

- Phones are equipped with GPS for use of e911.
- Often used for mapping/ driving & social connections
- Other forms of GPS include monitors for cars/parents.

12

OnStar's New Look
VOICE COMMAND BUTTON
Changed to speech icon to show expanded voice services
EMERGENCY BUTTON
Changed to SOS symbol to be globally recognizable

Other Locators

13

Geotagging

- Added geographical location or labels to photos, videos, websites, SMS messages, etc.
- Often, social media removes the location from the public when you post to their site, but not always.
- Texting and email will show your location.

14

Safety Tips: GPS

Avoid family plans, if possible.

Be careful with location-based social media apps.

Check location settings for ALL of the apps installed on your phone.

Log incidents to show a pattern of behavior.

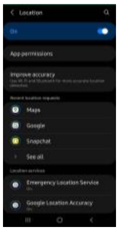
Ask questions to establish a timeline; When did the survivor notice that their abuser seemed to be everywhere?

Check your belongings and look through recent gifts given to the adult or child.

15

Safety Hands On:

Disabling Your Location



Location

On

App permissions

Improve accuracy

Recent location requests

Maps

Google

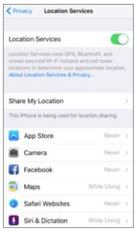
Snapchat

See all

Location services

Emergency Location Service

Google Location Accuracy



Privacy | Location Services

Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location. About Location Services & Privacy...

Share My Location

This iPhone is being used for location sharing.

App Store	Never
Camera	Never
Facebook	Never
Maps	While Using
Safari Websites	Never
Siri & Dictation	While Using

16

Safety Option: HB 1372

Provides an avenue for victims to separate their phone number and that of their children from a wireless telephone account as a component of their protective order.

17

Cell Phones and Tablets: Applications

Apps -

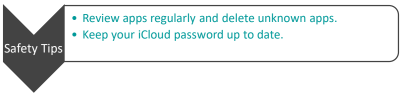
- Are everywhere; billions are downloaded every month
- Often ask for personal information like contacts
- Can be helpful; SAT prep etc.
- May have additional uses

Safety Tip: Review the permissions enabled for each App.

18

Stalkerware

- Apps that masquerade as something else, like a weather app, but have features used to stalk, spoof, or collect information etc.
- Some security apps can help identify stalkerware apps.
- Article: Google Removed 813 Creepware Apps from the Android Play Store



Safety Tips

- Review apps regularly and delete unknown apps.
- Keep your iCloud password up to date.

19

Safety Tips: The Internet of Things

The interconnection of everyday objects via the internet or Bluetooth.

Understand your device:

- Features, remote access, other security features
- What information does it store?
- Does it connect to Wi-Fi or Bluetooth? Can others connect?

Safety Tips:

- Turn off when not in use
- Change passwords and username
- Change authentication questions
- Keep a log of possible misuse

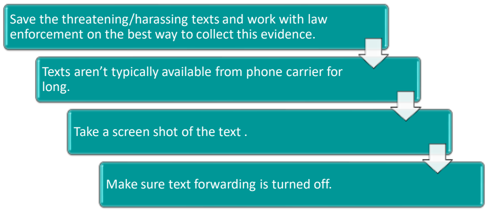
20

Safety Tips: Wi-Fi

- Has the abuser been connected to the home Wi-Fi or know the account information?
- Log in to your Wi-Fi account or a third- party app to help identify who is connected to your Wi-Fi.
- Be cautious connecting to public Wi-Fi.
- Review your phone and computer and remove Wi-Fi connection history.

21

Cell Phone Safety Tip: Texts


Save the threatening/harassing texts and work with law enforcement on the best way to collect this evidence.

Texts aren't typically available from phone carrier for long.

Take a screen shot of the text .

Make sure text forwarding is turned off.

22

Safety Hands On: Take a Screenshot

This Photo by Unknown Author is licensed under CC BY-NC

23

Cell Phone Safety Tips: Preserving Information

Four basic options for securing a phone's information:

1. Powering On / Off: data protection if off but may have to deal with lock codes.
2. Pulling the battery: data protection but may have to deal with lock codes and possible timestamp resets, which can result in challenges from defense. This can be the worse option.
3. Isolate the phone: data protected, but battery could die and then may deal with lock codes.
4. Airplane mode: isolation to protect data, but without concern for data compromise or battery depletion. This is the recommended strategy.

24

Social Media

25

Social Media: The Good News

Creating an online community for friends & family members or meeting new friends (e.g. Snapchat, Facebook)

Can bring people together in various ways:

- Message boards/pursuits of specific interests
- Online trading and commerce
- Community activism

26

JACKPOT.
endlessorigami.blogspot.com
CREEPY
SOCIALLY ACCEPTABLE

27

Common Social Media: Know the Basic Risks

Snapchat
- Images are easily/covertly saved.
- Location tracking.
- Some stories may be visible to strangers.

