Personal data and ethics: The economic stakes of trust

Patrick Waelbroeck,
Professor of economics, Télécom ParisTech

Abstract:
We leave tracks, whether knowingly or not, when using the Internet or digital devices. These tracks make us producers of personal information. The digital economy sets a price on these tracks (and this information), which are used to build business models. More and more users of the social media are concerned about how their data are being put to use. Because of the asymmetry of information that it causes between the producers and users of data, digital technology has upended the conditions underlying transactions. Thoughts about the economic issue of trust which is at stake in the production and use of data…

We leave tracks when using the Internet or other digital devices. Search engines and browsers on the Web store and analyze these tracks. Whereas some cybernauts leave tracks less unawares, others actively take part in "sociodigital communities" (as on Ebay, Amazon, Wikipedia, Twitter or YouTube) by posting notes, recommendations, comments or files or by ranking products or services. Owing to their tracks and posts, the people who use the Web and digital devices produce personal data that the digital economy uses to build business models. The websites financed by advertising repeatedly target prospective customers with personalized offers and prices. Furthermore, Internet firms such as Amazon or Netflix use these personal data to develop their business models by identifying cybernauts' preferences and customizing the recommendations made to them. Likewise, eBay uses the ratings of transactions by its users to build an online reputation system. YouTube and Facebook owe their existence to the contents generated by their users.[1]

Although the digital economy feeds on the personal data provided (in some cases voluntarily) by cybernauts, more and more users of the social media are concerned for the processing of their data. Millions of personal data have been stolen, thefts involving companies such as Yahoo, Equifax, ebay, Sony, LinkedIn and, recently, Cambridge Analytica. Revelations from the Snowden affair about widespread government surveillance have aroused so much distrust toward the agents of the digital economy that, in 2015, 21% of cybernauts were unwilling to share any information, as compared with but 5% in 2009.[2] Does the Internet's for-free model not have a societal cost?

Digital technology has disrupted the conditions for transactions owing to the asymmetry of information it generates — what has been called the "*black box society*" (PASQUALE 2015). The users of digital devices do not know how their personal data will be used or exchanged by the firms that have collected them. Worse yet, these firms can manipulate the context of a transaction — so that customers believe they are in a trustful environment (MANTELERO 2013) — and thus induce them to disclose personal information.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references.
[2] Source: confidence barometer of the ACESL-CDC.

This article seeks to shed light on the economic stakes in this "confidence game". In economics, confidence can be understood in relation to the risks linked to transactions: risks stemming from the terms of a particular transaction or from the institutional environment in which transactions take place.

The economic source of risks

What types of data do firms use? And what are the risks to consumers? When personal data are collected from the tracks left unwillingly by cybernauts in their browsing history, risks arise because the persons leaving these tracks are not always aware of the consequences of how digital firms will put this information to use. In the case of voluntary contributions, as when a consumer posts a comment on a blog or rates the quality of a product or a seller's reputation, risks arise related to data theft. Malevolently used data can produce negative externalities, such as identity theft, online harassment, the disclosure of private information, the fraudulent use of banking references, price discrimination or unwanted advertisements (whether targeted or not). Such negative externalities result from a market failure, since an economic agent's actions have a negative impact on other agents without any market compensation. These externalities — negative for consumers — are caused by the firms that collect too many data (in relation to a social optimum); and their existence is an economic justification for protecting personal data.

The asymmetry of online information aggravates problems related to the misuse of personal data. For one thing, it is hard for consumers to verify how the companies that collect and process their data will use them; and hard for them to know whether or not these uses comply with the law. This holds even more during the era of big data, since independent databases with little personal information can be easily combined to identify a person. For another thing, the individual is hardly capable of technically assessing the level of digital security protecting personal data as they are transmitted and stored. Sometimes even the firms concerned are unable to fully assess the security of their information systems: they might not even know whether a cyberattack has targeted their information system. The economic consequences are serious. In the work for which he received the Nobel prize in economic sciences, George Akerlof showed that situations characterized by asymmetric information can push good products out of the market. The digital economy is not exempt from this theory, and the loss of confidence creates risks that push some cybernauts to disconnect.[3]

Two types of risks can be distinguished.

