Working with Law Enforcement

CS 152 — Trust and Safety

Alex Stamos

Stanford Cyber Policy Center

May 19, 2026

Content Warning:

This lecture will contain frank discussion of criminal activity that many people may find challenging or upsetting. We will also mention cases that led to victim suicide. **We will not show images of this activity during the lecture**. Our learning objective is to understand how platforms are misused to commit offences and the responses of individuals, law enforcement agencies, governments, and the platforms themselves to minimize offense and victimization.

What Will We Discuss Today?

What Will We Discuss Today?

- A quick review of some of the key laws that govern the relationship between tech companies and law enforcement.
- A review of two major OCSE cases I participated in::
  - An international child sex trafficking ring
  - An advanced, individual sextortionist
- What these cases teach us about the relationship between technology and law enforcement:
  - The normal flow between law enforcement and tech companies
  - How that breaks down in real life
  - The risks and pitfalls of working with law enforcement

The Most Relevant Laws

Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

Pre-ECPA Supreme Court cases

Supreme Court: 4A protects conversations from warrantless surveillance.

- **In-person conversations:** Berger v. New York, 388 U.S. 41 (1967): Held unconstitutional a New York state statute that authorized judges to issue warrants allowing police officers to trespass on private premises to install listening devices; didn't meet 4A's "probable cause" or "particularity" requirements
- **Phone calls:** Katz v. United States, 389 U.S. 347 (1967): Officers affixed a listening device to the outside of a phone booth Katz regularly used; Court held warrantless eavesdropping unconstitutional: 4A protects people, not just places, against unreasonable search & seizure
- Concurring opinion: "reasonable expectation of privacy" test – still the touchstone for courts' 4A analysis today

But it’s the 2020s, not the ’60s & ’70s.

We do most of our communicating online. Does the 4th Amendment protect email and other online communications?

Congress's response

- In 1968, after Berger and Katz, Congress passed original federal Wiretap Act
  - Enacted as Title III of the Omnibus Crime Control and Safe Streets Act of 1968
- In 1986, Congress passed ECPA
  - Amended the Wiretap Act (now Title I of ECPA), 18 U.S.C. S 2510 et seq. – extended it to include transmissions of electronic data via computers.
  - Added the Stored Communications Act (Title II of ECPA), 18 U.S.C. S 2701 et seq. – applies to stored electronic communications.
  - Added the Pen Register Statute (Title III of ECPA), 18 U.S.C. S 3121 et seq. – applies to transactional info about wire & electronic communications
- Remember: 4A is a **floor**; Congress (and the states) can and do pass laws that provide **more** protection than the courts say the 4A provides, e.g. ECPA (and California's CalECPA)

ECPA Definitions: 18 U.S.C. S 2510

Contents = "substance, purport, or meaning" of the communication

- What the communication means, conveys, says
- Example: subject line + body of an e-mail (or contents of a snail-mail letter)

Non-content information = information about the communication

- Metadata
- Think: header of an e-mail (or the outside of the envelope the letter is sealed in)

Content/non-content distinction becomes really blurry in the context of the internet

- Internet's complex architecture means one particular unit of data might change status (from content to non-content, or vice versa) as it travels from sender to recipient
- Content or non-content status might also depend on where in the network that unit of data resides at that particular moment in time
- We no longer live in the world of Katz and Smith – hence calls for reforming ECPA

ECPA Definitions: 18 U.S.C. S 2510

2510(8): “contents”, when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication; 2510(12): “electronic communication” means any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce, but does not include:

- (A) any wire or oral communication;
- (B) any communication made through a tone-only paging device;
- (C) any communication from a tracking device (as defined in section 3117 of this title); or
- (D) electronic funds transfer information stored by a financial institution in a communications system used for the electronic storage and transfer of funds;

Wiretap Act, 18 U.S.C. S 2510 et seq.

