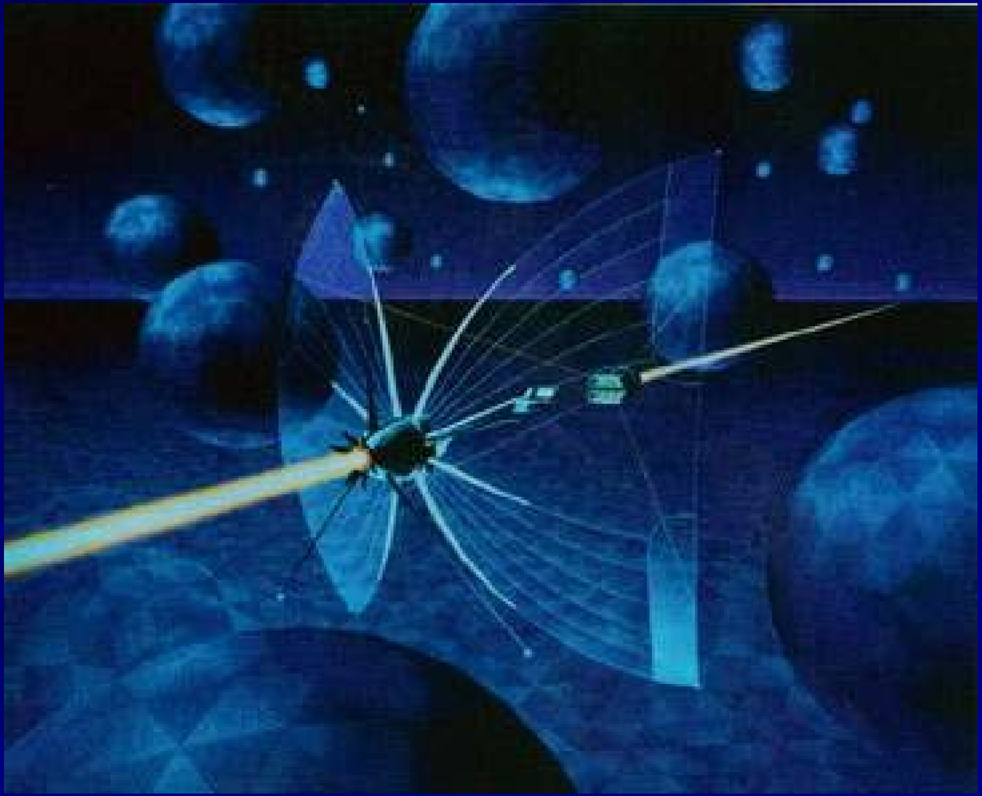
Cybercrime: Challenges for Law Enforcement



Susan Brenner

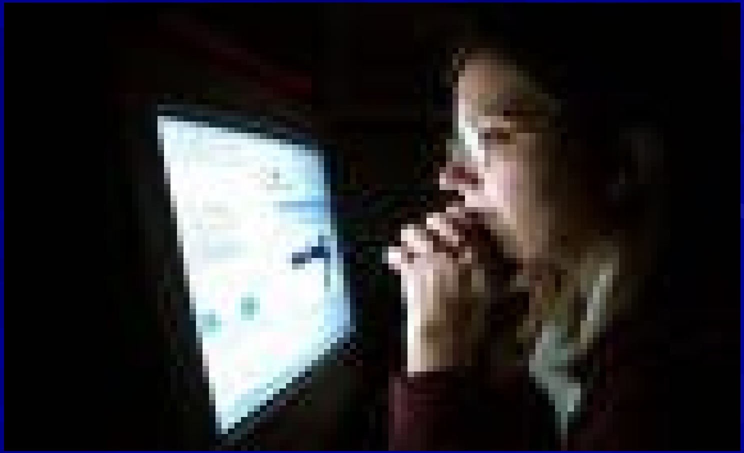
NCR Distinguished Professor of Law & Technology

University of Dayton

Real-world & cybercrime

- Current approaches evolved to deal with real-world crime

- Cybercrime occurs in a different context and therefore presents different issues



Example #1: Theft

- Real-world theft: possession of property shifts completely from A to B, i.e., A had it now B has it

- Cyber-theft: Property is copied, so A "has" it and so does B

Copying as theft?

- Randall Schwartz worked for Intel
- Charged with computer theft for copying a password file
- Claimed it wasn’t theft because Intel did not “lose” anything – Intel still had the passwords, and so did Schwartz

Enter Network Password

Please type your user name and password.

