

Reducing Crime in Cyberspace: A Privacy Industry View

Stephanie Perrin

Adam Shostack

Zero-Knowledge Systems, Inc

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialogue

Who We Are

- Formed in 1998 to build strong privacy systems
- Venture Funded Montreal Company
- Attracted top privacy and cryptography experts
- Selling *Freedom 1.1*, world's best privacy software

Overview of Talk

- **Our Goals**
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialog

Our Goal

- Prevent People From Being Victimized
 - Victims of criminal invasions of privacy
 - Victims of non-criminal invasions
 - By Individuals
 - By Organizations
 - By Technical Accident
- Our goal today is to open a dialogue with you
 - We share many goals
 - We look forward to working together

Overview of Talk

- Our Goals
- *A Short history of Privacy*
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialog

A Short History of Privacy

- Provide Context For Discussion
 - Understand Laws, International Activity
 - Privacy Invasive Technologies
- OECD
- EU Data Protection
- Canada's Bill C-6, Charter of Rights
- US Constitution and case law

Overview of Talk

- Our Goals
- A Short history of Privacy
- **Crime in Cyberspace**
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialog

Crime in Cyberspace

- Cyberspace crimes
- Physical World Crimes
- How they blend
 - Line can be hard to define
- Privacy and Hacking

Cyberspace Crimes

- Cybercrime is Diverse
 - Denial of Service & distributed variants
 - Stealing money
 - Stealing bits
 - Hacking
- Cybercrimes that blend into the real world
 - Stalking
 - identity theft

Cyberspace Crimes (2)

- Some types are aided by privacy (DDOS, Hacking)
- Some types are privacy-neutral
 - Stealing money from a bank
- Some types are hindered by privacy
 - Identity Theft
- Some the only defence is privacy
 - Stalking

Real World Crime and Cyberspace

- Talking about cybercrime often blends into physical world crime
 - Planning terrorist acts with email
 - Drug Trafficking
 - Money Laundering
 - Fencing Stolen Goods
 - Who wants to shut down Ebay?
 - Kiddie Porn

Real World Crime and Investigation

- Who cares if its encrypted?
- Subject under investigation can be targetted even with encryption
 - Traditional Surveillance
 - Computer Security is poor
 - Undercover Activity

Real World Policing and Cybercrime

- Desire for Perfect Information
 - Doesn't exist offline
 - Won't exist online
 - Perfect information is a myth
- Why try to create it online?
 - Good reasons not to
 - Fundamental liberties
 - Cost of transactions
- Risk of “perfect” data being abused

Privacy and Criminals

- Criminals have privacy
 - Motivation to learn
 - Motivation to buy
 - Identity theft
- Normal People and Police don't
- The worst of all possible worlds

Privacy and Hackers

- Hackers have privacy
 - Break into system
 - Destroy the logs
 - Repeat as needed
 - They don't use or need our software
- Normal People and Police don't
- The worst of all possible worlds

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- **Monitoring of Cyberspace**
- Technologies of Privacy
- Opening a dialog

Monitoring of Cyberspace

- Investigation
- Traffic Analysis and Surveillance
- Undercover Operations
- The Threat of Perfect Knowledge

Investigation

- Freedom reduces utility of logs
- Freedom blocks sniffers
- Freedom hides information that an investigator may want
- Freedom does not prevent
 - People from revealing information
 - People hacking into computers (DIRT, Back Orrifice)
 - One-on-One surveillance (TEMPEST, video)

Traffic Analysis and Surveillance

- Freedom reduces ease of traffic analysis
 - We're not sure how much
- Use of Freedom is observable by analyst

Undercover Operations

- Are an effective tool
- Freedom makes it easy for a law enforcement officer to infiltrate
- Freedom protects privacy of family of LE

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- **Technologies of Privacy**
- Opening a dialogue

Technologies of Privacy

- The Freedom System
- Critical Infrastructure Protection
- Minimal Disclosure Technologies

The Freedom Network

- Designed to maximize privacy
- No back doors
- Known flaws listed in whitepaper

The Freedom Network

- Diagrams etc
- Identity/Anonymity Slider
- Distributed Ownership and Control
- Zero Knowledge

No Back Doors

- Systems with backdoors are hard to defend
- Digital Millennium Copyright Act (US)
- Raytheon, Northwest Airlines
- Too many keys must be distributed
- Due Process weakened by back door
- Weakens evidence chain
- Industrial Espionage
- Rouge States

Known Flaws Enumerated

- Security Experts like public analysis
- We encourage analysis and examination
- Some flaws can be exploited
- Listed in a whitepaper

Critical Infrastructure Protection

- Freedom can protect
 - Whistleblowers
 - Security Exploit Information
- Privacy is part of the information infrastructure
 - *Requires* Protection
 - Enables growth of the medium

Minimal Disclosure Technologies

- Exciting new privacy tools
- Invented by Chaum, extended by Brands
- Envelope with a window
- Certified information revealed selectively
- Online Spaces where different levels of “True Name” are accepted

Minimal Disclosure Technologies

- Exciting new privacy tools
- Invented by Chaum, extended by Brands
- Envelope with a window
- Certified information revealed selectively
 - Dating services require over 18
- Online spaces where different levels of “True Name” are accepted:
 - Stock boards require identity

Overview of Talk

- Our Goals
- A Short history of Privacy
- Crime in Cyberspace
- Monitoring of Cyberspace
- Technologies of Privacy
- Opening a dialogue

Opening a dialogue

- Our goal today is to open a dialogue with you
 - We've explained what we do and why
 - We share many goals
- We look forward to working together
 - Education
 - Risks
 - Proper Behavior
 - Sharing information and education

Reducing Crime in Cyberspace: A Privacy Industry View

Stephanie Perrin

Adam Shostack

Zero-Knowledge Systems, Inc

www.zeroknowledge.com