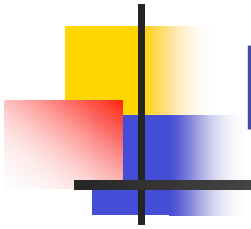
Beyond "I Fought The Law"

Educating Law Enforcement about Privacy Services

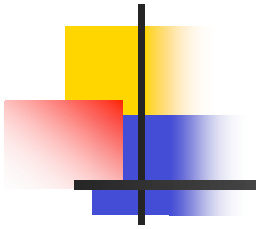
Adam Shostack

(Presented at PET2003)



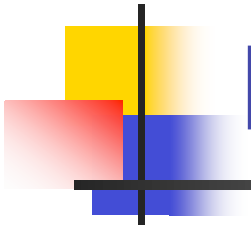
Motivation

- 3 Years at Zero Knowledge Systems
- Freedom Network didn't succeed
  - Problems was sales, not law enforcement
  - LE moved from scared to a customer
- Not enough remailers, privacy services
- Some potential operators are scared
- Share learning
- See more privacy technology deployed



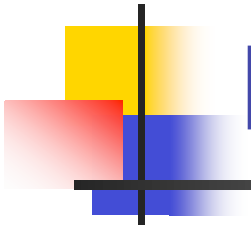
The *Cypherpunk Attitude*™

- Is lots of fun
  - Has brought enourmous publicity
  - Has encouraged a great deal of leading work
- Is a liability in talking to LE
  - Doesn’t do any good
  - Generates resistance and hostility
- Most cops are decent people
  - Trying to solve crimes, help people
  - Initial impressions are very important



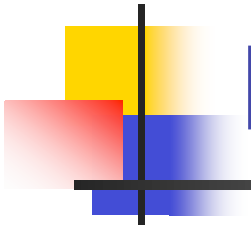
Mellontrafficers.com

- Is a fine domain
- Got Len in trouble
- He hasn’t changed it
- Compare and contrast



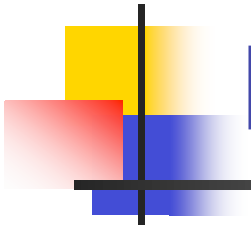
Basic Message

- Privacy reduces crime
  - ID theft
  - Spam
  - Stalking
  - Crypto is not an unmitigated anything
- LE should be in favor of privacy
  - Lets get along
- Method can be used with any privacy service



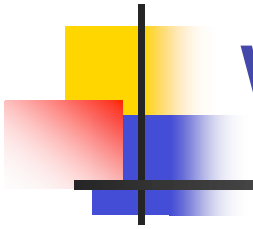
Delivered Message Regularly

- At ZKS Offices
- At RCMP, Interpol meetings
- Over phone
- Had LE outreach materials ready at abuse, legal, elsewhere
- Slides will be under http://www.homeport.org/~adam/zks/



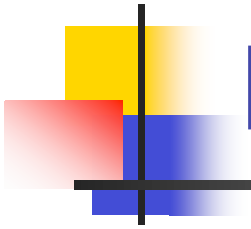
How to Present

- This is why we do what we do
- Here's how it prevents crime
- Here's why we don't log
- Here's how you can make progress
- Avoid
  - "Bugger off"
  - "I know your job more than you"
  - Taking this talk as legal advice



Why We Run Remailers

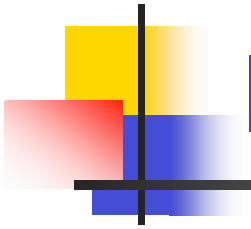
- Privacy prevents crimes
  - Stalking
  - ID theft
  - Spam
- Privacy is a Social Good
  - Whistleblowing
  - Communication
  - Schoeman's "Philosophical Dimensions of Privacy"



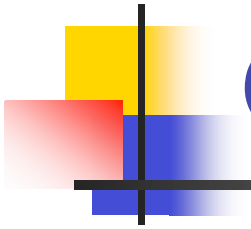
Prevent Crime

- This is a key point
- Preventing crime is better than solving crimes
- “Would you prefer a lock or a video camera?”
- Easy examples: Crypto prevents CC theft, password theft