Site: sysf.onr.navy.mil

Realm New DB Login

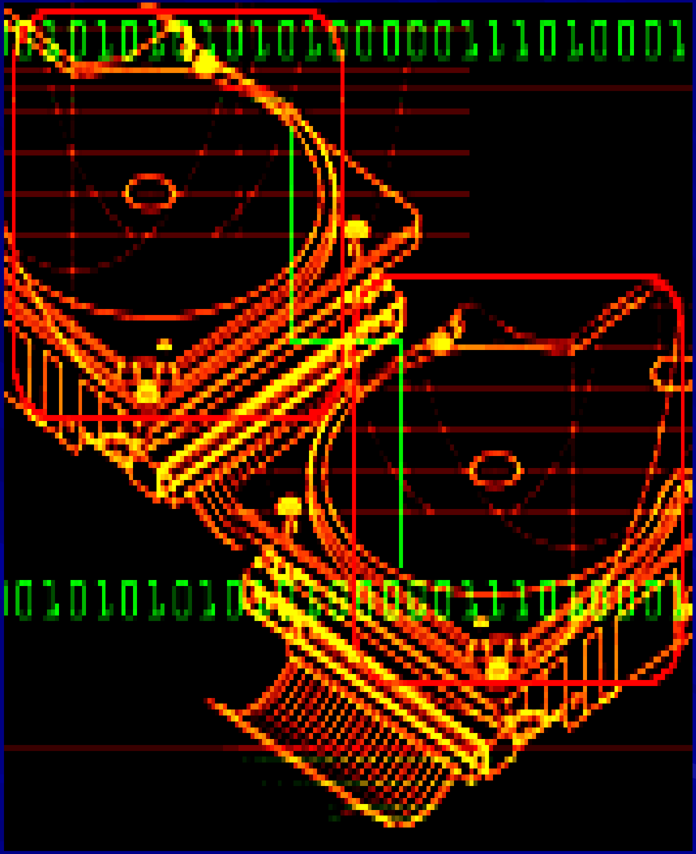
User Name

Password

□ Save this password in your password list

Example #2: Seizure

- Is copying files a seizure under the Fourth Amendment
- Same as theft?
- Nicky Scarfo logger



Nicky Scarfo logger

- FBI executed warrant at Scarfo's office
- Seized files from his computer – one was encrypted
- Agents installed a keystroke logger on his office PC, copied his passphrase – seizure?

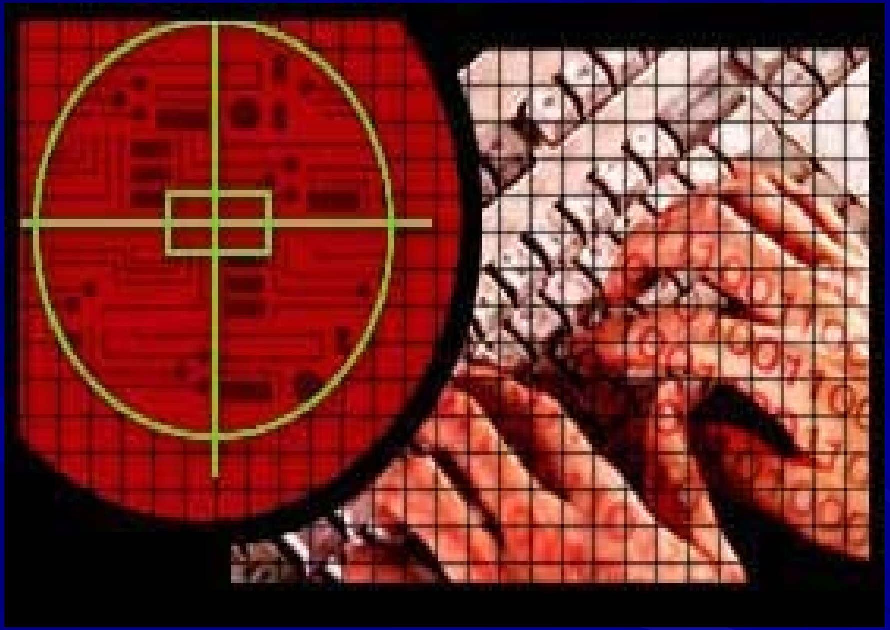
What is cybercrime?

Cybercrimes are divided into 3 categories:

- crimes where a computer is the target of the crime,
- crimes where a computer is a tool of the crime, and
- crimes where a computer is incidental to the commission of the crime.

Computer as Target

- Hacking (trespass)
- Cracking (burglary)
- Malicious code (viruses, worms, Trojan horses)
- Vandalism (web site defacement)
- Denial of service attacks



Target case: John Sullivan

- Hired to develop software program for Lance, Inc.
- Demoted, he hid a logic bomb in the program
- It shut down 824 handheld computers sales reps used to contact headquarters, costing Lance, Inc. over $100,000
- *U.S. v. Sullivan,* 40 Fed. Appx. 740 (4th Cir. 2002)

Target Case: Czubinski

- IRS customer service rep who could use IRS computers to answer customer questions
- Looked up tax returns of a woman he dated, ADA prosecuting his father, etc.
- Charged with wire and computer fraud
- Charges dismissed – no evidence of scheme to defraud