- Prohibits interception of contents of wire, oral, electronic communications (whether by government or private actor) except as authorized
  - For example, S 2511(2)(c)&(d): interception not unlawful if you're "a party to the communication" or "one of the parties to the communication has given prior consent to such interception" (except if you're doing the interception to do crimes, S 2511(d))
  - Wiretap Act = one-party, California = all-party
  - Even if an interception isn't a federal violation, it may still violate state law!
  - This is why customer support calls (& Zoom) tell you a call is/may be recorded
- Wiretap orders to law enforcement aka "superwarrants" or "Title III orders"
- Limited suppression remedy if evidence is gathered in violation of the law

Pen Register Statute, 18 U.S.C. S 3121 et seq.

- Prohibits the interception of the non-content parts of electronic communications except as authorized
- Lower standard than search warrant (probable cause) or wiretap order:
  - Govt's application must certify that the info "likely to be obtained" through the pen/trap is "relevant to an ongoing criminal investigation being conducted by that agency"
  - Court must issue the order if it finds the govt has certified to the court that the info likely to be obtained is "relevant to an ongoing criminal investigation"
- Regulates real-time collection of communications' non-content info
  - Dialing, Routing, Addressing, and Signaling (D/R/A/S) information
  - E.g., incoming & outgoing phone numbers, email to/from addresses, IP addresses, URLs
  - 3121(c) says govt is supposed to use tech to restrict collection to DRAS & not contents
  - Remember, to collect contents requires a Title III wiretap order

non-content	content

Stored Communications Act, 18 U.S.C. S 2701 et seq.

- Regulates access to, and disclosure (both voluntary and compelled) of, stored communications, records, and subscriber info held by third-party service providers (ISPs, social media, email, cloud, etc.)
- "Electronic comms service" vs. "remote computing service" providers
  - ECS: "any service which provides to users thereof the ability to send or receive wire or electronic communications," 18 U.S.C. S 2510(15)
  - RCS: "the provision to the public of computer storage or processing services by means of an electronic communications system," 18 U.S.C. S 2711(2)
  - Different rules apply depending on whether ECS or RCS
  - Written before modern Internet, webmail, cloud, etc. – courts now recognize that nowadays, most modern tech providers act as both

Stored Communications Act, 18 U.S.C. S 2701 et seq.

- 2701: prohibits unlawful access to stored communications
  - We'll see "access without authorization" language again in Computer Fraud and Abuse Act
  - 2701 applies only to ECS, not RCS
- 2702 & 2703: govern disclosure by ECS & RCS providers
  - Contents of comms "in electronic storage" vs. non-content customer records
  - Voluntary disclosure (S 2702) vs. compelled disclosure (S 2703)
- Warrant vs. administrative subpoena vs. 2703(d) order
- 180-day distinction for disclosing contents of stored electronic comms?
  - Statute says that a warrant is required if contents have been in storage for 180 days or less, but only a subpoena/court order (less stringent than a warrant) is needed if > 180 days
  - In practice, feds get a warrant ever since U.S. v. Warshak, 631 F.3d 266 (6th Cir. 2010)
  - Email Privacy Act: bill that would, if passed, amend SCA and codify Warshak as federal law
- No technical-assistance provision, unlike Wiretap Act & Pen Register Act

Stored Communications Act: Who Can Get What, How

	Governmental entity (e.g. fed/state prosecutor)	**Non-governmental entity** (e.g. civil litigant, criminal defendant)
Basic Subscriber Information	Federal, state, or local administrative, grand jury, or trial subpoena; Court order under SCA section 2703(d); Federal or state search warrant	Federal or state court civil or criminal defense subpoena or court order
Other non-content records or information	Court order under SCA section 2703(d); Federal or state search warrant	(Foreign government requests require domesticated order)
Contents of communications	Federal or state search warrant	No means to compel; must seek it from the user (but case law saying that a subpoena + consent can

Provider can be sued if it violates the rules for disclosing information (but provider may raise “good-faith reliance” defense)

