Protecting Your Kink Identity
Part 2

Dating Kinky
June 2020

Vir Cotto

Second Part of Three Part Series

- Session 1
- Understanding and Managing Risk
  - How to handle risks without getting overwhelmed or overworked
- Session 2
  - **Understanding and mitigating being tracked both online and offline**
  - **Evaluating information tracking and incorporating it into our risk planning**
- Session 3
  - How to help others and keep us all safe collectively
  - How to be a responsible event organizer and promoter with privacy in mind

(Re) Introductions

Vir Cotto

he/him pronouns

Lifestyle Kinkster

Dominant/Sadist

https://vircotto.com

vir@vircotto.com

@VirCotto on Fetlife

Quick Review

- We have positive actors, neutral actors and negative actors
- We have threats with varying severity and probability
- Different threats have different levels of effort to either prevent or remedy
- We generally want to address threats that are severe, likely and easy to prevent

What we will cover

- We will be focusing on privacy
- We will be focusing on practical steps
- We will provide frameworks for evaluating products/services in the future

- There’s going to be a lot in here..
  - We practiced for this last time… take small steps and iterate!
  - Take from them what you can… Even I don’t follow all these tips!

Your Privacy is Under Attack

- Companies make money based on tracking your activities, online and offline
- Companies sell your activity to each other to provide a “more complete picture” of who you are
- Governments are passing increasingly invasive laws allowing for and encouraging tracking of citizens
- Governments buy your data from these companies

Fighting Deterministic Pessimism

- We acknowledge that we can’t fight off all threats to our privacy
- We can take reasonable steps to obscure our identity
- We can take reasonable steps to fend off passive or mass data collection
- We can accept that this won’t protect us against some determined threats

The Four Ways Information About You is Discovered

- You tell them
- They observe it
- They infer it
- Someone else tells them

Common ways you disclose secrets

- Give it away
- Using our wallet name when signing up/registering
- Using the same communication system for kink and non-kink
  - Email, phone, social media
- Leaving something around with our name on it

Who sees your information to in a common online purchase

- Your ISP/Mobile Provider
- Browser/Plugins that May Track You
- Advertisers
- The vendor
- Your bank and payment processor
- Your email provider (when they send you a receipt)
- The shipping company

Attending an in-person you signed up for online

- Your ISP, Browser, Plugins
- The website with the event
- Advertisers on that event
- Payment processor (if applicable)
- Email provider
- Location tracking apps (Google, etc.)

Metadata and Inferences

- Metadata is information about the information
- The more metadata one has, the more identifiable it becomes
- “We kill people based on metadata”

Inferences

- Inferences are information that can be gleaned from other information
- Can be used to de-anonymize data
- Is used to determine information about you when advertising at you, etc.

Our Strategy

- We (still) want to do things online
- We can’t be entirely private, so let’s be selective
  - Be selective about the information we disclose
  - Separate our activity to the same party
  - Try to prevent inferences through leaking metadata
  - Create an isolated “identity” around our kink persona

Browser Choice and Browser Security

- Google has been leveraging Chrome against privacy
- Run Firefox!
- Disable “Helpful Plugins” (Honey, etc.)
- Chromium as a Last Resort chromium.woolyss.com

