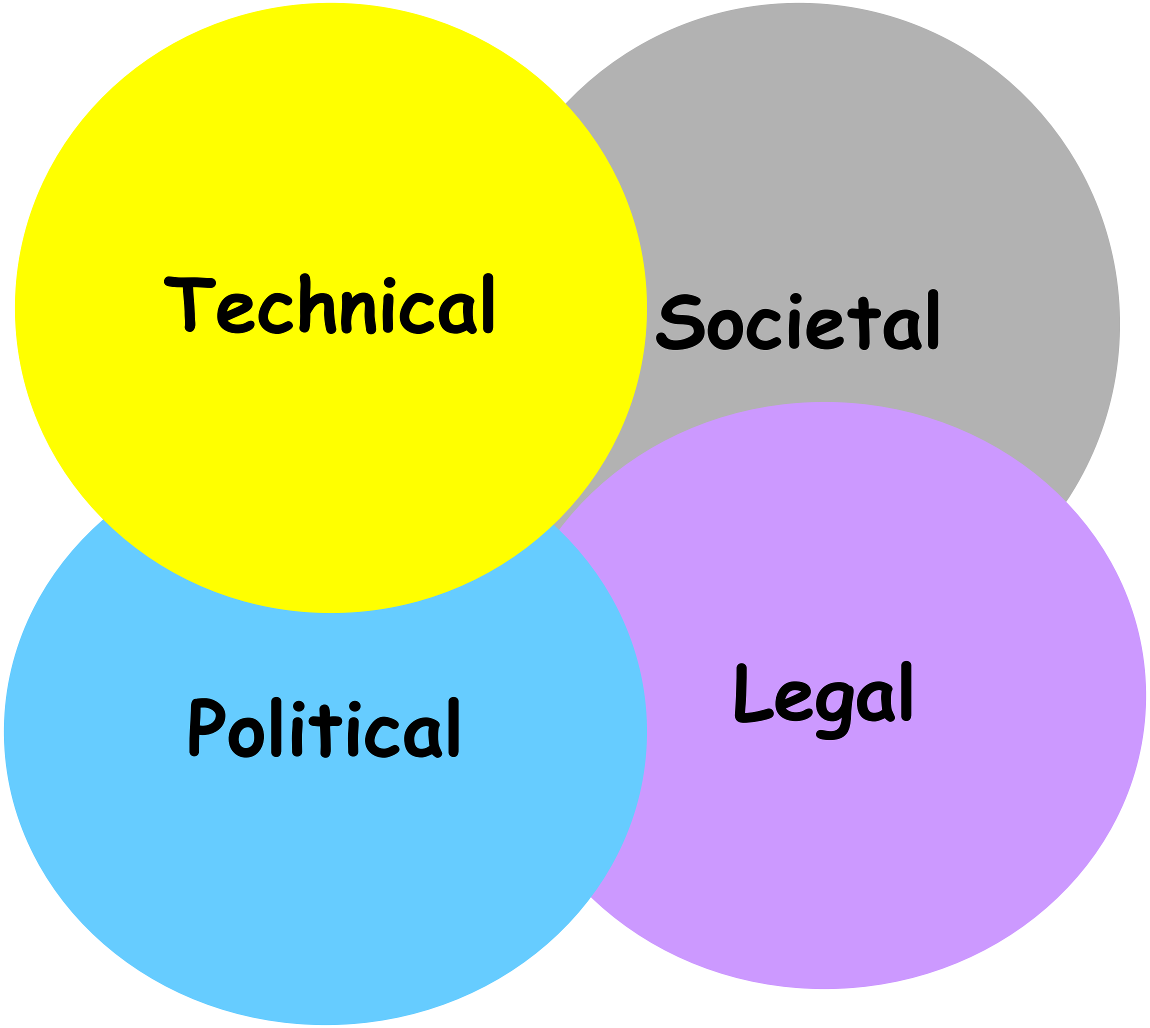
Privacy: Technical Challenges

Jeannette M. Wing

Assistant Director
Computer and Information Science and Engineering Directorate
and
President's Professor of Computer Science
Carnegie Mellon University

Data Confidentiality Workshop, September 6, 2007, Arlington, VA

Aspects to Privacy



Broader Context: Trustworthy Systems

- Trustworthy =
  - + Reliability
    - Does it do the right thing?
  - + Security
    - How vulnerable is it to attack?
  - + **Privacy**
    - Does it protect a person's information?
  - + Usability
    - Can a human use it easily?

