Solutions to Homework 3

Please note that some of the following solutions contain more information than you needed to provide to receive full credit. Others only provide examples, rather than an exhaustive list, of correct answers.

1. eBay AND ITS LEGAL RESPONSIBILITIES (25 points)

Arguments that one could make in favor of eBay's being held responsible for (at least some) illegal acts that eBay users profit from include but are not limited to:

- The fact that eBay was designed simply to be a "venue" for commerce, *i.e.*, to facilitate others' buying and selling things rather than to buy and sell things itself, does not automatically mean that it bears no responsibility for the acts that it facilitates. There are many situations in which the law holds people and companies responsible for facilitating illegal acts. For example, Napster was sued successfully (and ultimately shut down) because it facilitated copyright infringement.

- Although it is true that it would be technically infeasible for eBay to "vet" the legitimacy of all of its users and of all of the transactions that they engage in, one might still be able to define a set of circumstances under which it would be technically feasible for eBay to intervene in order to prevent an illegal act. For example, auctions of certain classes of items in which there is known to be a great deal of illegal traffic could be flagged automatically, and then a person could look at them and either shut them down (if they are obviously illegal) or notify appropriate law-enforcement personnel (if it's unclear whether they are illegal). Such a procedure would not catch all illegal transactions, but it might catch a reasonable number of them, and one could argue that eBay should be held responsible for making this type of good-faith effort not to facilitate crimes. It could work with law enforcement in order to figure out which classes of transactions could be screened for and flagged by a computer program before a human intervenes.

- From a moral point of view (and a public-relations point of view as well), eBay should try to avoid facilitating or giving the appearance of facilitating illegal acts. If there are technically feasible and reasonable actions that it can take to prevent such acts or to stop them once they've started, then these actions should be part of eBay policy.

Arguments that one could make in favor of eBay's not being held responsible for any illegal acts that eBay users profit from include but are not limited to:

- The fundamental technological reason that eBay is so popular and profitable is scalability. Having designed and launched a good website, eBay can just let technology (*i.e.*, scalable Internet protocols) and economics (*i.e.*, network effects) do the job. There is nothing in the business model that requires eBay employees do any per-customer or per-transaction work. If holding eBay legally responsible for the actions of its customers changed that fundamental fact, then its spectacular scalability (and popularity and profitability) would be undermined.

- Law enforcement agencies (from any country in the world) are already free to peruse the eBay website and to contact the participants in what appears to be illegal activity. They should not expect eBay to do their work for them.

- It might be reasonable to expect eBay to post clear guidelines for users that discourage illegal activity, but ultimately it is the users who do something illegal who should be prosecuted, not eBay.

- It is not clear that there is much useful action eBay could take by way of crime-prevention and still remain a successful C2C business. For example, if users had to have their "identities" verified before they could buy and sell items, they would have to wait days or even weeks between first noticing something enticing on the web site and actually trying to buy it (or between having the impulse to sell something and actually posting it for sale). Such a delay would cut down drastically on the number of users, and that would in turn cut into (or even reverse) the network effects that eBay's success relies on. We do not expect shoppers to have to go through a vetting process before entering a mall, and it seems clear that shopping malls would be much less plentiful and much less useful if one could not simply walk into them and buy things. Furthermore, eBay users live in many different countries, and each country has a different notion of "proof of identity." How could eBay establish procedures for verifying all of these different types of proofs efficiently and remotely? Without traceable users who could be arrested if they did something illegal, it is not clear what an online business can do by way of policing. There is no standard procedure (much less widely available software) for doing the automatic classification of transactions into high risk and low risk of being illegal that is suggested above.

2. PORTALS AND PRIVACY (35 points)

A. Encryption can be used to provide confidentiality while data are in storage or in transmission. It is already used by some standard Internet protocols (*e.g.*, SSL) to protect transaction data (*e.g.*, credit-card numbers and passwords) that are transmitted when customers interact with websites such as Amazon, eBay, *etc*. Privacy-conscious companies could guarantee to customers that they would go beyond encryption of transaction traffic between customer and website and, for example, store only encrypted versions of personally identifying information in their customer databases. The downsides of encryption are that (1) key management imposes costs and is easy to get wrong, and (2) it is not the silver bullet that it sometimes appears to be. For example, data generally have to be decrypted in order to be used, and once they are in the clear they can be misused. Furthermore, a large fraction of data theft and misuse is attributable to "insider attacks" by people who have legitimate access to decryption keys in the course of their jobs but betray the company and its customers (*e.g.*, in anger at the company or in exchange for financial gain).