IRS
Department of the Treasury
Internal Revenue Service

Denial of Service - 02/2000

- Yahoo, Amazon, eBay, CNN & Buy.com were all attacked

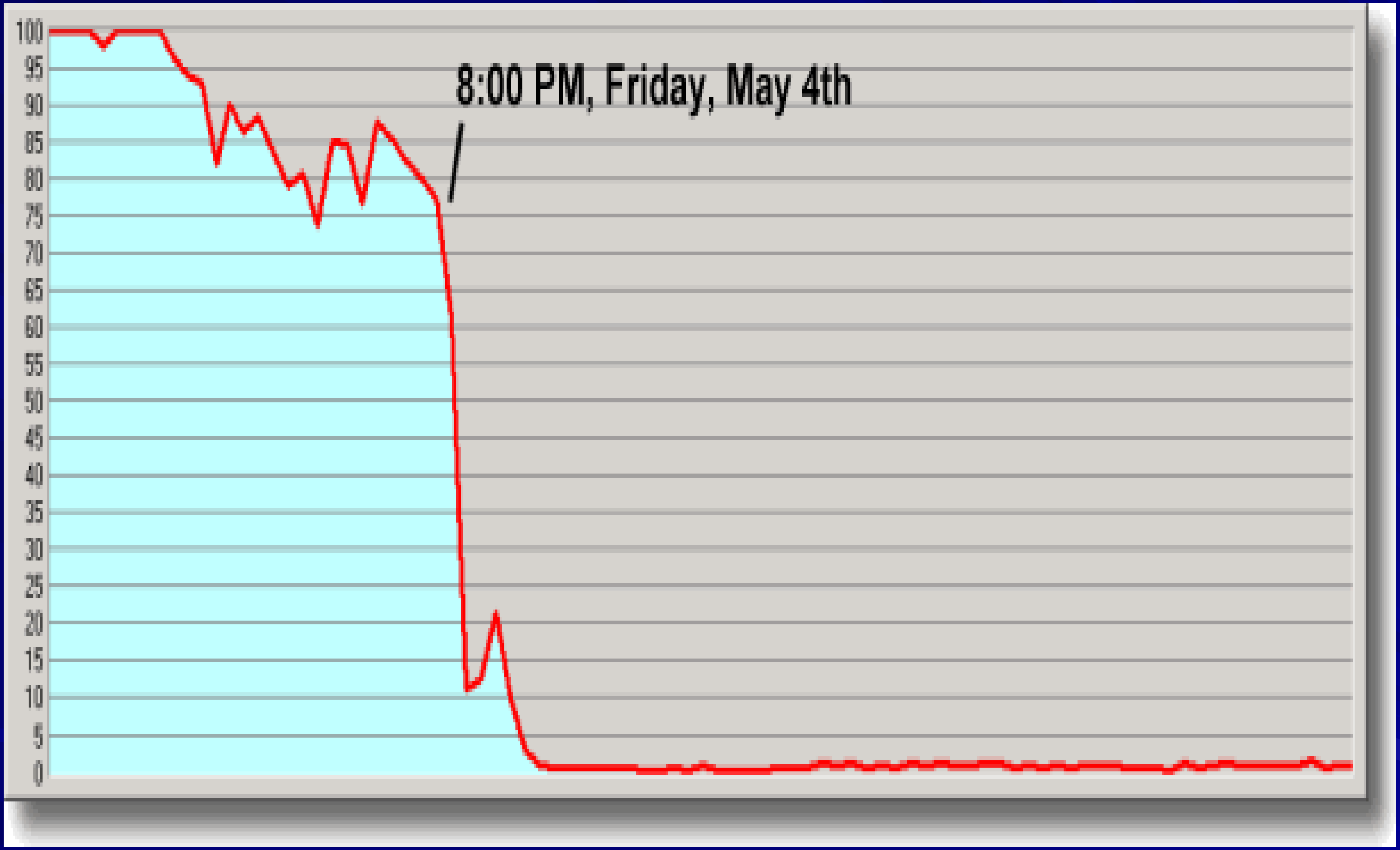
- 15-year-old pled guilty to the attacks, which did an estimated $1.7 billion in damage

- 8 months in a juvenile detention center

YAHOO!
What's New
Check Email
Personalize
Help
Yahoo! Auctions
Tiger Woods, autos
Win a Trip to Paris from proflowers.com
Click Here
Free Internet Access
Search
advanced search
Shopping - Auctions - Yellow Pages - People Search - Maps - Travel - Classifieds - Personals - Games - Chat - Clubs
Mail - Calendar - Messenger - Companion - My Yahoo! - News - Sports - Weather - TV - Stock Quotes - more...
Yahoo! Shopping - Thousands of stores. Millions of products.
Departments
Apparel
Bath/Beauty
Computers
Electronics
Flowers
Food/Drink
Music
Video/DVD
Stores
Macy's
FTD
Coach
Banana Republic
Products
Valentine's Day
Pokemon
MP3 players
DVD players
Arts & Humanities
Literature, Photography...
News & Media
Full Coverage, Newspapers, TV...
In the News
more...
Marketplace