Cross-Border Demands by Law Enforcement for User Data

- Issue with the SCA, internationally:
  - MLAT: foreign investigators' requests for evidence held by American service providers go through DOJ, which files the request in federal district court
  - Slow processing times
  - Probable cause standard
- Solution: CLOUD Act (2018)
  - "Clarifying Lawful Overseas Use of Data" - because Congress loves backronyms
  - CLOUD amends Wiretap & Pen Register Acts as well as the SCA
  - Once a country signs an agreement with the US government, its law enforcement can serve legal demands directly on US-based service providers instead of going thru DOJ
  - Country is only eligible if it sufficiently respects human rights (privacy, free expression, etc.). Eligibility is reviewed every 5 years once an agreement is in place.
  - Who's got an agreement with US so far? Only the UK (as of 2019); Australia probably soon

Word of the Day

fox

Busting a Major Sex Trafficking Ring

Verizon Media Threat Investigations

- Teams of investigators, engineers, analysts in the VZM infosec team (Paranoids)
- E-Crimes Team: Criminal attackers
  - CSAI, ATO, BEC, click fraud, tech support fraud, etc
- Advanced Threats Team: Nation-state attackers
- Insider Threat: Internal concerns

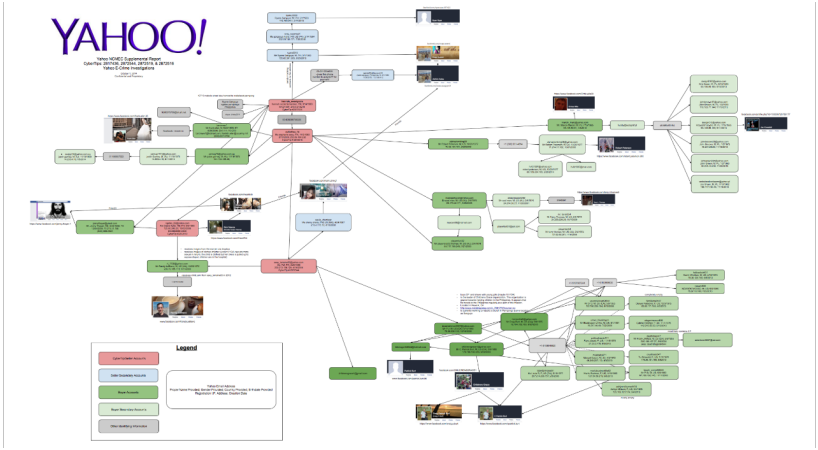
Yahoo: Fighting Child Sexual Abuse Imagery

- VZM operates many services where user-generated content can be uploaded or exchanged
  - Flickr
  - Tumblr
  - Yahoo Messenger
  - Yahoo / AOL Mail
  - Yahoo Groups
- Multi-tiered approach to fighting CSAI
  - Industry cooperation / abuse reporting
  - Detection at scale: PhotoDNA and machine learning signals
  - Manual review and investigation - “old fashioned detective work”

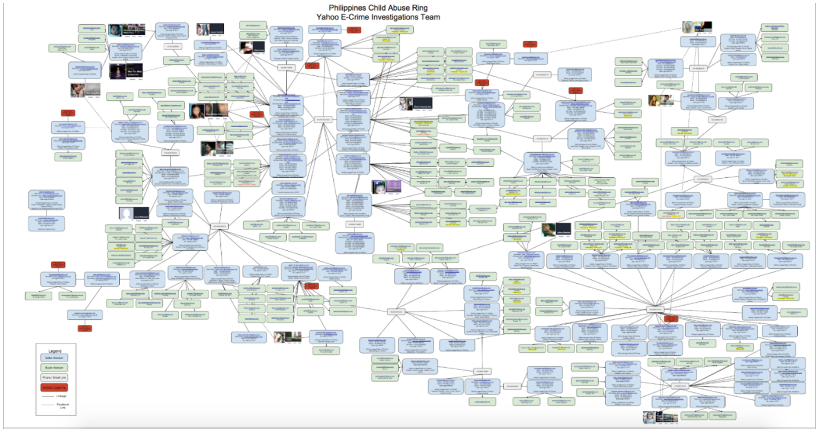
Case Study: Philippines Sex Tourism Investigation