Incognito/Private Mode Browsing

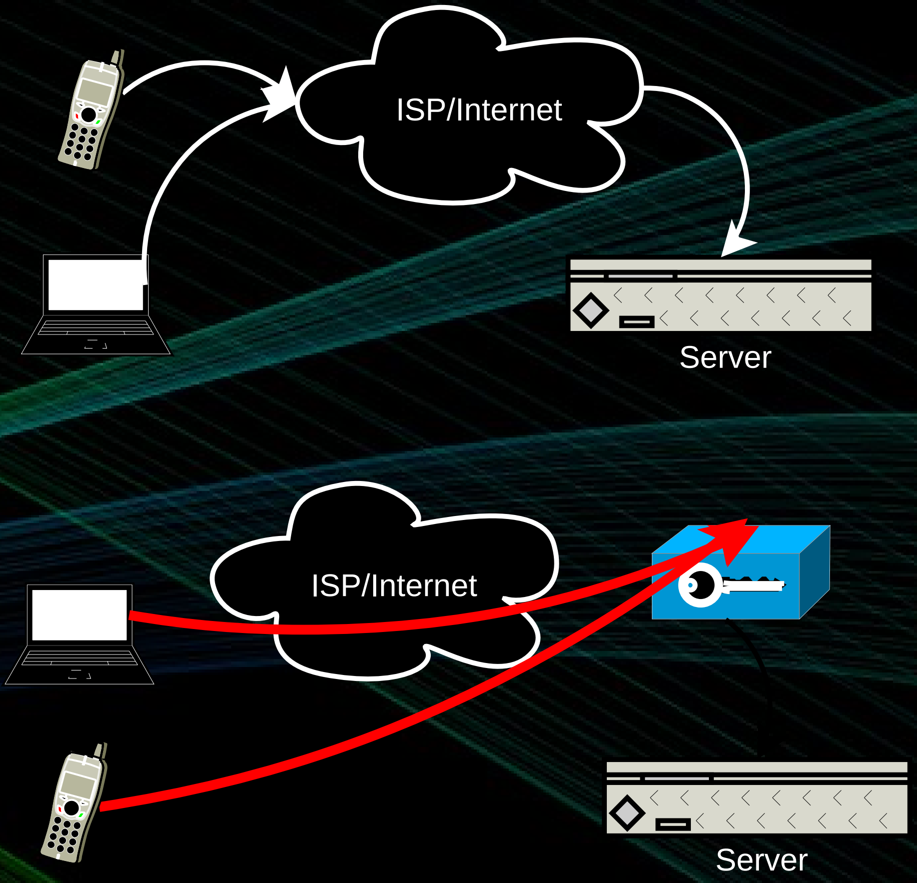
- Incognito or “Private Mode” do not protect your identity online
  - They log you out of your existing sessions
  - They don’t write your browsing history to the hard drive
- Logging into a website instantly wipes away most of the benefits!
- There are ways to protect your identity online, but Incognito Mode only protects you from a snooping roommate

Our ISP/Mobile Provider

- How does our ISP learn about us?
  - Directly looking at traffic (if unencrypted)
  - DNS lookups
  - User/device tagging
  - Geolocation

VPN

- A VPN encrypts the traffic to the ISP first
- Your ISP will only know you’re using a VPN
- The website will only know you came from the VPN
- *VPNs don’t protect your privacy in any other way!*
- ***Can you trust your VPN provider?***



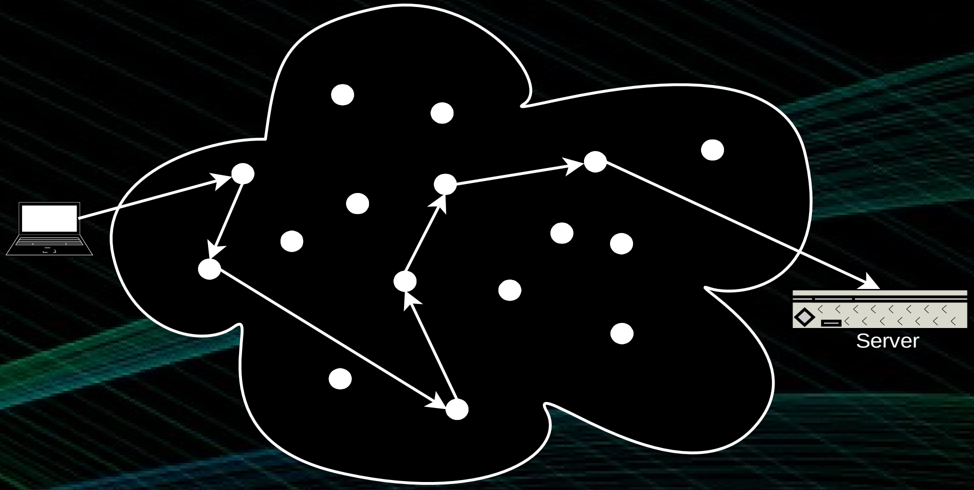
Choosing a VPN Provider

- Do they have a good privacy policy? A good logging policy?
- Are they associated with an advertising/social media company?
- Will they allow you to pay them without a credit card?
- Are they free? Stay away!

- ProtonVPN
- NordVPN
- ExpressVPN
- Surfshark

Tor

- Onion routing
- Only be effective if you aren’t logged into other services and block ads
- Tor will be slower
- Tor will use your bandwidth for others (but not to the Internet)
- Tor Onion Services



Other Onion Routing Protocols

- I2P
- ZeroNet
- Loki
- GNUNet
- Freenet

A Quick Aside on Encryption

- At Rest
- Transport
- End to End (E2E)

Information Brokers

- Advertisers or Social Media companies
- Techniques they use
  - Buying our information from other brokers
  - Collecting information directly from us (our name, viewing history, Likes, etc.)
  - Tracking us across websites
  - Tracking our phone activity

Do Not Link Accounts

- Don’t “Sign in with ___”
- Use different email addresses when signing up for a kink service (or use disposable addresses)
- Be sure to be logged out from other accounts (use Firefox Multi-Account to help)

Disabling Advertising Trackers/Browser Fingerprinting

- Use Firefox, Firefox on Android
  - Firefox for iOS*
- Use the EFF’s Privacy Badger
- Use uBlock Origin
- Use Firefox Multi-Account Containers
  - Cookie AutoDelete
- Bloody Vikings!

