oxera
compelling economics

Agenda

Advancing economics in business

Too much information? The economics of privacy

New technologies are increasing the amount of personal information that is collected from users, especially on the Internet. Consumers often happily provide information in exchange for services, but also express rising concerns over privacy. How much privacy is good, and who should be paying for personal information? Economic insights into consumer behaviour and the costs and benefits of sharing personal information can inform the ongoing debate on privacy

'Big data' is becoming bigger every day, and so is the amount of personal information that consumers share with firms. The Internet has opened up new opportunities for businesses to interact with consumers online and use their data to provide a variety of products and services, ranging from traditionally high-street domains such as online shops or banking to new business models such as auction platforms and social networks. The demand for these products is high—the average Briton had 19 online accounts in 2013.[1] At the same time, survey results suggest that consumers are increasingly concerned about their privacy, with around 40% of UK residents 'not trusting at all' in how personal data is used.[2]

These trends suggest that the privacy debate has only just begun. Economic analysis can provide useful answers to a variety of questions to help advance this debate. How do consumers and firms interact in the 'market for privacy'? What are the costs and benefits associated with the disclosure of personal information? And what can be inferred from the seemingly paradoxical behaviour of consumers who use more information-intense services, but also express more concerns?

Privacy as an economic 'good'

Online privacy usually concerns personally identifiable data, such as a person's name, IP address, birthday, location, browsing behaviour and purchase history. This personal information is a special kind of good for at least two reasons.

- Individuals value privacy both as an **intermediate** good and as a **final** good.[3] Personal information is seen as an intermediate good when, for example, consumers prefer a firm not to know their high valuation of the firm's product in case they are charged a higher price. Individuals may also value privacy as a final good—i.e. they may feel uncomfortable sharing their data. This aspect is more explicitly dealt with in political and philosophical debates; economic analysis focuses on the value people assign to privacy, without debating their reasons.

- Privacy is a **non-rival** good from a firm's perspective. This means that when consumers share a piece of personal information with one firm, the information is still valuable to other firms that do not have access to it. Consumers still own their private information and are free to consider trades with other firms in isolation.

There are at least three types of transaction in which consumers make decisions about their privacy.[4]

- Consumers share personal information as a **by-product** of an exchange of ordinary goods, such as in an online purchase of a book from the online retailer, Amazon, or a flight on the travel website, Expedia. In this case, consumers trade their data in order to be able to use a certain platform or service, but may be unaware of the transaction.

- Consumers provide personal information in exchange for otherwise **free services**, such as social networks, email programmes and search engines.

- Consumers sometimes explicitly choose not to share personal information by purchasing **privacy-enhancing products**, such as encryption programmes.

Consumers would be expected to be consistent across the levels of privacy accepted for different types of transaction, reflecting their valuation of keeping information private. However, as shown below, consumers can fail to relate their decisions to each other, which may lead to inconsistent privacy outcomes.

Why more information is often good

From an economic welfare perspective, it is generally considered desirable for all market participants to have access to the same information. Information asymmetries can prevent welfare-increasing exchanges, which supports the stance that the sharing of personal information should be encouraged. In particular, the Chicago School[5] in the 1980s argued that consumers and firms should trade information to achieve a market outcome with free access to personal information. More information would allow interactions to take place that otherwise would not, or would do so only at a higher cost. The context of the Internet provides several examples.

- Consumers and products can be **matched better** if firms know more about consumers' preferences, for example by using cookies. Firms may use this personal information to develop niche products[6] or to target advertisements (for example), thereby reducing the cost of market research and wasteful advertising.[7]

- As personal information is valuable to firms, they can provide services to consumers at a lower price or even a price of zero, **creating new markets and expanding existing ones**. Zero prices are charged for a variety of services such as Twitter, Google Maps, TripAdvisor and LinkedIn. These services create value for users and profit for firms.

- Sharing personal information can also **facilitate transactions** and **enhance the user experience**. For instance, the third-party log-ins of Facebook, Google or Twitter allow users to be recognised on many other websites without having to create multiple accounts. This may increase the convenience of browsing, and the firms' ability to reach potential customers who do not have a separate account with them.

The collection and storage of information comes at a cost. This cost puts a limit on the amount of information exchanged, as firms invest in collecting personal information (according to the Chicago School) up to the economically efficient point.

Why more information can be bad

Various studies cast doubt on whether personal information is always used to the consumer's benefit, and to what extent consumers make well-informed decisions about privacy. Three types of concern are presented below.

Negative externalities

When deciding how much personal data to collect and how to use it, firms do not necessarily take into account any negative effects that this could have on their consumers. This is an example of the negative externality problem in economics.