- Afghan airliner hijacking
- Yugoslav defense minister killed
- Tiger wins sixth straight
- Steven Spielberg has kidney removed

DDos Attack on GRC.Com

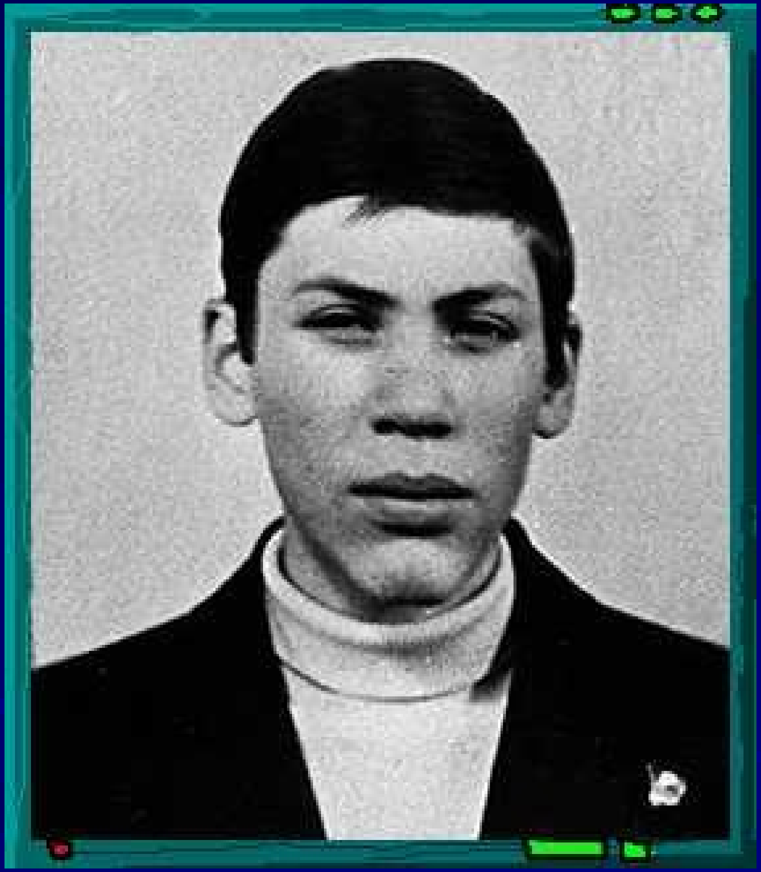


"I just ddosed you," Wicked, 13

Computer As Tool

- Fraud
- Theft
- Extortion
- Stalking
- Forgery
- Child pornography
- Other???

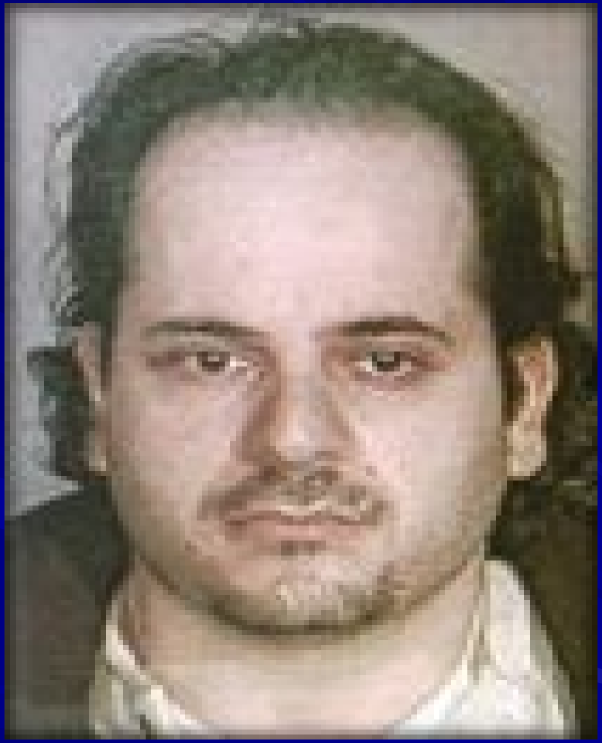
Theft: Citibank



- Vladimir Levin took responsibility for siphoning $10 million from Citibank and transferring it into foreign accounts
- Sentenced to 3 years in prison