Instagram
- Easy to spy on someone.
- DM's used to intimidate.
- Risks with sharing personal videos/photos.

Twitter
- Sub-tweeting a form of cyberbullying.
- Misinformation may be everywhere.
- Difficult to remove content.

TikTok
- Can receive messages from anywhere.
- Easy to encounter adult content.
- Risks with sharing personal videos.
- High risk of cyberbullying

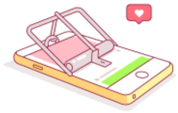
28

Offenders & Social Networking

- Friending family, friends, significant others
- Impersonation
- Sending Messages/ Threats
- Inquiring/Gathering Information
- Using children's sites to gather info

29

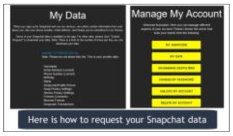
Safety Tips: Social Networking



- Know your privacy settings and use them; check them often as they can change
- Be aware that not everyone will use the same settings
- Tell your friends and family not to post pictures or information on you
- Use caution when adding friends/followers
- Discuss your boundaries with young people
- Caution with shared accounts and other remote access
- Disable "check in" features/other geolocation

30

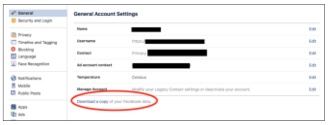
Social Networking Safety Tip: Download Your Data



My Data

Manage My Account

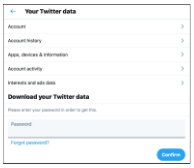
Here is how to request your Snapchat data



General Account Settings

Name	[redacted]	Edit
Username	https:// [redacted]	Edit
Contact	Primary: [redacted]	Edit
Ad account contact	[redacted]	Edit
Temperature	Celsius	Edit
Manage Account	Modify your Legacy Contact settings or deactivate your account.	Edit

Download a copy of your Facebook data.



Your Twitter data

Account

Account history

Apps, devices & information

Account activity

Interests and ads data

Download your Twitter data

Please enter your password in order to get this.

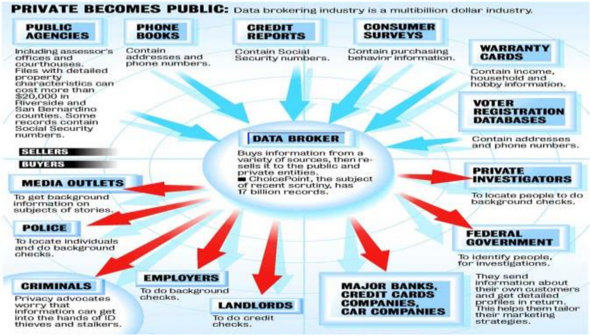
Password

Forgot password?

31

The Internet

32



PRIVATE BECOMES PUBLIC: Data brokering industry is a multibillion dollar industry.

PUBLIC AGENCIES
Including assessor's offices and courthouses. Files with detailed property characteristics can cost more than $20,000 in Riverside and San Bernardino counties. Some records contain Social Security numbers.

PHONE BOOKS
Contain addresses and phone numbers.

CREDIT REPORTS
Contain Social Security numbers.

CONSUMER SURVEYS
Contain purchasing behavior information.

WARRANTY CARDS
Contain income, household and hobby information.

VOTER REGISTRATION DATABASES
Contain addresses and phone numbers.

SELLERS

BUYERS

DATA BROKER
Buys information from a variety of sources, then re-sells it to the public and private entities.
■ ChoicePoint, the subject of recent scrutiny, has 17 billion records.

MEDIA OUTLETS
To get background information on subjects of stories.

POLICE
To locate individuals and do background checks.

CRIMINALS
Privacy advocates worry that information can get into the hands of ID thieves and stalkers.

EMPLOYERS
To do background checks.

LANDLORDS
To do credit checks.

MAJOR BANKS, CREDIT CARDS COMPANIES, CAR COMPANIES
They send information about their own customers and get detailed profiles in return. This helps them tailor their marketing strategies.

PRIVATE INVESTIGATORS
To locate people to do background checks.

FEDERAL GOVERNMENT
To identify people, for investigations.

33

Safety Tips: Digital Hygiene and the Internet

Internet Browsers

- Use a private browser.
- Add "s" before the website name.
- Delete cookies and internet history frequently.

Data/Reputation Management

- Remove personally identifying information from the internet
- Opt-out options-
  - Reputation management companies
  - Data broker websites
    - Safe Sheperd
    - World Privacy Forum Top Ten Opt-Outs

34

Safety Planning Tools for Survivors

35

Safety Planning: The Internet and Email

- Use a computer the abuser never had direct access to; like at a public library or college.
- Have anti-virus software and use it to scan your computer.
- Talk to friends/family about your privacy.
- Have more than one e-mail account, including one that is not identifiable.
- Be cautious of using the internet to purchase items or to join websites that require identifying information.
- Know the privacy polices of websites.
- If your abuser has access to the same computer be aware of deleting internet history; there are pros and cons.
- Do not open suspicious e-mails/attachments.