Consumers may receive **unsolicited marketing** such as spam when a firm passes their personal information on to other firms (on the so-called secondary market). In this transaction, the data-collecting firm does not consider the hassle it imposes on consumers when selling on the data, and may collect more of it than is optimal.[8]

If firms can use information on consumers' past purchases, they can engage in **adverse price-discrimination**—i.e. they can aim to set prices that reflect the willingness-to-pay of individual consumers. The make of the customer's computer,[9] and their location or route to the product[10] (e.g. through a price-comparison website), have been found to affect the prices consumers pay. Sellers may also use information on browsing behaviour to infer the individual consumer's level of sophistication in making purchases, and adjust pricing models accordingly.[11] The impact of price-discrimination is ambiguous—if firms can set prices for each consumer individually, consumers would pay a price equal to their willingness-to-pay, with all benefits from the trade going to firms. If prices differ for different groups of consumers, consumers can be better or worse off than if only one price exists, depending on the characteristics of the market.[12]

The negative impact of reduced privacy could be limited if consumers were asked to approve the sharing of their data with third parties, or other uses of their data. Privacy policies are meant to govern these transactions; however, they may not be efficient in achieving this objective, as discussed below.

Little bargaining power

Consumers generally do not have an opportunity to negotiate their desired level of online privacy, but have to decide whether to accept or decline individual privacy policies. Rejecting a privacy policy may come at a high cost, because few alternatives allow consumers to keep information private. For example, consumers need to accept cookies to browse large parts of the Internet, and need to provide their name and email address to sign up for most online services.

Certain features of privacy policies raise doubts about whether they help consumers to make a good and educated choice about privacy: they are often only one of many features of the product the consumer is interested in; they can be lengthy and hard to understand; and they often change over time.

Consumers often do not pay much attention to privacy when personal information is only a **secondary feature** of a product. For example, if a consumer wants to buy a book online, comparing multiple privacy policies before making a purchase seems a prohibitively costly exercise, as they are likely to value their time more than a possible gain in privacy.

Besides, the **complexity and length** of most privacy policies discourage the majority of consumers from engaging

with them. Research indicates that significantly less than 1% of online shoppers read the terms and conditions before making a purchase.[13] This is likely to limit the awareness of consumers and the privacy-oriented competitive pressure they can exert: if consumers do not compare, there is little incentive for firms to compete by offering more attractive privacy policies.

Incremental **changes over time** tend to aggravate this problem, especially if consumers do not expect them. If firms can award themselves more discretion over the collection and use of personal data, their optimal strategy would be to give users just the level of privacy required to not drive them away.

Hence, it is difficult for consumers to understand the implications of accepting a privacy policy for the future—what exactly it permits the firm to share with whom, how likely it is to change and to what extent, and what other types of personal information may become available to firms in the future.

Behavioural biases

It can be argued that people do share their personal information in exchange for small amounts of money. Numerous experiments have found that even privacy-concerned individuals easily give away personal information for small discounts or mere chances of winning money.[14] This seemingly paradoxical behaviour can be attributed to at least three patterns of deviation from the rationality assumption that underpins much of standard 'textbook' economics: availability bias, present bias, and loss aversion.

With **availability bias**, individuals care more about risks when they are reminded of them. Hence, consumers can become more aware of privacy concerns in situations where their anonymity is asserted than when they are not aware of it. Experiments[15] have shown that individuals are more likely to share sensitive personal data when they are not thinking about privacy, and they may even be triggered to do so by observing others sharing information. The mere reminder that privacy concerns exist was seen to lower the amount of information shared.

With **present bias**, individuals tend to focus on the immediate situation and do not fully account for the impact of their current decisions on future outcomes, especially where those outcomes are uncertain. The reason for this is a changing pattern in discount rates over time: individuals apply high discount rates over a short horizon, and much lower discount rates over a long horizon.[16] This can make individuals happy to give away their data today for a small discount, but suffer in the future from large amounts of spam that they would otherwise not have signed up to.

With **loss aversion**, people value a good more when they own it and are asked to sell it than when they are asked whether they wish to buy it. This is often expressed as a low willingness-to-accept for the loss of a good (i.e. a high valuation of keeping the good) and a low willingness-to-pay for the same good. In the case of privacy, individuals have also been found to put a higher value on privacy when they believe they already own it than when they are willing to purchase it in exchange for a fee. This is shown by the experiment in the box above, which attempts to estimate the gap between these two valuations.

Estimating inconsistent consumer valuations

Acquisti, John and Loewenstein (2013) conducted an experiment in which participants—unaware of the purpose of the study—were asked to choose between two rewards for responding to a survey: one gift card worth $10 that was not tracked, and another one worth $12 on which purchases were tracked. They were not presented with both options at the same time, but received one card and were then asked whether they wanted to exchange it for the other. Hence, some individuals first 'owned' their privacy and a smaller monetary amount, while others first had a higher amount without privacy.