Technical Progress: Reliability

- Formal definitions, theories, models, logics, languages, algorithms, etc. for stating and proving notions of correctness.
- Tools for analyzing systems—from code to architecture—for desired and undesired properties
- Use of languages, tools, etc. in industry.
  - "Reliable" [= "good enough"] systems in practice: POTS, the Internet, desktop software, your automobile
- Examples:
  - Strongly typed programming languages rule out entire classes of errors.
  - Database systems are built to satisfy ACID properties: atomicity, consistency, isolation, durability
  - Byzantine fault-tolerance, $n > 3t+1$
  - Impossibility results, e.g., distributed consensus with 1 faulty node

Current challenge: Nature and scale of systems and their operating environments are more complex, forcing us to revisit these fundamental results. E.g., cyber-physical systems, safety-critical systems.

Technical Progress: Security

- Formal definitions, theories, models, logics, languages, algorithms, etc. for stating and proving notions of security.
- Tools for analyzing systems—from code to architecture—desired and undesired properties
- Use of languages, tools, etc. in industry.
  - Secure [= "secure enough"] systems in practice: POTS, the Internet, desktop software, your automobile *(today)*
- Examples:
  - Cryptography
  - Systems designed to satisfy informally CIA properties (confidentiality, integrity, availability).
  - Logic of authentication [BurrowsAbadiNeedham89], logic for access control [LampsonAbadiBurrowsWobber92]

Current challenges: (1) Assumptions have changed; revisit the blue. (2) Fill in the gray. (3) Nature and scale of systems and their operating environments are more complex, forcing us to revisit the fundamentals E.g., today's crypto rests (mostly) on RSA, i.e., hardness of factoring.

Technical Progress: Privacy

?

Examples:

- K-anonymity [Sweeney02], [Williams04]
- Privacy-preserving data mining [DworkNissam04]
- Private matching [LiTygarHellerstein05]
- Privacy policy language [BarthDattaMitchellNissenbaum06]
- Privacy in statistical databases [Fienberg et al. 04, 06]

Extracting Confidentiality Properties from Source Code [TshantzWing07]

- Property: *Incident-Insensitive Non-Interference*
  - Motivation
    - Clerks and doctors can see different parts of a patient record
    - Students can submit grad school applications on-line
  - Strictly weaker than Goguen-Meseguer non-interference
  - Not expressible in terms of standard temporal logics

- Approach
  - Rather than show code satisfies a given IINI policy,
  - Extract the program-specific IINI policy from code
    - On-going: All-counterexamples model checking algorithm, program dependence graph analysis, symbolic execution
  - User (or tool) validates extracted policy