Digital signatures can ensure provenance of data transmitted from the customer to the portal or vice versa. Secure and correct use of signatures could obviously prevent impersonators from corrupting the portal's databases of customer information, from luring customers to spoofed websites that collect and misuse personal data, or from foisting harmful traffic onto a customer. However, secure and correct use of signatures is technically nontrivial – in particular, the signature keys of companies are subject to insider theft just as encryption keys are, and individuals have no obvious "secure" place on their personal machines in which to store signature keys. (Efforts such as the Microsoft Next-Generation Secure Computing Base discussed in LaMacchia's lecture may change that and lead to wider use of signatures.) Furthermore, unlike companies and other large organizations, individuals have so far had little motivation to acquire certificates. As discussed above in the answer to Question 1, commercial websites do not generally require individuals to "prove their identity" before they use the service, and it is unclear that requiring such proof would be compatible with successful Internet business models.

The ways in which P3P can be used to provide customer privacy are explained on pages 35-45 of Lorrie Cranor's lecture notes. (See the February 18 entry of the "schedule, lecture notes, and handouts" page of the class website.) However, it is unclear to what extent a portal company could build a privacy-enhancing business around P3P for several reasons, including but not limited to: (1) It is unclear how many users would actually have both the skill and the patience to specify their privacy preferences correctly (*i.e.*, many people say that privacy is important to them but give incomplete or even contradictory answers when probed about exactly what "privacy" means to them); (2) P3P can help to match up the privacy policy of a website with the privacy preferences of a user, but it cannot ensure that the website actually enforces its privacy policy consistently.

The ways in which standard HTTP and cookies convey information about users are explained on pages 5-9 of Cranor's lecture notes. A portal company that wanted to differentiate itself by promising privacy preservation could, of course, make only "legitimate" use of this information that customers reveal through HTTP requests and cookies. However, it could not stop other websites that users visit without first going through the portal from misusing this information, and that might make this whole business strategy unworkable (see part B below).

The use of DRM-like technology to protect users' private data is discussed in Brian LaMacchia's lecture notes. (See the March 27 entry of the "schedule, lecture notes, and handouts" page of the class website, particularly page 28 but also the preceding discussion.) There are at least two main problems with a portal company's relying on it, however. First of all, the use of DRM-like technology to protect user privacy requires that users be able to specify their privacy policies; it is unclear that they have the skill and the patience to do this (just as it is unclear that they have the skill and the patience to use P3P correctly). Second, even if DRM-like technology prevented a company's software from misusing a customer's data, some of that data (*e.g.*, address and social-security number) is succinct enough for an "inside attacker" simply to write it down and type it into a machine not owned by the company or controlled by the company's privacy policy.

B. The main argument in support of the proposition that aggressive privacy protection could be a successful business strategy for a portal company is the obvious one: Surveys and other indicators show that there is strong and growing concern about identity theft, deluges of spam and telemarketing, and other misuses of electronic data records. Thus, in principle, a portal company should be able to attract customers if it: (1) delivers the same quality of service with respect to content delivery, shopping opportunities, personalization, *etc*. that, say, Yahoo! delivers, (2) measurably improves the user experience from the privacy point of view (*e.g.*, measurably reduces the amount of spam and telemarketing that the user has to deal with), and (3) convinces users that it is responsible for the improvement.

The main argument against the proposition that this would be a successful business strategy is that (1), (2), and (3) would probably be very difficult to achieve – perhaps even impossible. The privacy-preserving technologies available to portal companies often create inconvenience for users or degrade quality of service; although users say that they are concerned about privacy, there is little evidence that they are willing to sacrifice convenience or quality of service in order to obtain it. Furthermore, even a portal company that deploys the best privacy-enhancing technology and does not itself cause violations of customer privacy cannot guarantee that customers will experience improvement. These customers might visit privacy-violating websites that they do not get to via the portal or might reveal personally identifying information in settings other than the Internet; if these actions result in privacy violations, customers may feel as though the portal company's promise of privacy has been broken. Finally, the same factors that make it difficult for even the most conscientious portal company to prevent violations of its customers' privacy make it difficult for that company to demonstrate that improvements in customers'

privacy are attributable to the company's efforts. A decrease in spam might be the result of changes in Federal Trade Commission policy or law-enforcement efforts rather than the portal company's efforts. Making a case to customers that one has provided a certain number of "units of privacy" for which one is charging a certain price per unit is probably infeasible. (Econ students should recognize the classical "moral-hazard" and "principal-agent" problems.)

3. VENTURE CAPITAL (20 points)

A. Investor's shares / Total shares = Investment / (Pre-money V + Investment)
⇨ 50 / (100+50) = Investment / (2M + Investment)
⇨ Investment = 1M

For parts B and C:
N1 = Founder's shares in first round = 100
N2 = Investor's shares in first round = 50
N3 = Additional shares = 10
p1 = Price of the shares in first round = 10
p2 = New price = 2
q = Parameter determined by calculation method