Over 50% of the individuals first given the privacy card kept it and were unwilling to accept $2 in exchange for their privacy. Only 10% of the individuals with the $12 gift card were willing to pay $2 to 'get their privacy back'. The implied ratio of willingness-to-accept and willingness-to-pay is 5.47—almost twice the ratio found for ordinary goods.

Source: Acquisti, A., John, L.K. and Loewenstein, G. (2013), 'What is privacy worth?', *Journal of Legal Studies*, **42**:2, pp. 249–74.

Multiple valuations of privacy by single individuals make it difficult, if not impossible, to say how much they actually value privacy. They also raise doubts about whether the fact that Internet users generally agree to give away personal information proves that they do not care very much; if they were made aware or reminded of the issue and the consequences, they might well decide differently.

Concluding remarks

Evidence suggests that consumers are not always making good choices about privacy, and that there may be incentives for firms to limit the options available to their customers. However, consumers most often benefit from the wide range of products that are available to them in exchange for their data. It is not clear which of these services firms would offer for free if they were given less access to personal information, or what consumers would do if they could choose between free services in exchange for personal information and paying for services that allow them to keep their privacy—their answer is likely to depend on how the question is put to them. Telling consumers what information firms are collecting and which costs this may create for them would allow them to make better-informed decisions. This could help them to overcome behavioural biases, in particular the availability and present bias, and may reduce the negative externalities.

Therefore, general statements about whether privacy is 'good' or 'bad' do not reflect the complexity of the market. The actual behaviour of both consumers and firms is likely to lead to different answers for different circumstances.

Economic analysis can shed light on these specific circumstances and assist consumers and firms in making well-informed decisions on a 'good' level of privacy.

[1] Beach, D. (2014), '5 tips to beat the online cyber-criminals', *Experian Experts Blog*, 10 June.

[2] CASRO (2014), 'GRBN Study Reveals Widespread Concern Over Personal Data Security', press release, 25 February. The original study is not publicly available. CASRO, which represents companies and market research operations, is part of the Global Research Business Network (GRBN).

[3] Farrell, J. (2012), 'The economics of privacy: can privacy be just another good?', *Journal on Telecommunications & High Technology Law*, **10**, pp. 251–65.

[4] Acquisti, A. (2013), 'The Economics of Privacy: Theoretical and Empirical Aspects', 12 September.

[5] For example, Posner, R.A. (1981), 'The economics of privacy', *The American Economic Review*, **71**:2, pp. 405–9; and Stigler, G.J. (1980), 'An introduction to privacy in economics and politics', *The Journal of Legal Studies*, **9**:4, pp. 623–44.

[6] Blattberg, R.C. and Deighton, J. (1991), 'Interactive marketing: exploiting the age of addressability', *Sloan Management Review*, **33**.

[7] Acquisti, A. (2010), 'The economics of personal data and the economics of privacy', Background Paper for OECD Joint WPISP-WPIE Roundtable.

[8] Varian, H.R. (1996), 'Economic Aspects of Personal Privacy'.

[9] Mattioli, A. (2012), 'On Orbitz, Mac Users Steered to Pricier Hotels', *The Wall Street Journal*, 23 August.

[10] Mikians, J., Gyarmati, L., Erramilli, V. and Laoutaris, N. (2012), 'Detecting price and search discrimination on the Internet', Proceedings of the 11th ACM Workshop on Hot Topics in Networks, pp. 79–84.

[11] Heidhues, P. and Kőszegi, B. (2014), 'Using Information about Naivete to Price Discriminate'.

[12] Hermalin, B. and Katz, M. (2006), 'Privacy, Property Rights, and Efficiency: The Economics of Privacy as Secrecy', *Quantitative Marketing and Economics*, **4**, pp. 209–39.

[13] In data for US Internet users, around 0.2% of consumers opened the agreement, but also spent too little time with it to actually read it. Bakos, Y., Marotta-Wurgler, F. and Trossen, D. (2014), 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *Journal of Legal Studies*, **43**:1.

[14] A short overview can be found in Acquisti, A., John, L.K. and Loewenstein, G. (2013), 'What is privacy worth?', *Journal of Legal Studies*, **42**:2, pp. 249–74.

[15] John, L.K., Acquisti, A. and Loewenstein, G. (2009), 'The Best of Strangers: Context Dependent Willingness to Divulge Personal Information', 6 July.

[16] Acquisti, A. and Grossklags, J. (2004), 'Privacy attitudes and privacy behavior', chapter 13 in J. Camp and R. Lewis (eds), *Economics of Information Security*, Kluwer, pp. 165–78.