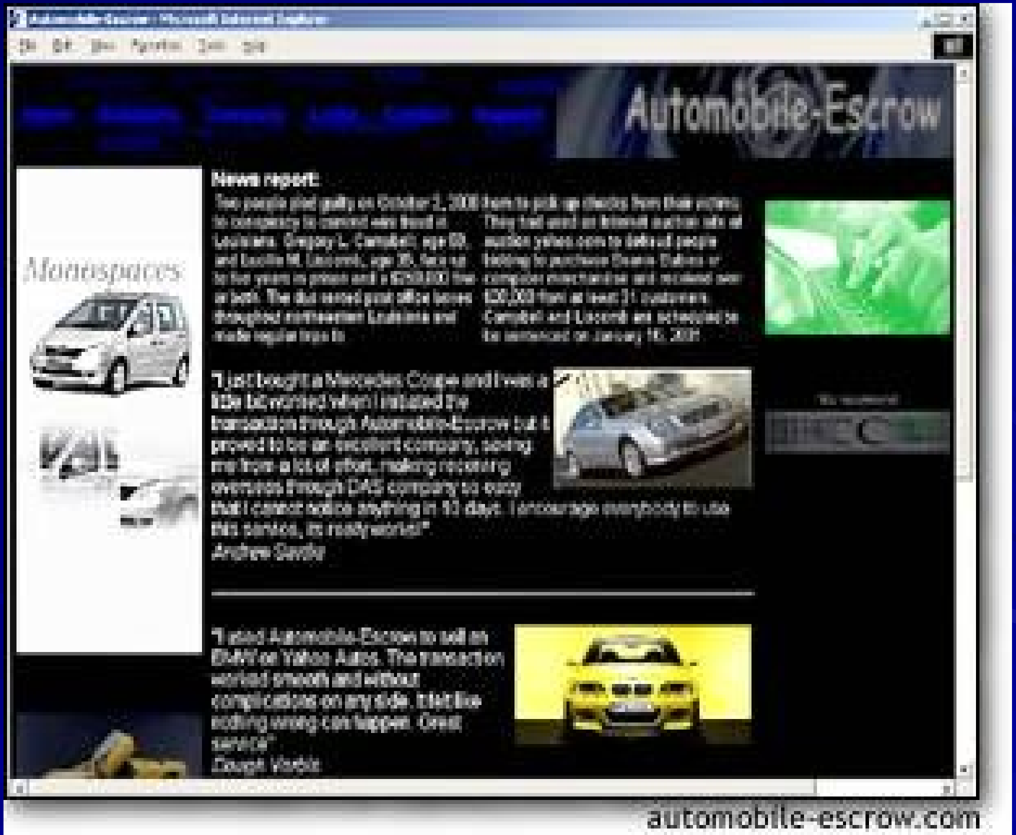
Identity Theft/Fraud

- Abraham Abdallah, a bus boy, stole the identifies of Oprah Winfrey, George Lucas, Ross Perot, etc.
- Transferred funds from their accounts to ones he set up using computers in public libraries



Fake Escrow Sites

- Dentist Bruce Lachot sent $55,000 to an escrow site to buy a BMW from a German seller
- Fake site
- Lachot never got his BMW or his money back



Automobile-Escrow - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Automobile-Escrow
Monospaces

News report:

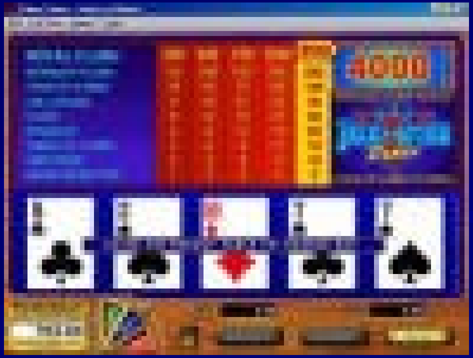
Two people pled guilty on October 2, 2000 to conspiracy to commit wire fraud in Louisiana. Gregory L. Campbell, age 53, and Lucille M. Lacomb, age 35, face up to five years in prison and a $250,000 fine or both. The duo rented post office boxes throughout northeastern Louisiana and made regular trips to them to pick up checks from their victims. They had used an Internet auction site at auction.yahoo.com to defraud people bidding to purchase Beanie Babies or computer merchandise and received over $20,000 from at least 31 customers. Campbell and Lacomb are scheduled to be sentenced on January 16, 2001.

"I just bought a Mercedes Coupe and I was a little bit worried when I initiated the transaction through Automobile-Escrow but it proved to be an excellent company, saving me from a lot of effort, making receiving overseas through DAS company so easy that I cannot notice anything in 10 days. I encourage everybody to use this service, its really works!"
Andrew Savdy

"I used Automobile-Escrow to sell an BMW on Yahoo Autos. The transaction worked smooth and without complications on any side. I felt like nothing wrong can happen. Great service"
Dough [illegible]

automobile-escrow.com

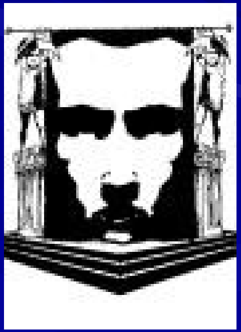
Fraud? Theft?