- Future work: change-impact analysis

Privacy: A Few Questions to Ponder

1. What does privacy mean?

2. How do you state a privacy policy? How can you prove your system satisfies it?

3. How do you reason about privacy? How do you resolve conflicts among different privacy policies?

4. Are there things that are impossible to achieve wrt some definition of privacy?

5. How do you implement practical mechanisms to enforce different privacy policies? As they change over time?

6. How do you measure privacy? (Is that a meaningful question?)

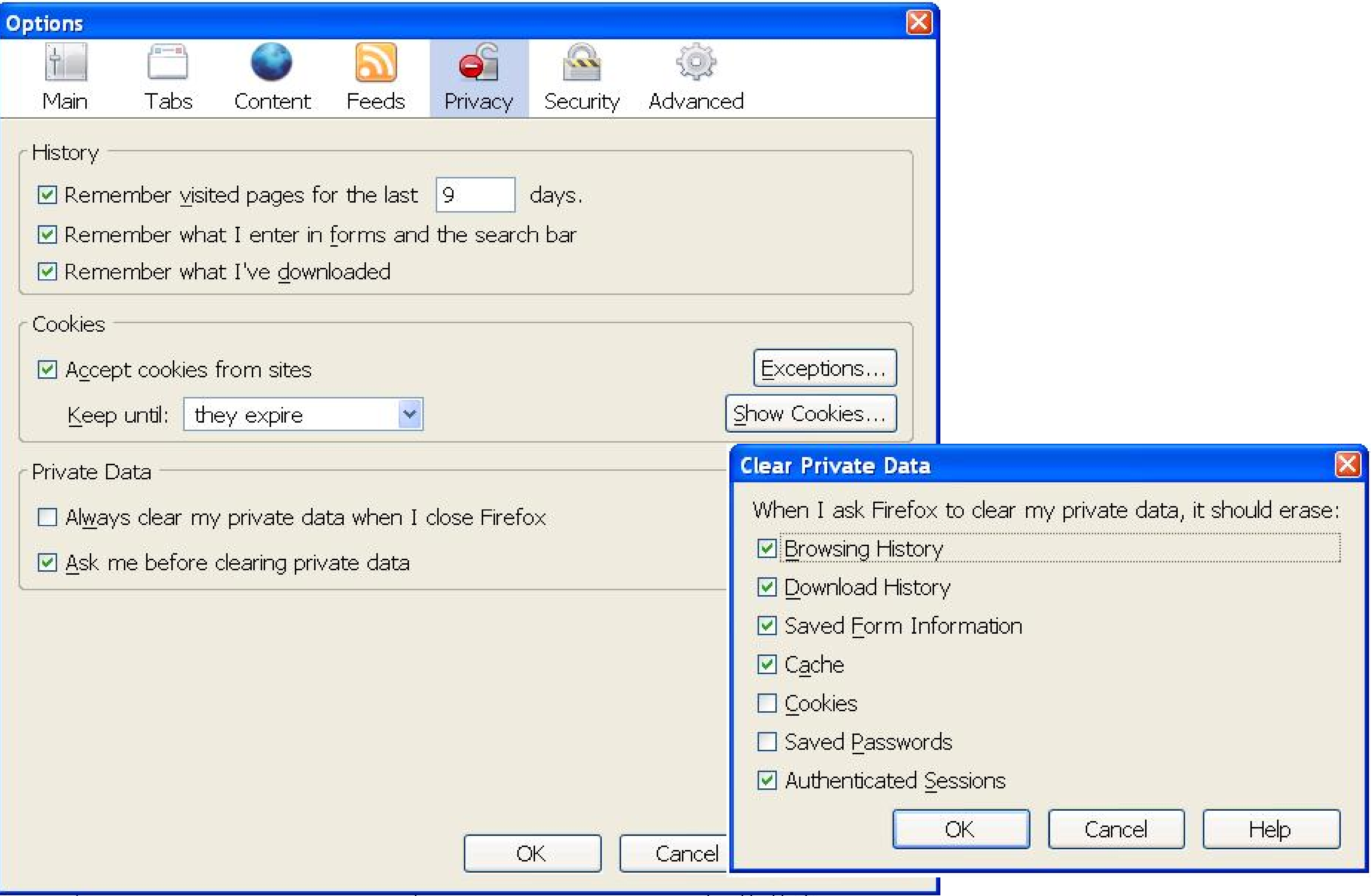
Issues to Consider

- Compositionality
  - Components A and B, privacy policies P_1 and P_2
    - $A \models P_1$, $B \models P_2 \Rightarrow A \oplus B \models P_1 \& P_2$?

- Complexity of systems today and tomorrow
  - Dynamic: in time and space
  - Borderless: physical and cyber
  - Unpredictable: Human, Mother Nature, The Adversary

- Tradeoffs
  - Privacy and {security, reliability, usability}
  - Technical and {societal, legal, political}

Clicking Your Way Through Privacy (Firefox)



History

☑ Remember visited pages for the last 9 days.

☑ Remember what I enter in forms and the search bar

☑ Remember what I've downloaded

Cookies

☑ Accept cookies from sites

Keep until: they expire

Private Data

☐ Always clear my private data when I close Firefox

☑ Ask me before clearing private data

When I ask Firefox to clear my private data, it should erase:

☑ Browsing History

☑ Download History

☑ Saved Form Information

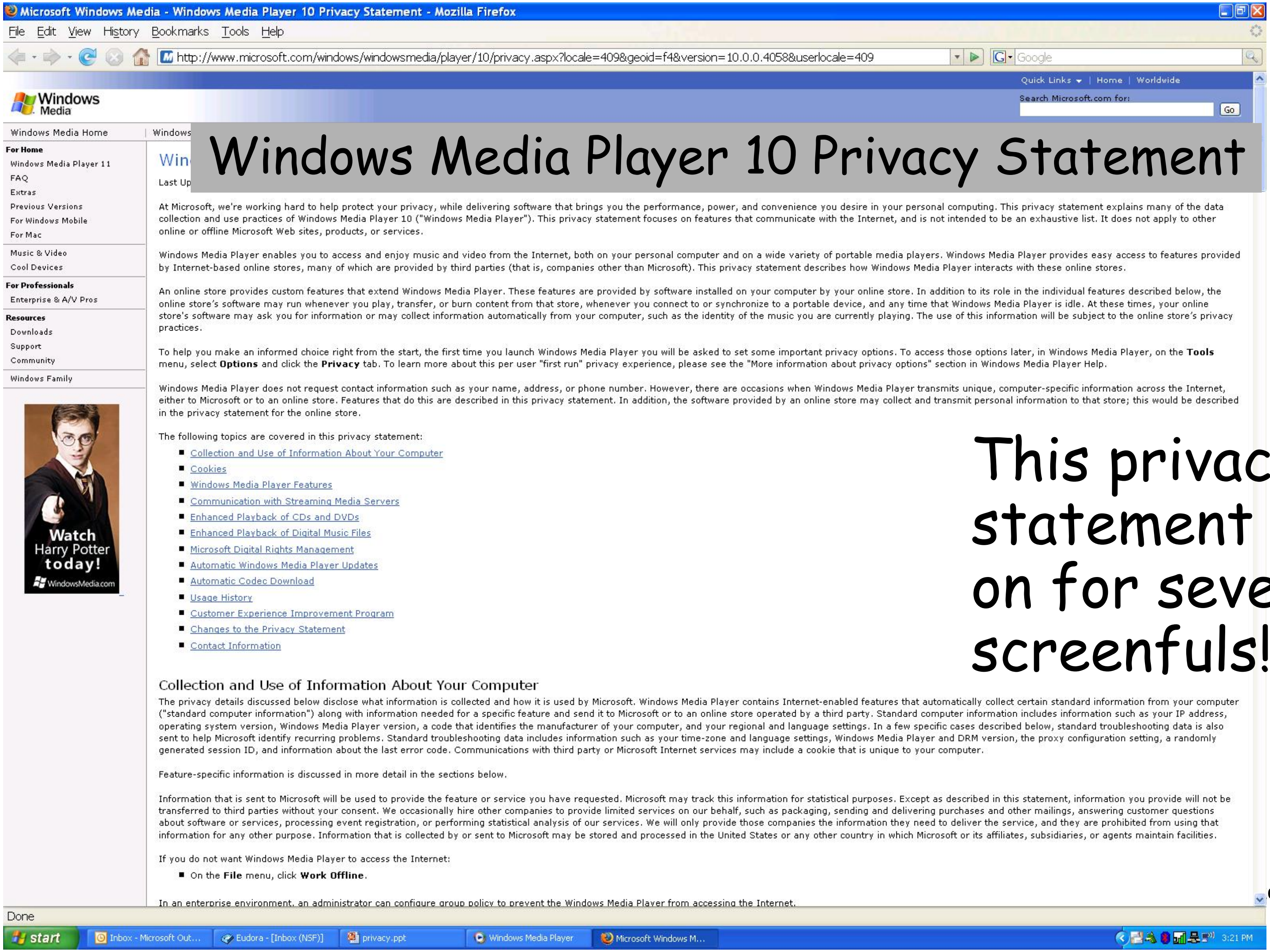
☑ Cache

☐ Cookies

☐ Saved Passwords

☑ Authenticated Sessions

Do You Read These? What Are They Saying?


Microsoft Windows Media - Windows Media Player 10 Privacy Statement - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.microsoft.com/windows/windowsmedia/player/10/privacy.aspx?locale=409&geoid=f4&version=10.0.0.4058&userlocale=409
Google
Quick Links | Home | Worldwide
Search Microsoft.com for:
Go
Windows Media
Windows Media Home | Windows
For Home
Windows Media Player 11
FAQ
Extras
Previous Versions
For Windows Mobile
For Mac
Music & Video
Cool Devices
For Professionals
Enterprise & A/V Pros
Resources
Downloads
Support
Community
Windows Family
Watch Harry Potter today!
WindowsMedia.com
Win
Last Up
Done
start
Inbox - Microsoft Out...
Eudora - [Inbox (NSF)]
privacy.ppt
Windows Media Player
Microsoft Windows M...
3:21 PM

Windows Media Player 10 Privacy Statement

At Microsoft, we're working hard to help protect your privacy, while delivering software that brings you the performance, power, and convenience you desire in your personal computing. This privacy statement explains many of the data collection and use practices of Windows Media Player 10 ("Windows Media Player"). This privacy statement focuses on features that communicate with the Internet, and is not intended to be an exhaustive list. It does not apply to other online or offline Microsoft Web sites, products, or services.