B. Weighted ratchet:
$q = (N1*p1 + N3*p2) / (N1+N3) = (100 * 10 + 10 * 2) / (100 + 10) \approx 9.273$

VC owns:
N2 * (p1 / q)
$= 50 * 10 / q = 500 / 9.273 \approx 53.920$

Total:
(N2 * (p1 / q)) + N1 + N3
= 53.920 + 100 + 10
= 163.920

C. Full ratchet:
q = p2 = 2;

VC owns:
N2 * (p1 / q)
= 50 * 10 / q = 500 / 2 = 250

Total:
(N2 * (p1 / q)) + N1 + N3
= 250 + 100 + 10
= 360

4. XML AND DOCUMENT EXCHANGE (20 points)

A. Two of the following document types are required for full credit:

- List of available flights
- Reservation request
- Ticket (Invoice, Order Confirmation)

B. Here are some possible DTDs for the three document types above. The number of points you receive will depend on the correctness of the syntax in your definition, the structure of your definition, and whether you included a reasonable amount of information. (These DTDs include more element definitions than what you would need for full credit.)

List of available flights:

```
<!DOCTYPE FLIGHTLIST [
<!ELEMENT flight
(number, origin, destination, deptime, arrtime, seats+)>
<!ELEMENT number (#PCDATA)+>
<!ELEMENT origin (#PCDATA)+>
<!ELEMENT destination (#PCDATA)+>
<!ELEMENT deptime (#PCDATA)+>
<!ELEMENT arrtime (#PCDATA)+>
<!ELEMENT seats (#PCDATA)+>
<!ATTLIST seats
      class CDATA #REQUIRED
      price CDATA #REQUIRED
> ]>
```

Reservation request:

```
<!DOCTYPE RESERVATION [
<!ELEMENT passenger (name, address, phone)>
<!ELEMENT billing (name, address, phone, amount, card?, exp?)>
<!ELEMENT flight (number, date, seat+)>
<!ELEMENT name (#PCDATA)+>
<!ELEMENT address (#PCDATA)+>
<!ELEMENT phone (#PCDATA)+>
<!ELEMENT amount (#PCDATA)+>
<!ELEMENT card (#PCDATA)+>
<!ELEMENT exp (#PCDATA)+>
<!ELEMENT number (#PCDATA)+>
<!ELEMENT date (#PCDATA)+>
<!ELEMENT seat (passenger)>
<!ELEMENT request (flight, billing)>
<!ATTLIST billing method (bill | credit | debit) 'bill'>
<!ATTLIST amount currency CDATA #IMPLIED>
<!ATTLIST card type (visa | mc | amex) #REQUIRED>
<!ATTLIST seat class (first | business | economy) #REQUIRED>
]>
```

Ticket:

```
<!DOCTYPE TICKET [
<!ELEMENT flight
(number, origin, destination, deptime, arrtime, seat+)>
<!ELEMENT number (#PCDATA)+>
<!ELEMENT origin (#PCDATA)+>
<!ELEMENT destination (#PCDATA)+>
<!ELEMENT deptime (#PCDATA)+>
<!ELEMENT arrtime (#PCDATA)+>
<!ELEMENT seat (#PCDATA)+>
<!ATTLIST seat
      class CDATA #REQUIRED
>
<!ELEMENT payment (#PCDATA)+>
<!ATTLIST payment method (bill | credit | debit) `bill'>
]>
```

C. Here are some sample XML documents using the DTDs given above.

List of available flights:

```
<flight>
      <number>UA86</number>
      <origin>JFK</origin>
      <destination>LHR</destination>
      <deptime>14 Mar 2003 2000</deptime>
      <arrtime>15 Mar 2003 0700</arrtime>
      <seats class='first' price='1000'>12</seats>
      <seats class='business' price='700'>20</seats>
      <seats class='economy' price='400'>50</seats>
</flight>
<flight>
      <number>AA101</number>
      <origin>JFK</origin>
      <destination>CDG</destination>
      <deptime>14 Mar 2003 1700</deptime>
      <arrtime>15 Mar 2003 0400</arrtime>
      <seats class='first' price='1200'>8</seats>
      <seats class='business' price='850'>12</seats>
      <seats class='economy' price='350'>70</seats>
</flight>
```

Reservation request:

```
<request>
      <flight>
            <number>AA101</number>
            <date>14 Mar 2003</date>
            <seat class='economy'>
                  <passenger>
                        <name>Vijay Ramachandran</name>
                        <address>New Haven, CT</address>
                        <phone>432-7037</phone>
                  </passenger></seat>
      </flight>
      <billing method='credit'>
            <amount currency='dollars'>350</amount>
            <number>1234 5678 9012 3456</number>
            <exp>01/05</exp>
            <name>Vijay Ramachandran</name>
            <address>New Haven, CT</address>
            <phone>432-7037</phone>
      </billing>
</request>
```

Ticket:

```
<payment method='credit'>350</payment>
<flight>
      <number>AA101</number>
      <origin>JFK</origin>
      <destination>CDG</destination>
      <deptime>14 Mar 2003 1700</deptime>
      <arrtime>15 Mar 2003 0400</arrtime>
      <seat class='economy'>33A</seat>
</flight>
```