

# Electronic Commerce

Stephen J. Turnbull

Economics

Lecture 18: May 29, 2008

## Abstract

Today we consider the issues of taxation on the Internet, and discuss security.

Brief list of chapters for 2d midterm: 9–13, part of 19, 16, 17, maybe 18.

# Advantages of a common market

Read Ch. 17 of Deak, *The Taxation of e-Commerce*.

- Economies of scale in economic bureaucracy
  - One accounting system, economies for *taxpayers*
  - Elimination of redundancy among *taxcollectors* (not realized!)
- Elimination of customs and tariff barriers
  - What about *weigh stations*? – highway maintenance
- Scheduling, location, and route flexibility
  - Substitute transport across boundaries for warehouses in each region

# Role of regions in a common market

- Goods are *geographically differentiated*
  - Personal services (more generally, labor) “are where” the supplier is
  - High transport cost/value ratio
  - Informational frictions at moderate transport cost/value ratio
- “Single tax” (Henry George, refers to tax on *land*) is perfectly adapted, the land in the region doesn’t move
  - But in modern economic quasi-rents are at least as big, want to tax corporate profits and high-income individuals, too
- Above frictions allow tax differentials by region

# Role of Internet in a common market

- Reduction of “frictions”
  - Interregional service delivery by Internet at marginal cost zero
  - Reduction of interregional information frictions: marketing, search, ordering
  - Reduction of financial frictions (efficient payment systems)
- **Location identification** of an Internet event is *impossible*: if the cost of transport is *zero*, how do you decide whether the customer visited the vendor, or the vendor visited the customer?
  - And where is the vendor (customer), anyway? Where the head office (residence) is? Where the server (client) host is?

# Effect of Internet on regional taxation regimes

- Punch line: avoidance a la offshore enterprises, jurisdiction conflicts, externalities (“race to the bottom”) a la European Union
- **Tax avoidance:** vendor/customer claims “this trade is not taxable in your jurisdiction” to vendor’s region and customer’s region at the same time!
- **Jurisdictional conflict:** different regions claim the exclusive right to tax a particular trade

# U.S. tax law and the Internet

- Definitions: tax on *income vs. tax on output* (**sales tax, VAT**)
  - Income tax easier to assign to entity, but bad incentive effects; output tax has bad distributional effects (*regressive*)
- Definitions: tax on *gross final output* (**sales tax**) vs. tax on *net intermediate output* (**VAT**)
- **Interstate commerce clause** prevents states from taxing *sales* in other states
  - Congress and the courts decided that there must be a **physical nexus linking the vendor and customer in a state**, such as a store, then mail-order transactions can be taxed even if they don't involve a visit to the store
  - Avoid tax by buying in a low-tax state and bringing it home

to a high-tax state (*cf.* cigarette and liquor smuggling even today)

– Alternative: **use tax** depends on self-reporting by consumers

- *Triangle* transactions: customer in NY pays company in CA, takes delivery from warehouse in Kentucky; who can tax?
- States started creating various special Internet taxes on the grounds that the presence of the Internet created a **nexus** between vendor and customer in a state, Congress said “no way, that’s our job” and pass the *Internet Tax-Freedom Act* (ITFA)
  - Primary rationale is to avoid killing the infant industry via the **tragedy of the anti-commons**

# Basic concepts of network security:

## Networks

- Networks are composed of **nodes** and **links**
  - **Nodes** are usually *general-purpose computers*, but may not provide services other than network routing—nevertheless, they are powerful enough to be worth subverting
  - **Links** are transmission channels, which may be wires, fiberoptics, or wireless
- Signals can be stolen from links; this is hard (but not impossible) with wired or fiberoptic links, relatively easy with wireless
- Usual point of attack are the *nodes*, including **hosts** (providing general services to clients and servers) and **gateways**, which do routing

# Basic concepts of security: Access

**Access** is granted based on three concepts

- A **user** must be **identified** as trying to get access
  - Users may be humans, ...
  - ... or computer programs (*e.g.*, a file sharing program or a virus)
  - From the security perspective, the important thing about users is that they have different sets of **access rights** (files, programs, *etc.*)
- The user must *prove his identity* to be **authenticated**
- The authenticated user is checked to see if they have **authorization**

# Mirror images: Privacy and security

- When we think of computer security, we usually think of the evil hacker trying to break into our computer ...
- ... but on the Internet we are often in the position of leaving our unlocked briefcase on the coffee table while we're in the restroom, and what is our host doing?
- Consider a time-sharing system with a wordprocessor (rather than personal computers)
  - Setting: the faculty dictate to staff for bulk input, and then edit themselves for final touches
  - But one professor decides to write a memo complaining about a secretary using the wordprocessor, and “just saves” the file in the shared folder ...

- ... where the target sees it and reads it! Oops ...
- Any service you use on the Internet is potentially like that!