Legal Issues Associated With Data Collection & Sharing

Jody R. Westby, Esq.
CEO, Global Cyber Risk LLC
Chair, American Bar Association Privacy & Computer Crime Committee (Section of Science & Technology Law)

BIC
July 6, 2011
Amsterdam

The Problem

- Researchers need data for problem definition & testing
- IRBs and legal counsel increasingly scrutinizing
- Legal issues are global in scope and highly complex, inconsistent
- Legal issues create barriers and restrict use
- Complexity & global nature of botnets is compounding problem
- Guidance for researchers is scarce
- Ethical issues clouding legal analysis
- Failure to properly analyze legal considerations may result in embarrassment, tarnished reputations, loss of research funding, ruined careers, significant fines, and/or imprisonment

Help is On the Way!

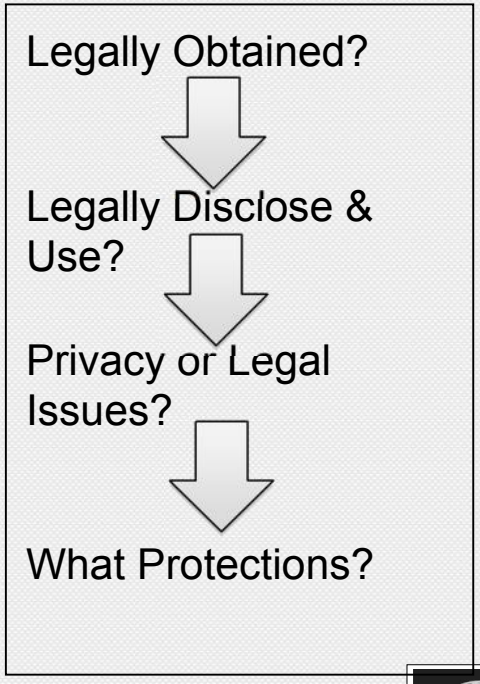
- US Department of Homeland Security PREDICT project provides datasets to the R&D community and conducts comprehensive legal analysis on each dataset
- PREDICT risk process rovides researchers and organizations with more certainty
- DHS Broad Agency Announcement funded development of two publications
  - Legal & Policy Tool Chest for Cybersecurity R&D
  - Legal Guide to Cybersecurity Research on Botnets
- To be published by American Bar Association Summer 2011
- BADGER & other efforts help clarify

Legal & Policy Analysis Tool Chest

- Three Tools
  - Legal Analysis Tool on Obtaining & Using Network Communications Data
  - Privacy Tool on Using Network Communications Data
  - Protection Measures Tool

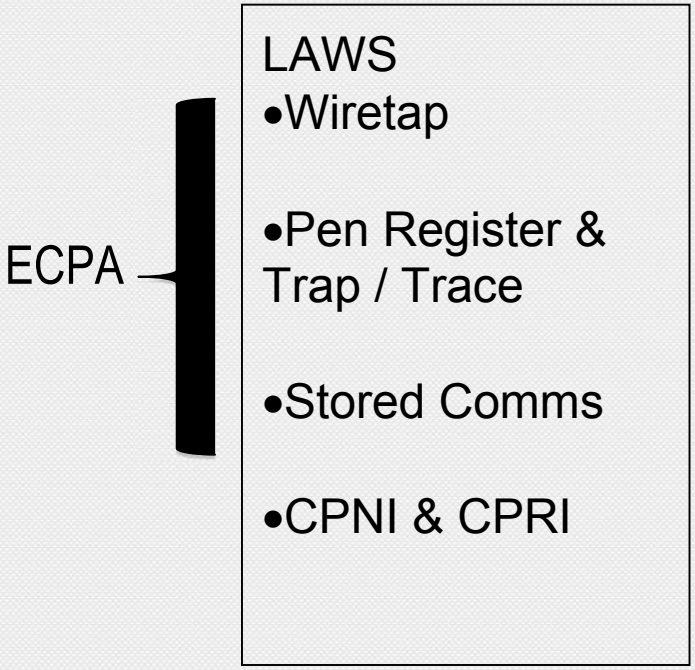
- Based on U.S. Laws

- Goal: Provide researchers, IRBs, legal counsel, & others with tools to understand legal & policy issues with using communications data in cyber security R&D project.