Disable Location Tracking

- Many apps put on location tracking when they don’t need to
- Turn off location tracking generally or per-application in either iPhone or Android
- Use web application versions of services where you can more easily control what they do
- Always check and then manually configure application settings

Banks and Payment Processors

- Banks and Payment Processors Collect and Sell your Personal Data
- Buy things with cash if possible
- Use Pre-paid credit cards
- Privacy.com (maybe?)

Cryptocurrency

- Cryptocurrency is semi-anonymous
- You don’t need an online wallet, but if you do use one, be aware that your information is trackable
- Cryptocurrency is highly volatile
- You need to keep your wallet information (millions of dollars have been lost this way!)
- The decision to use cryptocurrency is a personal one

Email

- Email communications are in plain text (not encrypted)
- Free email providers advertise and scan email contents
- You want a different email for your kink activity

- Self-Hosting/Community Hosting
- Throw-away email providers
- Protonmail
- Countermail
- Tutanota

Search and Social Media

- Migrate away from Google
  - DuckDuckGo for search
  - Paid email provider
  - Paid phone provider
- The money you are paying is what Google would be making off your private data

- Move away from (or leave) Facebook
- Consider alternatives such as Mastodon
  - the-federation.info
  - joinmastodon.org

Shipping Provider

- Shipping Companies will know the vendor and your address
- If your address is your personal address, they can know a lot about you
- Alternatives:
  - Use a PO Box or Mailbox

Phone Numbers

- Phone numbers allow someone to contact you
- Reverse lookups
- Can be used as de-facto identifiers
- Getting a second line is a good idea

- Phoner
- Burner
- Hushed
- Google Voice (?)

Messaging

- Many of us use messaging systems to communicate
- Phone and other messaging providers store your messages forever
- Secure messaging apps provide an alternative

- Signal
- Riot (Matrix)
- Briar
- DeltaChat
- XMPP/Jabber with OMEMO (Conversations.im)
- Use your 2nd phone line’s SMS

Collaboration/Teleconferencing

- Use Matrix (Riot.im) or Rocket.Chat instead of Discord or Slack
- Use Nextcloud instead of Google Suite, Dropbox, or MS Teamwork
- Use Nextcloud Talk or Jitsi instead of Zoom

Don’t Use Spy Devices

- Amazon Alexa
- Siri
- Google Home
- Fitbit
- Smart TVs
  - Samsung
  - LG
  - Vizio

- These devices are primarily designed to collect information about you, and also perform other tasks
- Don’t buy or use them
- Try Mycroft.ai if you’re adventurous
- Check out GadgetBridge for libraries for your existing health trackers
- Guides online for disabling Smart TV tracking
  - Though it was shown some TVs still collected and sent the data!

Teledilconics Alternatives

- Many remote vibrators collect your private information!
- We-Vibe was forced to pay $4m Canadian for privacy violations regarding customer data after it was shown how easy it was to collect and control the device remotely

- Buttplug.io is a software library designed for many existing vibrators
- The US patent on teledildiconics expired in 2018, so we should see new open source devices soon!

Run Open Source Software

- Open Source means anyone can read the code, audit it, fix bugs
- Tend to be less buggy, more secure
- Tends not to have privacy issues

- F-Droid for Android
- AlternativeTo
- OStatic.com
- Run a Linux Desktop

How to Evaluate a New Service/App

- What does it do?
- What information does it collect?
- Does it link with other accounts?
- How does it make money?
- What is the privacy policy?
  - tosdr.org or the tosdr browser plugin!
- Can I opt out?
- Does it support End to End Encryption
- Is it Open Source?

Challenges in Protecting Our Privacy Online

- Protecting our privacy requires more work
- Protecting our privacy requires more money
- Protecting our privacy requires consistency
- Active thwarting by commercial interests

Resources to Learn More

- EFF’s Surveillance Self-Defense Guides at ssd.eff.org
- Umbrella Security for Android and iPhone
- Holistic Security Manual
    - holistic-security.tacticaltech.org

Thank you!

Preview of the Next Session

- Review or questions from last two sessions
- Some steps to take if you’ve been outed
- How to be a good ally to other kinksters
- How to be a good organizer and community leader from a privacy perspective
- How widespread video chat has change kink culture

Questions!

- Thank you to all in attendance or viewing!
- Special Thanks to Nookie Notes and Dating Kinky!

- Question time is now and feel free to reach out in the future!

- **Vir Cotto**
- VirCotto on FetLife
- vir@vircotto.com
- vircotto.com