



Privacy and Security in a Wireless World

Sherman Hall

Atherton Police Department

REACT Task Force



Overview

- Two Competing Pressures
- Search Warrant Barrier
- The Status Quo
- Hazards of Complete Anonymity
- Registration: What information to Collect
- Record Retention, Sniffing, Content Monitoring, and User Notification



Introduction

- 15 years IT experience
- LE is second career
- Assigned to REACT
 - High technology crime
 - Computer forensics



Two Competing Pressures

- Move on Internet Anonymously vs. Tracking
- Goal is to achieve a balance
 - Protect life and property without chilling free speech
 - Fund the wireless system without giving up privacy
- Law Enforcement's Balance Proposition
 - User Registration
 - Narrow scope of information – no content
 - Warrant requirement



The Search Warrant Barrier

- Search Warrants
 - Law enforcement can not seize user information without probable cause
 - Investigative resources are scarce
 - Search Warrants take time
 - Barrier to government intrusions; only big cases
- Exigent circumstances
 - Imminent threat of death or great bodily injury
 - Write a warrant later



The Status Quo

- Paid services mean we enjoy partial anonymity
 - Identity information is available
 - Billing records require name, address, and credit relationship
- Advocate keeping what we have
 - No loss of freedom over what exists today



Hazards of Complete Anonymity

- Free wireless Internet model could bring **complete** anonymity
 - No need to collect subscriber information
 - Could be move anonymously on the Internet
- In a perfect world, this would be the ideal
- Unintended Consequences
 - No deterrence to online crime
 - Frustrate Investigations
 - No controls for minors



Registration: What information to Collect

- NOT INTERESTED IN CONTENT
- Narrow Scope of Information:
 - Identify the user and contact information
 - Location information
 - Leased IP information tied to the user



Other Issues: Record Retention

- Ninety Days of Information
 - Financial crimes can take a long time to discover
 - Provider needs time to seize the information



Other Issues: Sniffing

- Possible to intercept and mine the data
- Increased demands on law enforcement
 - More identity theft
 - Network intrusions
- Need to secure the wireless transmissions
 - User education and free tools
 - WEP / WPA technology



Other Issues: Content Monitoring

- No expectation that the provider would monitor content
- Could be a victim of network intrusion
- Could find child pornography on their servers; should report that Law Enforcement



Other Issues: Notification

- Acceptable to notify the target unless ordered otherwise by the court.