- In 2014, Yahoo E-Crimes received information from our industry partner Xoom
  - Xoom had identified numerous Yahoo accounts in the Philippines that were receiving small amounts of money in regular intervals, consistent with webcam payment activity
  - Xoom used open-source tools to examine the profile pictures of the senders and observed probable CSAI
- E-Crimes launched a major investigation and initially identified two distinct rings of child pornography sellers in the Philippines and buyers worldwide
  - Streaming child abuse over webcam
  - Sending child abuse imagery over email
  - Arranging in-person abuse in the Philippines

Case 1: Small Ring



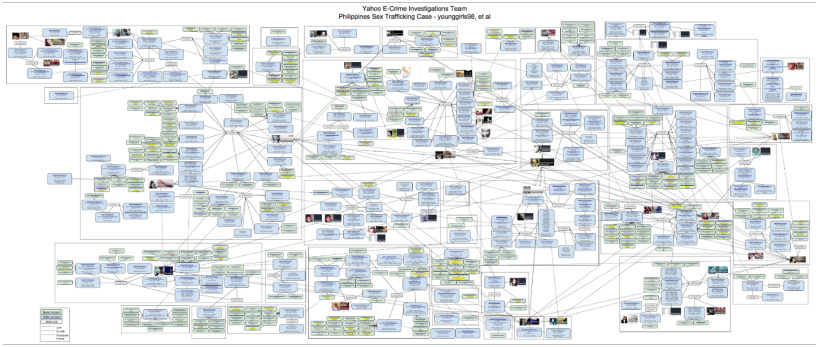
Case 2: Larger Ring



Case Study: Philippines Sex Tourism Investigation

- Identified dozens of buyers, sellers, and travelers
- Both cases sent to NCMEC, and then to FBI / Homeland Security, in 2014
- Met directly with FBI and HSI to highlight importance of investigation
- Began working on third investigation by manual links off of second case

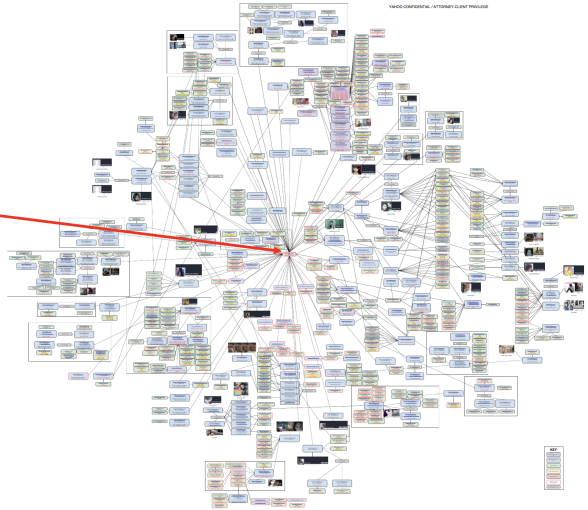
Case 3: Even Larger Ring



Case Study: Philippines Sex Tourism Investigation

- Referred third case to NCMEC, FBI, and HSI in 2015
- Most leads from Case 2 and Case 3 exhausted, but knew there was likely more activity ongoing
- Solution: proactive PhotoDNA scan of all Yahoo Messenger profile pictures (1B+) to detect potential CSAI at scale
- Led to the discovery of additional Philippines webcam accounts, including a very prolific buyer based in Dallas
- Fourth case referred in 2016

Case 4: Largest Ring



Case Study: Results

- In total, over 1,000 individuals identified worldwide
  - Primarily US, Canada, and Western Europe, but everywhere
- 250 buyers were determined to be traveling to the Philippines to abuse children
  - Not just a “virtual” crime
- To date, at least 100 individuals have been arrested and dozens of children rescued in the Philippines and in the US
  - Charlie Burks - the “Dallas Buyer” - received a 20 year sentence
  - Teachers, sex offenders, law enforcement officer, operator of sex tourism company, orphanage owner, US expat who had a “webcam house”, many others

12 minors rescued from sex trafficking

BY THE MANILA TIMES ON NOVEMBER 4, 2015

Singapore charges former German banker Michael Frank Hartung for promoting sex tours with minors

■ The 45-year-old has also been charged with the possession of 245 obscene and 8 uncensored films.