- Hacker fixes online casino’s server so people playing craps and slots could not lose
- Players won $1.9 million
- Others have done similar things, then demanded money not to repeat it

Stalking a School

- 1999 – Massachusetts middle school is stalked by an unknown person
- Students, faculty, parents and the entire town are panicked
- Christian Hunold, a 20 year old paraplegic, eventually identified as the stalker



The Nuremberg Files

Black font (working)

Grey font (wounded)

Strikethrough (dead)

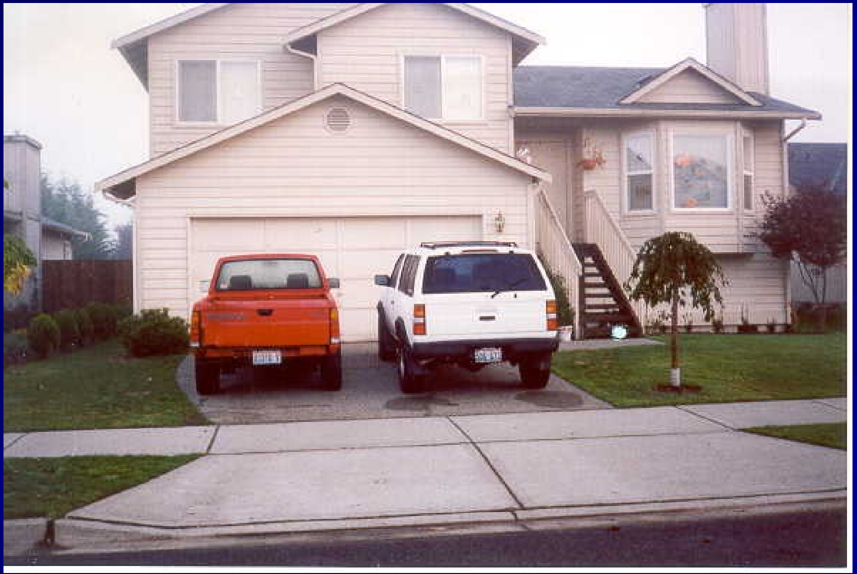
http://www.christiangallery.com/atrocity

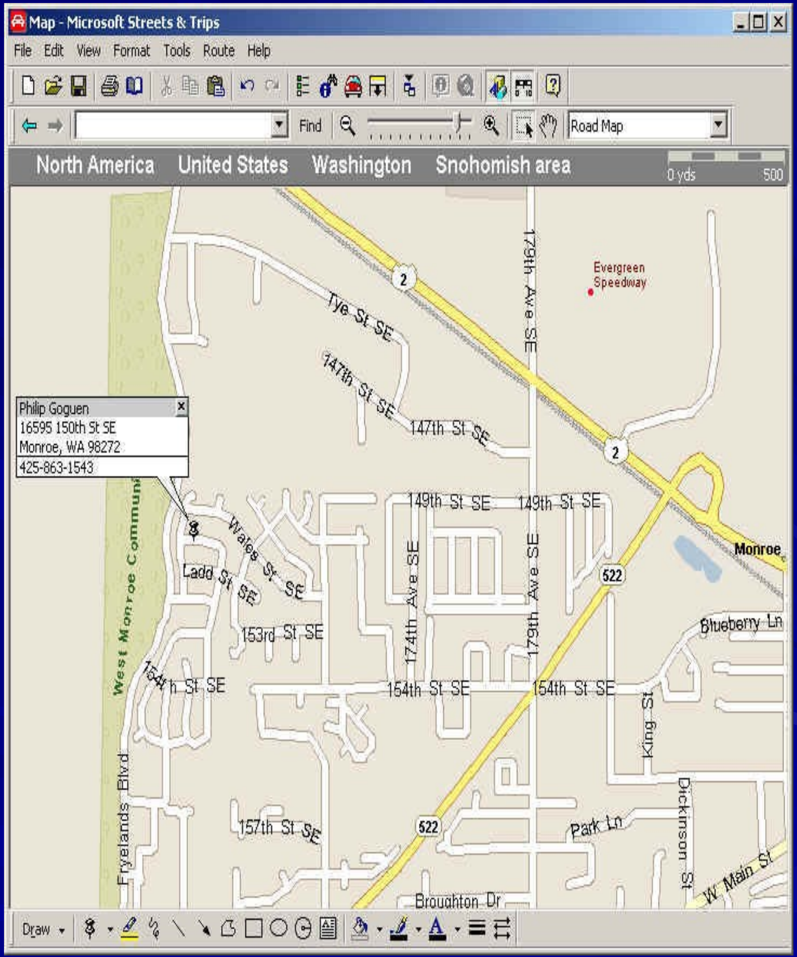
JusticeFiles.org

Philip C. Goguen, Kirkland Police officer

This is a picture of Officer Goguen's home.

This is a map to Officer Goguen's home.





