Privacy Inalienability and Spyware/Adware

Prof. Paul Schwartz
Visiting Professor, Boalt Hall, UC Berkeley
Anita and Stuart Subotnick Professor, Brooklyn Law School
Boalt Hall Spyware Conference, April 1, 2005

What is privacy inalienability?

- Susan Rose-Ackerman– an inalienability is a restriction on the transferability, ownership or use of an entitlement
- Is it possible to set up a model for propertization of personal data that safeguards info privacy?
- Need for restrictions on an individual's ability to trade information

What does this topic have to do with spyware/adware?

- Alienability, or a right to trade data, has not yet emerged as a policy issue in this context
- No notice, no free choice
- But what if H.R. 29 is enacted?
- Why not then let people sign up to trade their personal data online?



My Model

1. Inalienabilities, including use-transfer restrictions
2. Defaults
3. Rights of exit
4. Damages
5. Institutions

Property, Privacy and Personal Data, 117 Harv. L. Rev. 2055 (2004)

What About Spyware and Adware?

- No need for outright ban on data trade in context of adware (contrast with implantable chips)
- Potential weakness, however, of pure notice-and-consent approach– hence, need for use-transfer restrictions
- Need for right of exit– in this context, right to disable the data collection software

What about H.R. 29 (the SPY ACT)?

- Excellent sharpening of notice-and-consent approach ("This program will collect and transmit information about you.")
- Use-transfer restriction? Subsequent notice if information collected or sent that is of a type or for a purpose that is materially different"
- Right of exit-- required functions include "disabling function"
- Damages– high penalties set
- Institutions– FTC to enforce Act. Private right of action not included

- Thank you!