The Mercury News

Founder of Bay Area children's charity sentenced to prison for child pornography

Former Middletown High School teacher facing federal child pornography charges resigned

CBS SF Bay Area

Pacifica Man Gets 10 Years In Prison For Child Porn Possession

SEX OFFENDER ARRESTED FOR POSSESSION OF CHILD PORN

FBI: Washington sex tourist paid hungry kids for child porn

'If you want me to send you money for food you better get online'

By Levi Pulkkinen, SeattlePI Published 12:25 pm, Tuesday, August 2, 2016

Southbridge teacher Scott Peeler allegedly admits to receiving child porn in audiotape

FBI: Windermere man exploited children in Philippines, planned trip to 'rape little ones'

Updated: Sep 13, 2016 - 6:18 PM

Ventura County Probation Officer James Schmitt Arrested For Child Pornography

Brooklyn park worker charged with sexually exploiting kids from Philippines in online videos and chats

Inside sordid webcam den where suspected predator filmed child sexual abuse

Legal Challenges

- US v Rosenow
  - 2017: Indicted
  - 2018: Suppression hearing
  - 2019: Guilty verdict
  - 2019: Civil suit against FB and Yahoo
  - 2020: Ninth Circuit appeal
  - 2021: Ninth Circuit arguments (ACLU, EFF, Yahoo amicus)
- US v Wolfenbarger
  - 2016: Indicted
  - 2019: Suppression hearing
  - 2021: Jury trial testimony, guilty verdict
- US v Walter
  - 2019: Indicted
  - 2020: Declaration submitted
  - 2021: Jury trial testimony, guilty verdict

Lessons Learned

- Law enforcement is not a monolith
- Different agencies have different priorities
- Different countries have different laws
- Different cultures have different norms
- Multidisciplinary approach required
- Big data + manual investigation
- Industry & law enforcement collaboration is key

The Worse Person on Facebook

Widescale Sextortion Case

- Facebook has a dedicated child safety investigations team
  - Larger CSAM trading
  - Grooming/physical abuse
  - Sex trafficking
  - Live shows
  - Sextortion
- Shortly after I joined, the safety team began investigating a series of sextortion events
  - Physically distributed victims
  - Publicly posted threats
  - Good OpSec

Extortion, threats and control

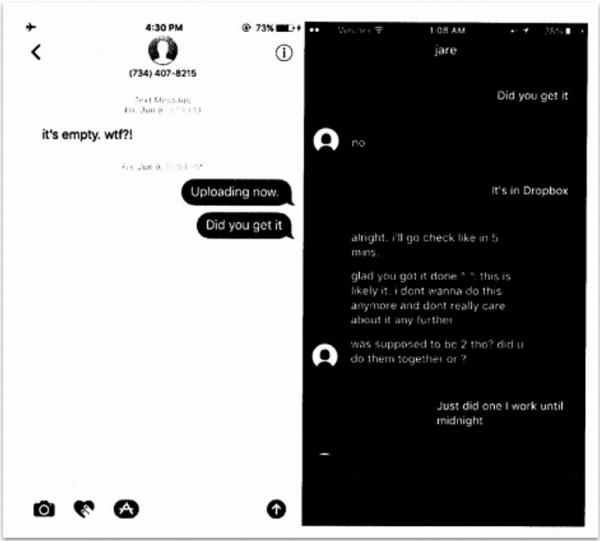


Figure 2: Extortion messages between perpetrator and victims

Public threats

Tomorrow will be a fucking bloodbath at plainfield high. I will open fire on all you sickening pieces of shit.

I have in my possession
3 home made pipe bombs,
2 handguns, and
1 semi auto rifle.

I will be targeting this whore [Victim 1] personally.