Philip Goguen
16595 150th St SE
Monroe, WA 98272
425-863-1543

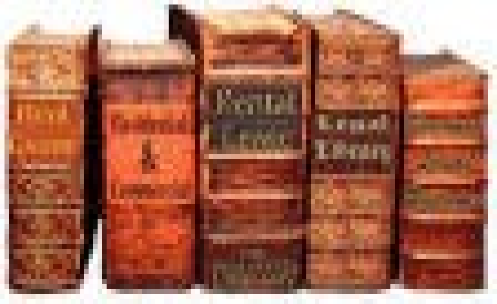
Computer Incidental

- Blackmailer uses computer to write blackmail letters
- Drug dealer stores records on computer
- Computer used to research murder methods

Divergences

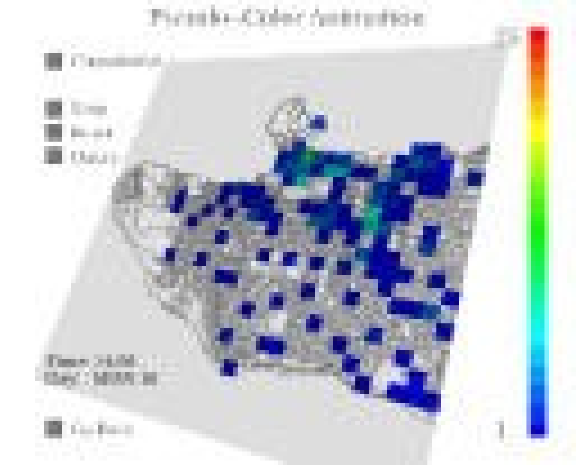
- Real-world crime and cybercrime differ in several respects

- Differences make it difficult to apply traditional principles of criminal law and law enforcement to cybercrime



Real-world crime

- Proximity
- Limited Scale
- Physical constraints
- Patterns



Real-world crime shaped law enforcement

- Reactive model
- Crime committed
- Investigation
- Apprehension
- Conviction
- Deterrence
- Crime controlled

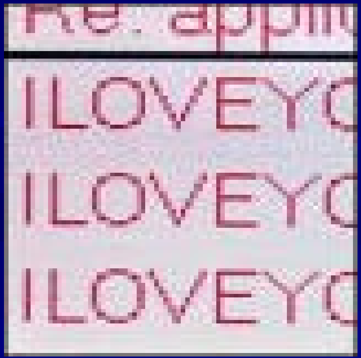
Cybercrime: proximity

"In the networked world, no island is an island."

McConnell International, *Cyber Crime . . . And Punishment Archaic Laws Threaten Global Information (2001).*

Proximity: example #1

E. Cortero / Newsmakers file



Re: appli

ILOVEYO

ILOVEYO

ILOVEYO

- Onel de Guzman, accused author of the “Love Bug” virus
- $10-$12 billion in damage in over 20 countries
- Not a crime in the Philippines, never prosecuted, anywhere

Proximity: example #2

- Attacked companies in 10 states
- Extorted money by threatening to sell stolen data/return and cause damage
- FBI identified Vasiliy Gorshkov and Alexey Ivanov as the hackers

Gorshkov Ivanov

Example #2 - continued

- Interview with Invita

- Used FBI laptop to access a Russian computer and demo hacking skills – arrested

- FBI used information obtained by a logger on the laptop to access the Russian computer and download evidence without a warrant

Invita: Implications

- Cybercrime is transborder, transnational crime
- Russians would not assist FBI -- no MLAT in effect
- In August, the Federal Security Service charged an FBI agent with hacking

Cybercrime: scale

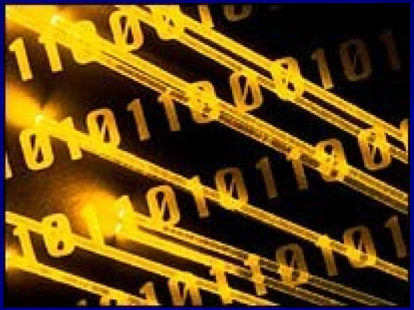
- Thomas & Janice Reedy provided a gateway to child porn sites

- 350,000 subscribers (35,000 in US & 1,300 in the UK)
- Estimate: it takes 80 hours to process one computer, which is only part of prosecuting

Physical constraints

- Anonymity
- Easier to avoid leaving trace evidence
- Crimes are committed quickly – more easily concealed

