By Eva-Maria Scholz, 1 June 2014

Putting a price on privacy – an Introduction to the Economics of Privacy

This is the second part of a three-piece series that discusses the value of personal information in the digital economy. You can find the first part here.

I started my previous post by asking how much you would be willing to pay in order to prevent your Internet provider from tracking and analysing your browsing history. This question was motivated by the pricing model the telecommunications provider AT&T employs for its new *GigaPower* broadband service. To recall, AT&T offers two different pricing plans based on a consumer's preference for privacy. For instance, its standard service is priced at either $70 or $99 a month, depending on whether or not a consumer agrees to let AT&T monitor his/her surfing habits (see, for example, here or here). That is, if it were up to AT&T the answer to my question would be *a monthly mark-up of approximately 30 percent*.

Of course, my question was rather a theoretical one. And indeed, although the question itself sounds simple, the issue of how to value private information is highly complex. That is why it is in my eyes instructive to first introduce you to some basic notions of what is called the Economics of Privacy. The third and final part of this series will then discuss some theoretical and empirical approaches that try to shed light on how to value private information in the digital economy.

Willingness to pay versus willingness to accept

I want to start with a small experiment. In the beginning of this post I asked how much you would be willing to pay in order to prevent your Internet provider from analysing your browsing history. Take a moment to think about this question and write down the monthly amount. Now let us look at the problem from a different angle. How much would your Internet provider need to pay you so that you accept this invasion of your privacy? Again, write down the monthly amount. If you compare your two answers, you might realise that they do not coincide.

This experiment illustrates that it is crucial to distinguish between an individual's willingness to pay (WTP) and willingness to accept (WTA). Or, to put it differently, how much individuals are willing to pay in order to protect their private data typically does not coincide with the amount of money that makes an equivalent decrease in their privacy acceptable. And indeed, as a recent study by the OECD points out;

> *Generally, the fraction of consumers who will reject an offer to obtain money in exchange for reduced privacy is larger than the fraction of consumers who will accept an economically equivalent offer to pay money in exchange for protection of privacy (Acquisti et al. (2009)).*

The importance of distinguishing between WTP and WTA is further highlighted by the fact that in our daily life privacy decisions are typically present in both forms (Acquisti et al. (2013)). In some situations we have to decide how (or whether) to secure our personal data (WTP), while in others we are asked to reveal private information in order to receive some type of benefit (WTA).

These differences between an individual's WTP and WTA cannot be explained by standard economic theory. As Kahneman et al. (1990) explain;

> *the standard assumptions of economic theory imply that when income effects are small, differences between an individual's maximum willingness to pay (WTP) for a good and minimum compensation demanded for the same entitlement (willingness to accept [WTA]) should be negligible (Willig 1976). […] and there is wide acceptance of the Coase theorem assertion that, subject to income effects, the allocation of resources will be independent of the assignment of property rights when costless trades are possible.*

What then could explain the observed WTP-WTA discrepancy? A potential answer to this question is given by Kahneman and Tversky (1979) and Thaler (1980) and comes in the form of the *endowment effect*. In a nutshell, the *endowment effect* captures the observation that individuals attach value to objects simply because they own them. Meaning, property rights do matter. The presence of such an *endowment effect* may in turn be explained by the concept of *loss aversion* (Kahneman and Tversky (1984)). According to the latter individuals attach more importance to losses than to gains. Acquisti et al. (2013), apply this concept to privacy concerns.

> *Applied to privacy, this explanation of the WTA/WTP gap would predict that someone who enjoyed a particular level of privacy but was asked to pay to increase it would be deterred from doing so by the prospect of the loss of money, whereas someone who was asked to sacrifice privacy for a gain in money would also be reluctant to make the change, deterred in this case by the loss of privacy.*

Composite transactions, salience and privacy preferences

To illustrate how privacy concerns may matter for our daily consumption decisions, let us have a closer look at online purchases. Online purchases may best be described as composite transactions. So as transactions between a consumer and an online service provider that not only concern a particular good or service, but also, as a by-product, information (Jentzsch et al. (2012)). Following Jentzsch et al. (2012), composite transactions (T), such as an online purchase, may consequently be expressed as the sum of the transaction of the good (GT) and the transaction of

the information (IT), i.e., as T=GT+IT.

One way to add privacy concerns is to include a parameter x in the latter expression so that T=GT+(1-x)IT. Here, x is a *salience parameter* (DellaVigna (2009)) that expresses the relevance of the information disclosure in the overall context of the transaction (and by this a consumer's privacy concerns or privacy awareness). For x=0 a consumer attaches equal importance or attention to the good and the information, for x=1 the information disclosure does not matter. Intuitively, the *salience parameter* may not only vary across transactions or online service providers, but also across individuals. All in all, this illustrates in a simple way how different individuals may choose different service providers depending on their privacy concerns (we will see a theoretical model that formalises this point later on). Moreover, it accounts for the fact that privacy concerns need not to be stable, but may vary across transactions. This directly brings me to my next point.

Privacy attitudes, privacy behaviour and contextual effects

Judging from the public discussion surrounding topics such as Facebook's privacy rules or the NSA scandal, we are living in a society that attaches a high importance to digital privacy. This is also supported by various studies (see e.g., Harris Interactive (2001) or Jentzsch et al. (2012)) that report privacy concerns for the majority of the surveyed individuals.

There is, however, no lack in anecdotal evidence that calls this conclusion into doubt. To give an example, more than 70 percent of office workers at London's Liverpool Street station were willing to exchange their password for as little as a bar of chocolate in a 2004 field experiment by Infosecurity Europe (see here for a summary). Rest assured, this example is not a particular case. Also other studies show that supposedly privacy-concerned individuals are happy to exchange personal information for small rewards (see Acquisti et al. (2013) for an overview). From a WTA perspective individual privacy valuations hence appear to be low. Studies that focus on the WTP draw a similar picture. Here, the bottom line is that although the majority of the surveyed individuals expresses privacy concerns, only a small percentage is willing to invest in the protection of their personal data.

If based on this evidence one were to draw a conclusion regarding consumers' privacy preferences, one would come to the paradoxical and maybe disillusioning result that consumers place little value on their personal data. Once again Behavioural Economics comes to the rescue and argues that the apparent discrepancy between privacy attitudes and privacy behaviour may be explained by *contextual effects*. In other words, the value consumers attach to their personal data most likely depends on things such as the type of information or to whom the information is revealed. For instance, according to a recent study by PwC

> *Consumers are more willing to share broad demographic data and information about their use of media content because they see it as being less personal and more anonymous. However, consumers are less willing to share more sensitive information that might compromise their private interests, such as their web browsing history; information about their personal social lives, such as mobile texting data or call history; or information related to their identity or security, such as social networking*

passwords, banking or financial information or their social security number.

Interestingly, a set of experiments by Frog (2011) shows that consumers in the United States, India and China put more trust in financial institutions or telecommunications providers than in government agencies or social networking sites.

What about you? What personal data do you value? Do you observe differences in your privacy preferences depending on whether you look at the issue from a WTA or WTP perspective? And finally, do your privacy preferences vary across transactions or with the context? Do you have examples for which type of online transactions you are more privacy-concerned or privacy-aware?