I know her exact schedule. I will slaughter EVERY SINGLE Peron who happens to have class with her. After I finish killing this whore [Victim 1] I wil turn my sights on her friends. I will methodically pick you off as you all run for your lives in the crowds. Those that I miss will be be blown to hell with the pipe bombs I set around campus. I plan on leaving no survivors.

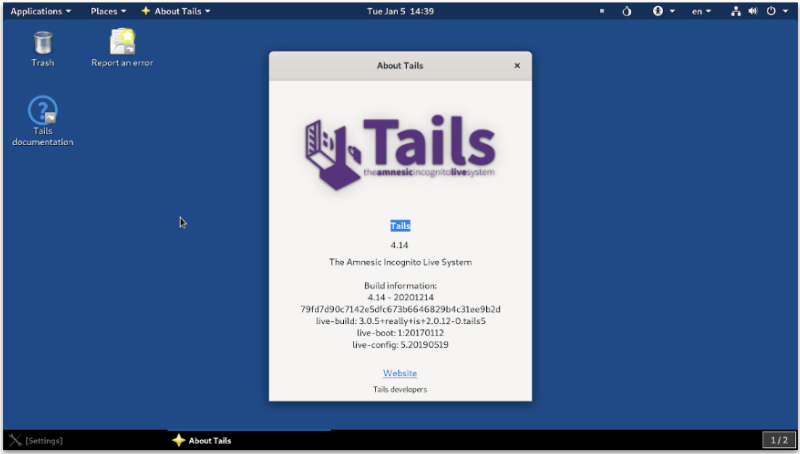
If you ever talked to [Victim 1], I swear to god I will put a bullet in your fucking skill. I suggest you stay home tomorrow if you value your life. If you think this is a joke then go to class tomorrow. I dare you. If you think the police have enough time to stop me this late at night then you know nothing about IP addresses.

After I kill her friends I will begin to erase all the faggots and nigger at plainfield. You sucking subhumans are ruining everything for everyone. The world will thank me for removing you all. You faggots will have to answer to God for your sins.

If you want the nudes of [Victim 1] now is the time to get them. I will be gone from this earth tomorrow and so will hundreds of plainfield students."

Good OpSec

1. Multiple email accounts
2. VOIP SMS numbers from bandwidth.com
3. Consistent use of Tor via TAILS



Network techniques catch Kil

F. Law Enforcement Identifies "Brian Kil's" True IP Address

51. On June 9, 2017, the Honorable Debra McVicker Lynch authorized the execution of a Network Investigative Technique "NIT" (defined in Cause No. 1:17-mj-437) in order to ascertain the IP address associated with Brian Kil and Victim 2.

52. As set forth in the search warrant application presented to Judge Lynch, the FBI was authorized by the Court to add a small piece of code (NIT) to a normal video file produced by Victim 2, which did not contain any visual depictions of any minor engaged in sexually explicit activity. As authorized, the FBI then uploaded the video file containing the NIT to the Dropbox.com account known only to Kil and Victim 2. When Kil viewed the video containing the NIT on a computer, the NIT would disclose the true IP address associated with the computer used by Kil.

Facebook went further than normal

MOTHERBOARD
TECH BY VICE

Facebook Helped the FBI Hack a Child Predator

Facebook paid a cybersecurity firm six figures to develop a zero-day in Tails to identify a man who extorted and threatened girls.

By Lorenzo Franceschi-Bicchierai

June 10, 2020, 7:57am Share Tweet Snap

Buster Hernandez aka Brian Kil

Lessons Learned

Conclusions

- A small number of offenders have disproportionate negative impact
- A small number of offenders have good OpSec
- Those things combined are terrible
- Fighting online abuse requires a multidisciplinary, multi-tiered approach
- Scalable, big-data approaches important, but don't be afraid of manual investigation
  - Would be very difficult to automate the expertise and contextual clues
- A key component is industry partnerships
- Direct engagement with law enforcement and NGOs drastically increases the chances of a successful outcome

Discussion: What is the appropriate role of companies?