Legal Analysis Tool: Introduction

- Data May Not Have Been Obtained Legally:
  - Wiretap Laws (Interception)
  - Pen Register & Trap/Trace Laws
- Data May Not be Disclosed to Third Party (Researcher)
  - Wiretap Laws
  - Stored Communications Act
  - Confidential Phone Record Information (CPRI)
  - Customer Proprietary Network Information (CPNI)
- Data May Not be Used by Third Party
  - Wiretap Laws



Simplified View

INTERCEPTION						
Real-Time Activity	**Researcher**		**Provider**		**Consent**	
	Headers	**Content**	**Headers**	**Content**	**Headers**	**Content**
Capture	NO	NO	OK	OK	OK	OK
Disclose to Others	NO	NO	Silent - Use MOA Also c/ be CPNI or CPRI	NO – Use MOA	OK	OK
Use by Others	NO	NO	Silent – Use MOA Also c/ be CPNI or CPRI	NO – Use MOA	OK	OK
Equipment	Possess-OK	Possess-NO	Possess-OK	Possess-OK	N/A	N/A
	Install–NO	Install–NO	Install-OK	Install-OK	N/A	N/A
	Use-NO	Use-NO	Use-OK	Use-OK	N/A	N/A

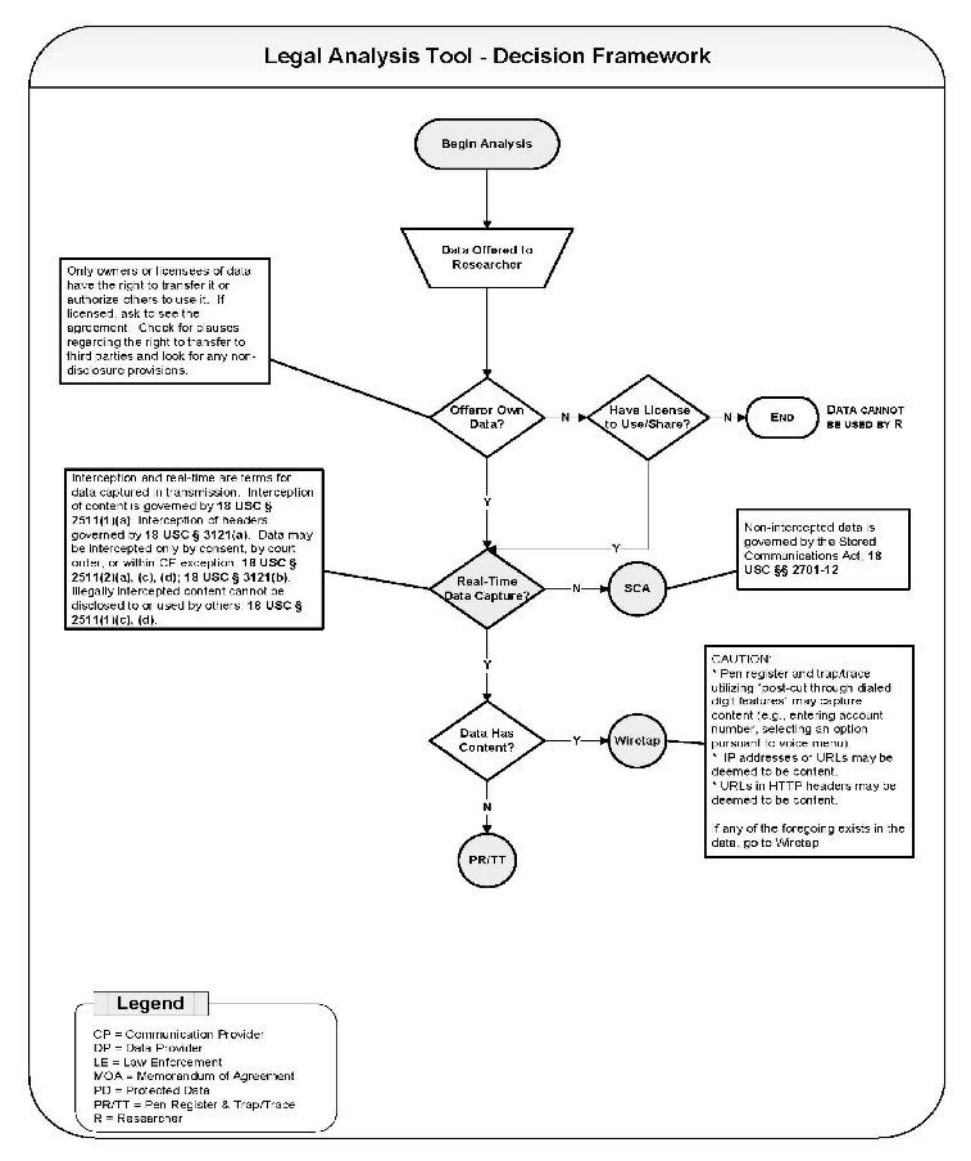
Simplified View

STORED COMMUNICATION ACT			CPNI or CPRI		
Provider	**Headers**	**Content**	**Provider**	**Headers**	**Content**
Private Provider Disclose	OK	OK	Private Provider Disclose	OK	OK
Private Provider Use	OK	OK	Private Provider Use	OK	OK
Public Provider Disclose to Others	OK –BUT Not to Gov't Entity C/ be CPNI or CPRI; If so use MOA	NO—USE MOA	Public Telecom or IP-Voice Provider Disclose Intercepted	NO—See Below	NO—See Below
Pubic Provider Use by Others	OK-BUT Not to Gov't Entity C/ be CPNI or CPRI; If so use MOA	NO—Use MOA	Public Telecom or IP-Voice Provider Disclose Stored	NO—See Below	NO—See Below

Sample Scenarios (truncated)

Scenario	Permitted Activity?	Pen Register/ Trap & Trace	Wiretap	Stored Comms	CPNI & CPRI	Comments
