Tutorials for CFP 2009
Monday, June 1

8:00 – 9:00	Registration & Continental Breakfast (Room 302)			
9:00 – 10:30 & 10:45 – 12:15	Electronic Health Records (Room 309)	Constitutional Law in Cyberspace (Room 310)	Data Mining: Privacy, Transparency, Democracy (Room 307)	Twittering in the Trenches: Activism Using Social Networks (Room 308)
12:15 – 1:45	Lunch			
1:45 – 3:15	Online Advertising: Pulling Back the Curtain (Room 309)	Making NSA Security Work For You (Room 310)	Data Mining: Privacy, Transparency, Democracy (cont.) (Room 307)	Twittering in the Trenches: Activism Using Social Networks (cont.) (Room 308)
3:30 – 5:00	Fusion Centers vs. Privacy Silos (Room 309)	The Web is a Dangerous Place (Room 310)		
6:00 – 9:00	Opening Night Reception at Public Citizen ▪ 1600 20th St. NW Washington, DC, 20009			

Data Mining: Privacy, Transparency, Democracy (Full Day Tutorial)

This day-long tutorial will provide a basic tutorial on how data mining works, some common applications, and the privacy issues that are the focus of research both from a technical and policy perspective. This session will open up a vigorous discussion on some of the key issues in preparation for the main conference.

Agenda

9:00	Introduction
9:10	Introduction to Data Mining
9:40	Policy Discussion
10:00	Health Information & De-Identification Techniques
11:15	Current U.S. Health Issues
12:15	Lunch
1:45	Legal and Profiling Issues Panel
2:30	From Online Advertising to Facebook
3:30	Privacy Enhanced Data Mining Techniques
4:15	Discussion & Conclusions

Twittering in the Trenches: Activism Using Social Networks (Full Day Workshop)
Presenters: various

An all-day workshop organized by Deborah Pierce, Sarah Granger, and Shireen Mitchell. Morning keynote will be by Ari Melber. Tracks will focus on technology, policy, and privacy, and there will be an online component as well for those who can't attend in person. Results will be presented back to the main conference.

Constitutional Law in Cyberspace (AM – ½ day) Presenter: Mike Godwin, Wikimedia Foundation

This half-day morning tutorial is designed to inform participants about the constitutional issues that underlie computer-crime and computer civil-liberties cases, as well as policy issues relating to intellectual property and jurisdiction on the internet. Godwin will cover the basics of constitutional law in cyberspace, emphasizing free-speech and privacy issues, giving participants foundation in understanding how constitutional law applies to cyberspace.

Tutorials for CFP 2009
Monday, June 1

Electronic Health Records (AM – ½ day)
Presenter: Ashley Katz, Patient Privacy Rights

This half-day morning tutorial will provide an overview on the variety of ways electronic health records are used within the health care industry and the marketplace. The tutorial will explore questions including:

- What are the privacy implications for health information?
- What kinds of electronic medical records tools are out there and how is the information used?
- What is the secondary market for health data?
- What does HIPAA actually do?
- What are the ramifications of the health IT legislation passed in 2009?
- What should we do now?

Online Advertising: Pulling Back the Curtain (PM – ¼ day) Presenters: Douglas Miller, Executive Director and Deputy CPO, AOL; Jules Polonetsky, Co-Chairman and Director, Future of Privacy Forum; Anne Toth, Yahoo

This tutorial will provide an overview of how advertisers, publishers, ad networks, search engines and other business models use data for tracking, analysis and targeting. Special attention will be given to the nuts and bolts of cookie use, IP address use, log-file mining and behavioral profiles.

Fusion Centers vs. Privacy Silos (PM – ¼ day) Presenters: Frank Pasquale; Danielle Citron, Professor at University of Maryland; Priscilla Regan, Professor in the Department of Public and International Affairs at George Mason University

This tutorial will examine the emerging legal and policy issues surrounding state-run fusion centers and address the question: What laws address the aggregation of medical, financial, criminal, library and other records?

Fusion centers maintain computer systems that collect and analyze tips and personal information obtained from the public sector (e.g., Social Security numbers, criminal records, etc.) and private companies (e.g., unlisted cell phones, credit reports, employment records, location and tracking data from private security cameras, etc.). The fusion centers, which are federally funded, produce system-generated intelligence that is shared with state and federal agencies.

The Web is a Dangerous Place (PM – ¼ day)
Presenter: David Campbell, Open Web Application Security Project (OWASP)

The World Wide Web is a dangerous place. As companies and government agencies have become more competent at vulnerability management, politically and/or financially motivated attackers have refocused their efforts on softer targets such as web applications and end-user web browsers.

This tutorial will provide the attendee with hands-on demonstrations of how vulnerable most web applications are and how vulnerabilities in the sites you visit can compromise your privacy and security. During this session, Campbell will discuss the evolution of web applications and show how application-layer vulnerabilities can completely subvert even the best designed security solutions.

Best practices and technologies for mitigating these new classes of vulnerabilities will also be discussed, and Campbell will provide specific guidance for individuals seeking to protect themselves from insecure web applications and web-borne malware.

Making NSA Security Work For You (PM – ¼ day) Presenter: John M. Willis, President and Principal Consultant for pINFOSEC.com.

In this tutorial, participants will learn how to take their personal information protection to the next level by applying information security methodologies developed by the NSA. Participants will learn techniques of mapping personal data classification, information flows, and layered defenses and gain clear understanding of anonymity, pseudonymity and asset protection issues with respect to personal information protection.

What information do others see about your personal life? Companies and other third parties that are entrusted with individuals' private information will be discussed, and a list of questions for these third parties will be provided to assist in assessing vulnerabilities and determining who to do business with.

Willis will also discuss techniques for testing the actual security of one's personal information in the possession of third parties. The tutorial will also address legal and policy issues pertaining to this privacy penetration testing.