

# Lecture 13: Privacy and Security; E-commerce

## Privacy

Two basic threats to privacy: government and business.

Should government have access to certain types of information? Privacy vs. safety (counter-terrorism)

Business access to information: good or bad? Targeted advertisements.

US has pretty weak privacy regulation.

Opt-in vs. opt-out

## Cookies

Cookies are small text files, stored on your computer by a server. They are used to maintain information between page requests to the server - for example, to maintain the contents of a shopping cart.

Problem with cookies: *third-party cookies* A web site may contract with an ad agency to place ads on its page. When you visit the server, it sends a request to the ad agency to display an ad - but then it is suddenly allowing that ad company to place a cookie on your computer, without your realizing it. If you later visit a different Web server that contracts with the same ad agency, it will be able to retrieve those cookies and the ad agency will now know which other companies you interacted with.

You can change the browser settings to deny cookies, or to warn you when cookies are being stored.

## E-Commerce - Secure Transactions

Information sent over the Internet can be intercepted by a third party, so credit card numbers might be collected. To keep information secure, it must be **encrypted**.

**SSL**- Secure Socket Layer protocol for secure transactions. Web pages using this protocol are accessed using https.

SSL uses **certificates** to verify that a Web server is really what it claims to be.

## Email

Email is NOT secure. PGP can be used to encrypt email messages.