Researcher buys equipment to capture mirror images of packet headers as they pass by	OK, if device only captures headers; No, if device could capture content or is intended for content	Law silent; OK only to purchase or possess	NO, 18 USC §2512(b); illegal to possess device that can capture content	N/A	N/A	Unlike wiretap, PR/TT laws are silent on possession of PR/TT equipment
Researcher installs equipment to capture mirror images of packet headers as they pass by on network of private provider	NO	NO, 18 USC § 3121(a); Illegal to install PR/TT device w/out court order or consent	NO, If device c/ capture content;18 USC § 2512(b); Illegal to possess device that can capture content; 18 USC § 2511(a)	N/A	N/A; laws do not apply to private provider	Need court order or provider exception in 18 U.S.C. § 3121(b). Wiretap laws may be triggered if HTTP packets or other content

Legal Decisional Framework



Privacy Tool: Introduction

Even if Data is Determined to Have Been Legally Obtained &

May Be Legally Disclosed to Researcher &

May Be Legally Used by Researcher **.....**from Legal Analysis Tool

The Privacy Tool Steps Researchers Through Legal & Policy Considerations to Determiner:

- If Dataset Has Privacy Issues Associated With It
- Whether Issues Are Fatal and Preclude Use of Dataset
- Whether Issues May Be Mitigated or Eliminated Through Anonymization or Other De-Identification Techniques

Foreign Laws & Other Considerations

- Privacy Tool Based on U.S. Laws
- Discusses Foreign Privacy Issues, esp. EU
  - –Treatment of IP Addresses Within Data Protection Directive
  - – Processing of IP Addresses
  - – Proposed Changes to Data Protection Directive
- Global Data Protection Laws Chart
- Other Considerations
  - – Policies (Privacy & Operational)
  - – NDAs
  - – Contract Provisions
  - – Court Orders
  - – Administrative Rulings