- The first, related to individual transactions, is the idiosyncratic risk of whether there will be a counterpart: will the contract be respected? Will all its provisions be applied? These risks cannot always be insured, since it is hard to foresee all contingencies in the context related to the contract, a situation that economists describe as an "incomplete contract".
- The second type of risks, related to the environment where a contract is executed, is systemic: is there a recourse if a problem arises? Although a transaction obviously takes place within a legal framework, the benefits of legal proceedings often do not cover the costs in cases of transactions involving small amounts.

Take as example a transaction on eBay. A buyer orders a product. Will it be delivered on time? Does it correspond to the order? These are the idiosyncratic risks, which are attenuated by the environment of confidence where the transaction takes place. The systemic risk related to this environment is reduced to two means. The first is punitive: the buyer, if deceived or disappointed, can rate the seller poorly. The second is related to the trusted third party, Paypal, which provides a procedure for filing a claim for a refund.

[3] *Cf.* the Chair Values and Policies of Personal Information (launched by Institut Mines-Telecom in April 2013): https://cvpip.wp.imt.fr/donnees-personnelles-et-confiance-quelles-strategies-pour-les-citoyens-consommateurs-en-2017/.

Digital strategies: Ethical problems with economic consequences

Besides the aforementioned negative externalities, the use of personal data by Internet firms in their sales strategies raises ethical questions with economic consequences. Let us examine three of them: free will (the possibility to make choices in a neutral "information environment"); autonomy (the ability to be in step with what is good for one's self) and discrimination (or the absence of systematic biases).

Free will and autonomy

To make an optimal economic decision, the consumer has to be able to choose in an information-neutral environment. Two trends, exacerbated (as already pointed out) by the strategies adopted in the digital economy, cause problems:

- First of all, consumers receive information filtered by the online platforms. For example, Google's search engine filters its findings as a function of the user's geolocation, browsing history and advertising profile; and Facebook filters information as a function of the user's "likes" and profile. These filters, since they can sway the cybernaut's behavior, raise important economic questions related, above all, to the construction of preferences, of "filter bubbles". The algorithms that filter information produce an information bubble that, specific to the cybernaut, has the potential of influencing how he/she thinks, behaves and makes purchases.
- Secondly, Amazon, Netflix and Spotify, among many other digital companies, execute algorithms to personalize product recommendations as a function of the individual's browsing history and purchases.

When the information environment is manipulated, economic agents no longer make optimal decisions. The ethical questions of free will and autonomy are reflected in these economic decisions, but the latter can be manipulated by information filters and targeted recommendation.

Discrimination and biases

Personal data might also be collected to practice price discrimination, *i.e.*, to sell a product or service at different "net prices" (*i.e.*, production costs plus delivery fees) to different consumers. Firms try to determine the best price for selling their products and services as a function of the potential customer's propensity to pay the price. For digital products, the most widespread form of price discrimination involves strategies for identifying groups of consumers to whom different versions of the same product or service will be offered. For example, a software developer might offer the same software with different features: a full business version and a basic (or academic) version without certain features. The consumer's personal information can thus be used to customize (often at a very low cost) the offer used to target him/her. While some consumers benefit from the lower price, those who are offered the product at a higher price might want to protect their personal data to avoid this discrimination.

The economic consequences

The manipulation of the information environment and targeting raise ethical questions with quite real economic consequences, in particular on competition and innovation. Five of these consequences can be pointed out.

First of all, the algorithms that influence consumers by imposing external values modify how consumers build their utility functions. We think of Facebook, which censors artworks deemed shocking (*e.g.*, Corbet's *L'Origine du Monde*) or feeds into its algorithms data collected on American citizens and then applies the results worldwide. The problems related to trust, or confidence thus give rise to cultural issues.

Secondly, if competition is not strong, the Internet platforms that control the user's access to data can work out strategies of foreclosure or strategies that bar third-party firms. Several examples exist. In June 2012, Facebook imposed as default e-mail address the domain @facebook.com. At the same time, Apple announced that it was installing by default its software Apple Maps in place of Google Maps in its new operation system iOS. In April 2013, Apple withdrew from its App Store the application AppGratis, which listed applications that were offered temporarily for free on App Store. In 2001, the United States demanded that Microsoft open its programming interface to third-party companies and put an end to its offer for bundling its operating system Windows with its browser Internet Explorer (so that consumers can install the browser they choose). In June 2017, the European Commission fined Google €2.4 billion for filtering search findings so as to promote Google Shopping while demoting competitors.