Crypto Hinders Criminals & Investigators

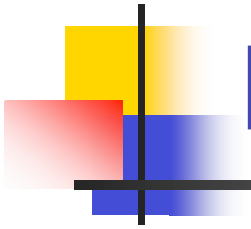


- Crypto can prevent crime:
  - Encrypted data harder to steal, monitor
  - Can’t sniff passwords
  - Can’t forge authentications
- Crypto can make investigations harder
  - Can’t read everything the bad guy says, stores
  - Their job is about investigation, not prevention
  - So, naturally police are very aware of this side of things, and sometimes miss the larger picture



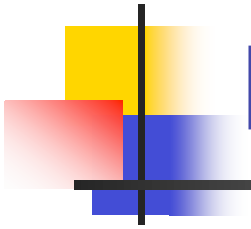
Ok, but the logs?

- We don't log because logs can be abused
- Available to anyone with a subponea
  - Raises cost of running remailer
  - Creates a security risk
- We don't know how to create a remailer where only the police can read the logs
  - (Blaze's broadcast escrow impractical to deploy)



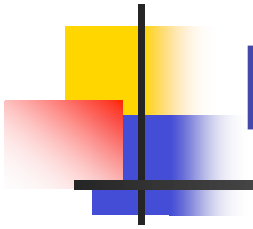
More on Logs, back doors

- DMCA Subpoenas
- Very hard to engineer security systems
  - Even harder to engineer backdoors
  - Clipper Chip example
- Which legal system?
  - Freedom Network ran in 10+ countries



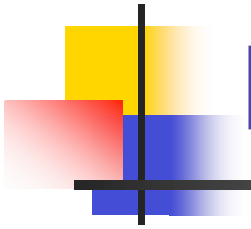
How to Investigate

- You are selling remailer system/privacy
- In sales:
  - Agree, Align, Convert
- Don’t start by arguing
  - “You’re just trawling”
  - “That’s awful, what can I do to help?”
  - “Actually, we don’t keep logs. Let me explain why.”



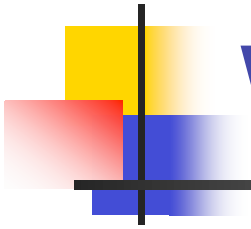
Know the Case Law

- Put the right to anonymity in context
  - McIntyre vs. Ohio
  - NAACP vs. Alabama
  - Federalist Papers
- Abuse of subpoenas
  - Northwest airlines and their union
- Clearly, this is US case law
  - Know your local law



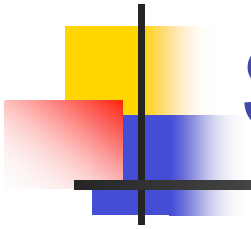
How To Investigate (more)

- “Clearly, I am not an investigator”
- Think about the basics
  - Means, motive, opportunity
  - Undercover work
  - Use privacy service to communicate with criminals
  - Privacy is a two-way street



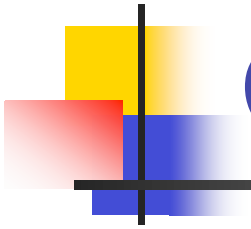
What A Privacy Service Offers

- Communicate without a name attached
- Block basic sniffers, logs
- Explain the limits of the remailer system
  - You can’t shoot someone through it
  - You can’t bring down the power grid with an email
  - Doesn’t stop hacking suspect’s computer
  - One on one surveillance



Summary

- Overview of ZKS' law enforcement message
- Overview of the thinking which drove it
- Lessons for the privacy technology world



Conclusions

- Biggest problems are not technical, or even legal, they're in business & economics
  - Press, analysts had trouble understanding Freedom Network vs Anonymizer,
  - MIX nets, real time and batch, need more users in their anonymity sets
- Police and national security have an interest in these systems existing