Concealment: framing

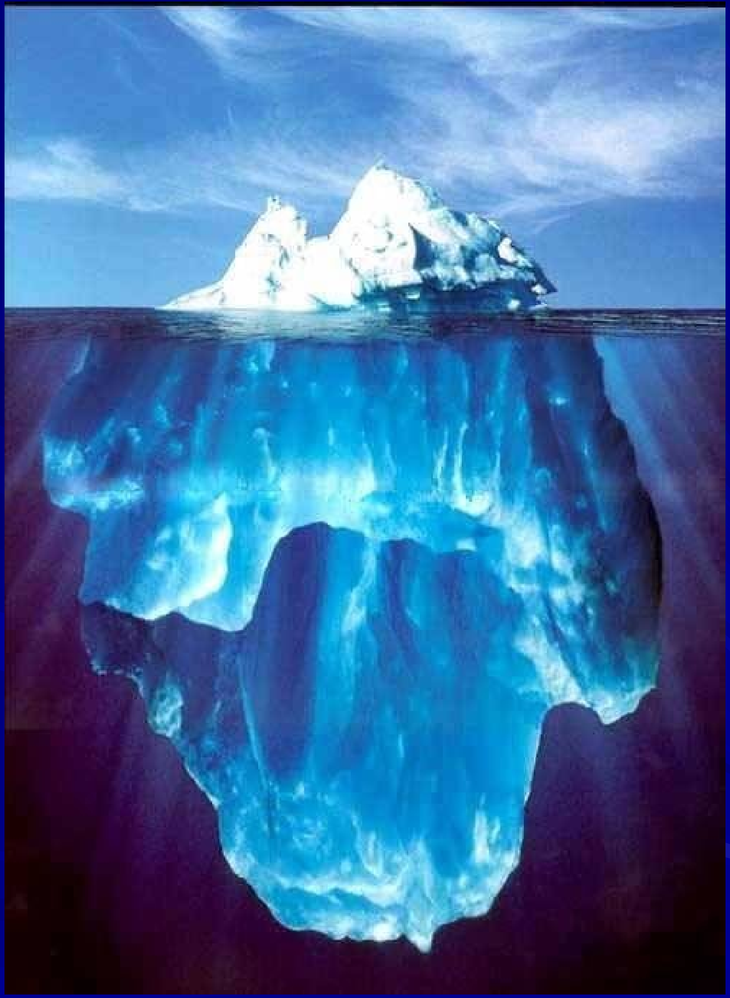


- NY executive discovered email was being tapped
- Traced to former employee, Joe Smith, in St. Louis
- Smith said he did not do it

- Further investigation showed Fred Doe, former employee in Seattle, tapped email and framed Smith

Cybercrime Patterns?

- Lack of accurate statistics
- No standard offense definitions
- Hard to parse a cybercrime into “offenses” – was the Love Bug one crime or thousands of crimes?

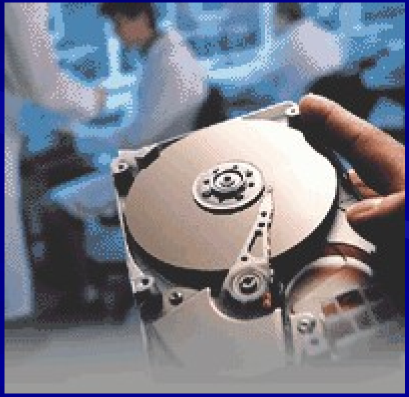


Different Approaches

- Collaborative model – commercial
- Prevention (information sharing, etc.)
- Informal reporting of cybercrimes
- Reacting – private resources supplement law enforcement resources

Legal issues

- Must private personnel abide by rules governing law enforcement?
- Permissibility of using private personnel in evidence-gathering
- Locus of the decision to prosecute



Private Person case

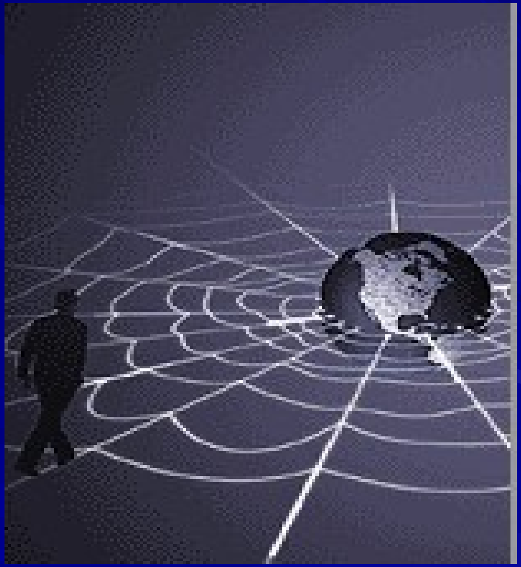
- Person claiming to be Turkish hacker gives police evidence of child porn/molestation
- Investigation and arrests
- Turkish hacker agent of the police?

- U.S. v. Steiger, 318 F.2d 1039 (11th Cir. 2003) (no); U.S. v. v. Jarrett, 229 F. Supp.2d 503 (E.D. Va. 2002) (yes_

Shift

- Emerging model is a shift from a law enforcement, primarily reactive model, to a collaborative preventive-reactive model

- Emphasizes prevention because of the difficulties involved in reacting to cybercrime



Expanding the Model

- Collaborative approach for individuals?

- Prevention?
  (Assumption of the risk?)

- Increased reporting?

- Reacting? Vigilantism?
  Victim reaction?

Institute

- University of Dayton School of Law establishing new institute
- International Institute for Technology, Security and Law
- Cybercrime research, training, policy analysis
- Formal announcement in August

Susan W. Brenner

Susan.Brenner@notes.udayton.edu

http://www.cybercrimes.net