Thirdly, who will see to it that the tools for privacy protection will be available to consumers? Development costs are high, and the technical solutions run counter to the strategies of digital firms and to government surveillance programs. In general, digital security is a public good of benefit to everyone. The risk exists, therefore, that firms will underinvest in protecting personal data — a situation that could result in more data being leaked and confidence being lost (DUBUS & WAELBROECK 2018).

Fourthly, the platforms that control the access to cybernauts' data have increased the cost of market entry for new firms. This can hamper the innovations that need personal data to be developed.

Fifthly, the algorithms that customize prices as a function of consumers can be misappropriated so as to favor market collusion among firms (OECD 2017). As an illustration, we might mention a book on the genetics of flies that was bid up to $23 million by two vendors using algorithms to optimize their profits on the platform Amazon Marketplace.[4]

Concluding thoughts

Underlying trust and confidence is an assessment of the risks that arise during electronic transactions. The two aforementioned types of risks (idiosyncratic and systemic) provide leverage for building confidence in the digital economy. For one thing, it is necessary to improve the cybernaut's knowledge about the uses of data and negative externalities. For another, feelings of reciprocity and fairness have to be restored by guaranteeing that transactions have a fair value: exchanging a for-free service for personal data no longer seems satisfactory. Furthermore, credible punitive procedures are needed to sanction misuses of personal data. The tighter sanctions foreseen by the EU's GDPR (General Data Protection Regulation) as of May 2018 take a step in this direction.[5]

Another way to build confidence is for consumers to adopt the new data protection tools. Software can conceal IP addresses. Browser add-ons can block scripts and advertisements, and make it harder to identify the user and practice price discrimination. As the survey we conducted in 2017 on a representative sample of the French population has shown,[6] the persons who protect themselves the best are those who make the most online purchases. Despite seeming paradoxical at first sight, this finding is logical since data protection tools allow consumers to make purchases with confidence. The consumer should not be seen as being passive when faced with e-business strategies.

[4] *Cf*. http://edition.cnn.com/2011/TECH/web/04/25/amazon.price.algorithm/index.html.

[5] The GDPR (General Data Protection Regulation): "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data". Available via: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478961410763&uri=CELEX:32016R0679.

[6] See https://cvpip.wp.imt.fr/donnees-personnelles-et-confiance-quelles-strategies-pour-les-citoyens-consume£ateurs-en-2017/.

The question of confidence about the uses of personal data is related to the economic value of anonymity. A simplistic theory postulates that people weigh the economic value of their data against the value of protecting privacy and being anonymous. Accordingly, there are two extremes: on the one hand, when the individual is fully identified and likely to receive targeted offers; and on the other hand, when the person is anonymous. In the first situation, the economic value of personal data is thought to be maximal whereas, in the second, the user's data has no value. If a shift is made toward targeting, the economic value of personal data increases to the detriment of protecting privacy; but if emphasis is shifted to protecting privacy, the economic value of personal data will decrease. This theory ignores the stakes related to trust and confidence when data are used.

To develop long-term relations with customers, it is necessary to reason in terms of the risks and externalities borne by the customer. Protecting privacy has, therefore, an economic value in relation to long-term customer relations, the concept of confidence, and the guarantee that consumers are able to exercise their free will and autonomy and will not be the target of discrimination. The principles related to pseudonyms and express consent in the GDPR tend in this direction.

References

DUBUS A. & WAELBROECK P. (2018) "La notion de confiance en économie" in C. Levallois-Barth (ed.), *Signes de confiance. L'Impact des labels sur la gestion des données personnelles* (Paris: Institut Mines-Télécom) pp.37-46. Available via: https://www.imt.fr/en/book-on-signs-of-trust-labels-and-personal-data-is-now-online/.

MANTELERO A. (2013) "Competitive value of data protection: The impact of data protection regulation on online behavior", *International Data Privacy Law*, 3(4), pp. 229-238. DOI: 10.1093/idpl/ipt016.

OECD (2017) *Algorithms and Collusion: Competition Policy in the Digital Age*. Available at: www.oecd.org/competition/algorithms-collusion-competition-policy-in-the-digital-age.htm.

PASQUALE F. (2015) *The Black Box Society: The Secret Algorithms That Control Money and Information* (Cambridge, MA: Harvard University Press).