Privacy Matrix (truncated)

Data Protected	Cable TV Priv Act	COPPA	Drivers Prot Act	FCRA	FERPA	GLBA	HIPAA
First Name	P	X	X	P		X	X
First Initial	P	P	X	P		X	X
Last Name	P	X	X	P		X	X
Address	P	X	X	P		X	X
City & State	P	X	X	P		X	X
Zip Code	P	X		P		X	X
County/Precinct	P	X	X	P		X	X
Country	P	X		P		X	X
Citizenship	P			P		P	P
Email Address	P	X		P		P	P

Privacy Analysis Worksheet

PRIVACY ANALYSIS WORKSHEET

Research Project:_____ **Page** _____ **of** _____
(complete for all pages)

Principal Investigator:_____
Date_____
(complete PI info only for initial page
Address:_____

_____

Email: _____
Telephone:_____

IRB Review Required: Y N
(circle Y or N)

Complete the following tables for each dataset to be used in R&D project

Name of Dataset: _____

PROTECTED DATA WITHIN DATASET

Indicate which *data elements* are believed to be contained in the dataset:

Data Elements Believed to be in Dataset	X	Description or Other Information About the Data	Data Elements Believed to be in Dataset	X	Description or Other Information About the Data
First Name			Certificate License #		
First Initial			Vehicle ID # or Serial #		

