

PREDICT Legal Aspects

**PREDICT Workshop
Newport Beach, CA
September 27, 2005**



***Douglas Maughan, Ph.D.
Program Manager, HSARPA
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170***



**Homeland
Security**

PREDICT Legal Process Activities

- Identify legal relationships and agreements needed between PREDICT participants
- Identify applicable laws and regulations (federal and state)
- Review policies and procedures and other available documents from providers
- Prepare risk chart
- Identify high risk data fields, datasets
 - ◆ Establish requirements for high risk fields
- Preparation of Memorandums of Agreement (MOAs)



Homeland
Security



27 September 2005

2

PREDICT Legal Process Activities

- Brief privacy advocates and obtain input
 - ◆ ACLU, Electronic Frontier Foundation (EFF), Center for Democracy and Technology (CDT), EPIC (invited)
- Prepare Privacy Impact Assessment (PIA)
 - ◆ Working with DHS Privacy Office
 - Will be posted on-line, once approved
- Brief government officials, privacy advocates, participants
 - ◆ DHS S&T General Counsel
 - ◆ DHS General Counsel
 - ◆ Department of Justice



Homeland
Security



27 September 2005

3

Table of Authorities

- Cable TV Privacy Act of 1984, 47 U.S.C. § 551, <http://www4.law.cornell.edu/uscode/47/551.html>
- Communications Act of 1996, Protection of Customer Proprietary Network Information, 47 U.S.C. § 222, <http://www4.law.cornell.edu/uscode/47/222.html>
- Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510-2521, <http://www4.law.cornell.edu/uscode/18/2510.html> (wiretap)
- Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2701-2708, <http://www4.law.cornell.edu/uscode/18/2701.html> (access to or disclosure of stored communications)



Table of Authorities (continued)

- Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 3123-3127,
<http://www4.law.cornell.edu/uscode/18/3123.html> (pen register and trap and trace devices)
- Family Education Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g,
<http://www4.law.cornell.edu/uscode/20/1232g/html>
- Freedom of Information Act, 5 U.S.C. § 552,
http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm
- Privacy Act of 1974, 5 USC § 552a,
<http://www.usdoj.gov/04foia/privstat.htm>



Existing Policies and Procedures

- Current Providers already had existing policies and procedures
- New Providers needed assistance developing access policies and procedure
- Review policies and procedures and other available documents from providers



Homeland
Security



27 September 2005

6

Dataset Risk Chart Example

Data Provider	Type of Data	Data Description	Documents Reviewed	MOA Provisions Specific to Data
University of Michigan	Blackhole Address Space Data	Meta-data will include info about the location of the address space being studied, the periods over which it is collected, any sampling performed on the data. Data will consist of information collected by monitoring dark or unused address space. Because the space is unused, any traffic destined to this space can be considered malicious or simply a misconfiguration.	<ul style="list-style-type: none"> -- IRB Submission -- CAEN Policies -- U-M Sponsored Uniqname Application & Compliance Agreement -- CAEN Confidentiality & User Certification -- Guidelines for Implementing the Proper Use Policy of U -M: Responsible Use of Technology Resources -- U-M General University Policies & Procedures 	<ul style="list-style-type: none"> -- Acceptable Use terms must be part of Researcher MOA -- IP addresses must be anonymized; no non-anonymized headers will be provided



PCC – Provider MOA

- They will make the data available to data hosts, for release to approved researchers and no others, under the terms and conditions for access and use as specified by them and the PCC.
- They will provide the PCC with metadata on the data they agree to make available and they will not provide any data or metadata to anyone other than those researchers approved by the PCC.
- They will provide **terms and conditions for access to and use of the data**, including identification requirements for the data custodian; permitted uses and specific restrictions; minimum safeguards to protect the data; procedures for receipt, handling, control, dissemination, and return of data; and restrictions on publishing or releasing information about the data (which is addressed below under Publication Review Board).
- **They are responsible for ensuring that any data they release complies with all applicable statutes and regulations of applicable governing or regulating bodies and contractual agreements and is consistent with the provider's privacy, security, or other policies and procedures.**
- They certify that the data provided for use in the PREDICT program has been sanitized, de-identified, or cleaned of any and all information that would not be in compliance or consistent with the privacy requirements as determined by PCC and DHS.
- Non compliance with these requirements may result in the data provider's expulsion from the PREDICT project.



Homeland
Security



27 September 2005

Privacy Impact Assessment (PIA)

- PREDICT Overview
 - Data collection activities
 - Identify privacy issues associated with data
 - Address how privacy issues will be addressed
-
- PIA



Homeland
Security



27 September 2005

9

Summary

- PREDICT is a national-level research resource that the cyber security community has really needed
- We believe we have addressed all of the legal and privacy issues that could have a negative effect on PREDICT and the availability of data
- Much of this documentation is (or will be) available on the PREDICT portal. If you don't find what you're looking for, please contact me directly.

End Goal: Improve the quality of defensive cyber security technologies



Homeland
Security



27 September 2005

10

Douglas Maughan, Ph.D.
Program Manager, HSARPA
douglas.maughan@dhs.gov
202-254-6145 / 202-360-3170



Homeland Security



Homeland
Security



27 September 2005

11