36

Fundamental Digital Hygiene

A username and password alone are no longer secure

- Use fake answers on your security questions.
  - Don't answer surveys that give away your security question answers.
- Use hard to crack passwords.
- Use different usernames and passwords.
  - Use a password manager.
  - Implement two-factor authentication.
  - Use an authentication app.
  - Updates apps and your cell phone system often- these patches are pushed out to deal with security risks!

37

Supportive Documentation

- Keep a log
- Save, save, save BUT only what you need to…
- Abuser's use of tech?
- Pictures

SAFETY FIRST

38

Safety Planning for Working Relationships

Safety plan with the survivor immediately.

Do not remove their technology.

Assess both the use of technology by the survivor as well as the offender.

Develop a relationship with your local law enforcement and know their preferred method of evidence collection.

Work with your local family violence program on safety planning.

Don't contribute to the problem by allowing private data to be shared or compromised.

39

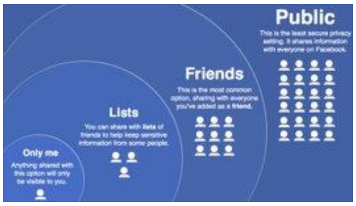
Top 5 Countdown!

40

5

41

Privacy Settings



Public

This is the least secure privacy setting. It shares information with everyone on Facebook.

Friends

This is the most common option, sharing with everyone you've added as a friend.

Lists

You can share with lists of friends to help keep sensitive information from some people.

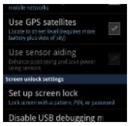
Only me

Anything shared with this option will only be visible to you.

4

42

3



mobile networks

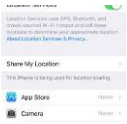
Use GPS satellites
Locate to street-level (requires more battery plus view of sky)

Use sensor aiding
Enhance positioning and save power using sensors

Screen unlock settings

Set up screen lock
Lock screen with a pattern, PIN, or password

Disable USB debugging m



Location Services

Location Services uses GPS, Bluetooth, and crowd-sourced Wi-Fi hotspot and cell tower locations to determine your approximate location.
About Location Services & Privacy...

Share My Location

This iPhone is being used for location sharing.

App Store	Never
Camera	Never

Check your GPS

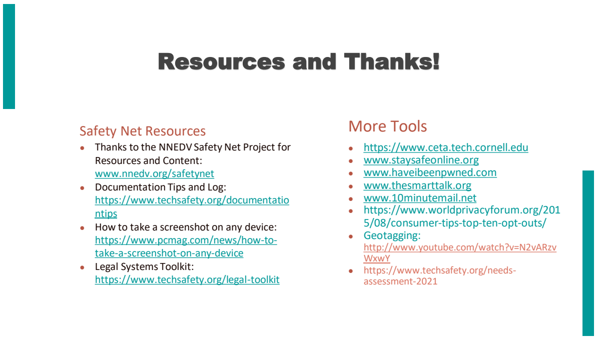
43

2

44

Trust Survivor's Instincts

45



Resources and Thanks!

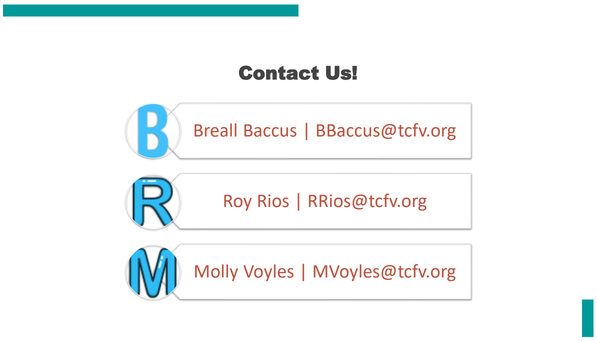
Safety Net Resources

- Thanks to the NNEDV Safety Net Project for Resources and Content: www.nnedv.org/safetynet
- Documentation Tips and Log: https://www.techsafety.org/documentationtips
- How to take a screenshot on any device: https://www.pcmag.com/news/how-to-take-a-screenshot-on-any-device
- Legal Systems Toolkit: https://www.techsafety.org/legal-toolkit

More Tools

- https://www.ceta.tech.cornell.edu
- www.staysafeonline.org
- www.haveibeenpwned.com
- www.thesmarttalk.org
- www.10minutemail.net
- https://www.worldprivacyforum.org/2015/08/consumer-tips-top-ten-opt-outs/
- Geotagging: http://www.youtube.com/watch?v=N2vARzvWxwY
- https://www.techsafety.org/needs-assessment-2021

46



Contact Us!

Breall Baccus | BBaccus@tcfv.org

Roy Rios | RRios@tcfv.org

Molly Voyles | MVoyles@tcfv.org

47