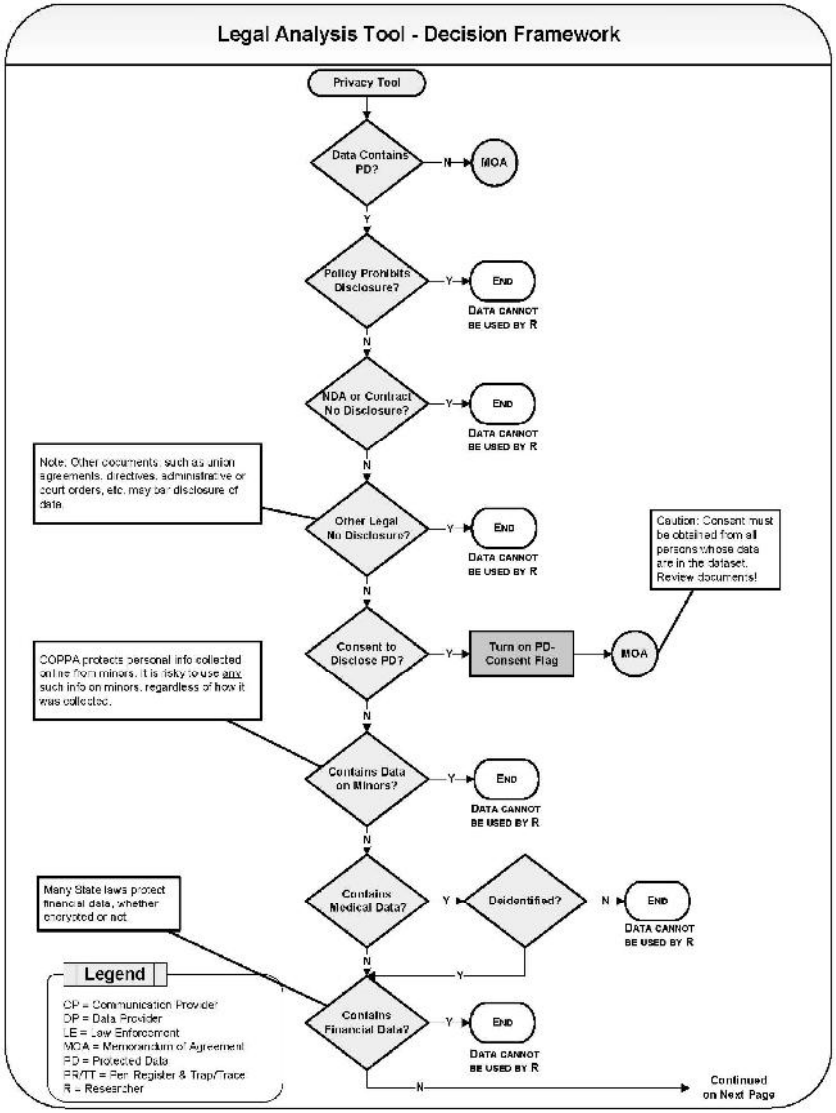
Privacy Analysis Worksheet

DATASET COMPLIANCE GUIDE

Complete blue columns for dataset if use is allowed — **Complete yellow columns**

Content of Dataset	Content X = Yes	Consent X = Y	Encrypted Or De-Identified? X = Y	Subject To Breach Laws? X = Y	OK To Use?	Anonymize or De-Identify? Y or N	Indicate suggested approach for anonymization or de-identification
Minors (< 13 yrs)					NO		
Medical Data					NO unless De-ID		
Financial Data					NO		
Veteran's Adm. Data					NO		
Credit Reporting Data					NO		
Government SOR Data					NO		
FERPA Data					OK if directory info		

Privacy Decisional Framework



Protection Measures Tool

- Brings Together Analysis from:
  - Legal Analysis Tool
  - Privacy Tool

  Using

  Decisional Framework Worksheet

  Privacy Analysis Worksheet

- Guides Researcher, IRB, Legal Counsel on Language for MOA Between Researcher & Provider and Privacy Clauses
- Provides Sample Policies for Researchers and Providers

Legal Guide to Cybersecurity Research on Botnets

- Beyond test data, cybersecurity R&D activities can also invoke a numerous legal considerations
  - Cybercrime
  - Intellectual property
  - Child pornography
  - Spam
  - Breach notification
  - Identity theft
  - Access device and wire fraud
  - Contract
  - Tort
  - Laws of other jurisdictions botnet involves (victim computers, dropzones, C/C)
- Analyzes 19 case studies of botnet research; summaries main research activities

Examples of R&D Activities With Legal Issues

- Infiltrating botnets and letting them run over live network, especially if involved in C/C functions may be aiding & abetting or willfully causing acts
- Infiltrate botnet and observe spam-related commands may be aiding & abetting
- Change a link in spam message to one under researcher's control to reduce harm may be actively perpetrating online fraud, directing spam operation, and sending commercial email messages to site they do not control
- Establish website to mimic those used by botnet may be infringing copyrights or removing or altering copyright management material
- Legal Guide lists tables of research activities, legal issues, & notes actions researcher may take to mitigate risk
- Sets forth laws and has table of laws and penalties

Relationship of Legal Analysis to Ethical Considerations

- Ethical considerations often based upon:
  - Whether benefits of research outweigh potential harms that may occur
  - Whether research activity is likely to engage in harmful acts
- Problem: “Beneficial” and “Doing No Harm” Not = Legal
- Many activities deemed “ethical” are illegal
- Illegal conduct is generally not viewed as ethical
- Research community at risk because another team engaged in similar activities and concluded they were legal, so others use original faulty legal analysis as justification for their own effort
- Little consideration given to international legal issues
- It is important that researchers undertake legal analysis first and after ensuring that the research activities are within the law, then proceed to examine ethical issues

Conclusion

Legal & Policy Tool Chest

Legal Guide to Cybersecurity
Research on Botnets

Companion Tools With
- Definitions
- Descriptions of laws
- Worksheets
- Decisional Frameworks
- Tables
- Conclusions

First comprehensive resources for researchers, IRBs, legal counsel, management

More needs to be done to examine international legal issues and simplify legal issues for researchers

Global Cyber Risk LLC

THANK YOU!

Jody R. Westby
westby@globalcyberrisk.com
+1.202.255.2700