Windows Media Player enables you to access and enjoy music and video from the Internet, both on your personal computer and on a wide variety of portable media players. Windows Media Player provides easy access to features provided by Internet-based online stores, many of which are provided by third parties (that is, companies other than Microsoft). This privacy statement describes how Windows Media Player interacts with these online stores.

An online store provides custom features that extend Windows Media Player. These features are provided by software installed on your computer by your online store. In addition to its role in the individual features described below, the online store's software may run whenever you play, transfer, or burn content from that store, whenever you connect to or synchronize to a portable device, and any time that Windows Media Player is idle. At these times, your online store's software may ask you for information or may collect information automatically from your computer, such as the identity of the music you are currently playing. The use of this information will be subject to the online store's privacy practices.

To help you make an informed choice right from the start, the first time you launch Windows Media Player you will be asked to set some important privacy options. To access those options later, in Windows Media Player, on the **Tools** menu, select **Options** and click the **Privacy** tab. To learn more about this per user "first run" privacy experience, please see the "More information about privacy options" section in Windows Media Player Help.

Windows Media Player does not request contact information such as your name, address, or phone number. However, there are occasions when Windows Media Player transmits unique, computer-specific information across the Internet, either to Microsoft or to an online store. Features that do this are described in this privacy statement. In addition, the software provided by an online store may collect and transmit personal information to that store; this would be described in the privacy statement for the online store.

The following topics are covered in this privacy statement:

This privacy statement goes on for seven screenfuls!

Collection and Use of Information About Your Computer

The privacy details discussed below disclose what information is collected and how it is used by Microsoft. Windows Media Player contains Internet-enabled features that automatically collect certain standard information from your computer ("standard computer information") along with information needed for a specific feature and send it to Microsoft or to an online store operated by a third party. Standard computer information includes information such as your IP address, operating system version, Windows Media Player version, a code that identifies the manufacturer of your computer, and your regional and language settings. In a few specific cases described below, standard troubleshooting data is also sent to help Microsoft identify recurring problems. Standard troubleshooting data includes information such as your time-zone and language settings, Windows Media Player and DRM version, the proxy configuration setting, a randomly generated session ID, and information about the last error code. Communications with third party or Microsoft Internet services may include a cookie that is unique to your computer.

Feature-specific information is discussed in more detail in the sections below.

Information that is sent to Microsoft will be used to provide the feature or service you have requested. Microsoft may track this information for statistical purposes. Except as described in this statement, information you provide will not be transferred to third parties without your consent. We occasionally hire other companies to provide limited services on our behalf, such as packaging, sending and delivering purchases and other mailings, answering customer questions about software or services, processing event registration, or performing statistical analysis of our services. We will only provide those companies the information they need to deliver the service, and they are prohibited from using that information for any other purpose. Information that is collected by or sent to Microsoft may be stored and processed in the United States or any other country in which Microsoft or its affiliates, subsidiaries, or agents maintain facilities.

If you do not want Windows Media Player to access the Internet:

- On the **File** menu, click **Work Offline**.

In an enterprise environment, an administrator can configure group policy to prevent the Windows Media Player from accessing the Internet.

Why This is Important for Society

- Timely
- What companies, including non-IT, want and need
- What policymakers and lawyers need
- It's an international, not national issue
  - E.g., Germany's privacy laws, globalization of corporations
- Our role as scientists in society

NSF/CISE Relevant FY08 Programs

- Cyber Trust: Late 2007
- Information Integration and Informatics: Oct 23, Nov 19, Dec 10, 2007
- Theoretical Foundations, Winter 07-08
- New FY08: Foundations of Data and Visual Analytics, Nov 20, 2007

Thank you!