Deutsche Bank
Research

Talking Point

Cash empowers the individual through data protection

July 2, 2019

Author
Heike Mai
+49(69)910-31444
heike.mai@db.com

www.dbresearch.com

Deutsche Bank Research Management
Stefan Schneider

By providing a high degree of privacy in payments, cash helps to slow the growing information asymmetry between consumers and companies as well as between citizens and public authorities. As knowledge about your counterparty is power, privacy is crucial for individuals to safeguard their position when dealing with organisations which are more powerful than a single person.

Cash enhances privacy

Cash leaves hardly any traces, but cashless funds and payments do. While the information accompanying electronic transactions traditionally only used to facilitate the payment execution, it is now a valuable product.[1] Personal data extracted from payments can be enriched with information from other sources, e.g. from data-generating applications like market places or social media. Modern data analytics allow the extraction and collection of information specific to an identifiable user, which enable the data receiver to approach an individual with offerings and information tailored to his (perceived) needs. Companies are interested in targeted advertisement in order to raise their sales. Political parties can send messages to a voter which he will likely agree with. Those who can access and analyse personal data profiles can take deep insights into an individual's life.

However, citizens have the right to preserve their personal privacy. Physical cash works without registers of cash holders and transactions. When paying with banknotes and coins, it is only the buyer and the seller who are aware of this transaction: what is bought, how much, when, where, by whom and at what price – all valuable information about an individual's habits.

But even cash purchases are not fully anonymous. Our world is becoming ever more digital, and even though a cash transaction is not recorded, the buyer may have left related data points: He might have searched for product information online before the purchase or might have commented on the purchase via social media. Besides the tracking of the buyer's deliberate online activities there can also be offline data generated e.g. from his smartphone's log-ins or a store's security video surveillance.

Nevertheless, banknotes and coins reduce your digital footprint. In contrast to an electronic payment, a cash transaction itself does not generate digital data

Cash empowers the individual through data protection

and no third party – e.g. a payment provider – will automatically receive the transaction data. Cash helps the individual to protect his privacy, even though it does not guarantee full data protection given today's digital environment.

"I have nothing to conceal?" – Knowledge is power!

Why does privacy matter? A law-abiding citizen might say "I have nothing to conceal." This is a misconception. In any debate, negotiation or competitive situation, it is an advantage to know about the other party's position in order to achieve one's own desired outcome. It should therefore be in anybody's interest to protect his privacy to strengthen his bargaining position. However, the data industry allows interested parties to gain insight into an individual's personal and financial situation. This can easily become detrimental to the individual.

Collecting information on individuals has a long tradition, be it for commercial ends (e.g. debtor registers, phone books) or public purposes (e.g. land registers). But the digitalisation has multiplied the data generated and facilitated processing and analysis, resulting in rather comprehensive personal profiles, which data users obviously deem so useful that they are willing to pay for it. Demand for meaningful data on potential consumers, voters, etc. drives the data industry. Maybe surprisingly, the data mined by large online platforms is not necessarily comprehensive enough. In order to get a picture of an individual as complete as possible, specialised companies – data brokers – buy and combine data from various sources (online and offline) to deliver information on exactly defined target groups to their customers.[2]

In Europe, the General Data Protection Regulation (GDPR) has introduced stricter rules on the use of personal data, i.e. data relating to an identified or identifiable living individual.[3] However, the use of personal data is allowed for specific purposes like fulfilment of contract or legal obligation, and also if the data subject has consented to it. In the online sphere, consent to processing one's personal data is often given with little consideration by clicking a box which then enables the customer to use the provider's services.

Data holders often claim that personal data is only used in an anonymised form. But data protection agencies upheld that most data is only pseudonymised and that persons can easily be identified.[4] Scientists were able to correctly identify 90% of 1.1 million credit card holders only based on their "anonymised" card transactions over three months, including day and shop of the purchase but without personal data like names or card numbers.[5]

Digital payments – both online and offline – are a rich data source which can give valuable insight into a person's consumption habits, daily routines and financial resources. Despite the wealth of its own data about its users, online platform Google took recourse to buying offline transaction data from Mastercard in order to prove to the customers of its advertising business that user clicks on an online ad correlate with subsequent in-store purchases. Both companies affirm that no personal data was provided.[6]

Balance of power: Individual (consumer) vs companies (merchants)

The digitalisation has tremendously increased the information asymmetry between companies and retail clients to the latter's detriment. Digital analysis of

internal client data as well as bought data profiles allow especially “click-world” merchants to know a lot more about their clients’ private and financial habits than the individual knows about the merchant company or its competitors. Given the increasing bargaining position of merchants, is the consumer still getting a good deal?

Advertisements can be targeted directly at clients who are likely to buy a certain product or service, based on their data history. On the one hand, the client might benefit from more meaningful advertisement. On the other hand, there is a higher risk the client is tempted to buy too much. The internet allows consumers to compare prices and products conveniently. However, online merchants are venturing into dynamic pricing, i.e. prices change frequently in order to decrease the market transparency and to create pressure to buy before the next price change might occur. Prices can even be tailored to an individual’s estimated willingness and financial ability to buy. E.g., prices can be higher for clients logging into a website with a tablet instead of a PC or for clients who have clicked on an offer several times.[7] The client’s bargaining power vis-à-vis a merchant is mostly based on his ability to turn to a better offer at a competing shop. If price transparency is seriously diminished, the consumer runs the risk of paying too much. The commercial value of personal data is even less transparent for consumers. Data has become an economic good for which the “producer” is usually not remunerated. Given the dynamic growth of data-based business models, it would be interesting to know how good a deal consumers get when they exchange their data for free-of-charge online services.

Balance of power: Individual (citizen) vs public authorities

The significance of physical currency runs deeper than the economic aspects discussed above. It touches upon the relation between citizens and the state. The shift to transparent and traceable electronic funds – with no easy option left to pay without a digital data trail and involvement of a third party – can open the door to data abuse and infringement of civil rights. In fact, comprehensive data about an individual citizen can facilitate surveillance for political reasons.

Even in democracies governed by the rule of law, citizens are well advised to be vigilant that state authorities do not abuse their powers. This does not only refer to obvious executive powers like the police’s use of force. Knowledge of the private and financial situation of individual citizens gives public authorities additional power over them. Even with stringent data protection rules in place, the unlawful abuse of such information asymmetry cannot be ruled out. Comprehensive data on individuals might tempt abuse for personal or political ends, be it by a single civil servant or by domestic or foreign intelligence services.

An abolition or strict limitation of cash usage carries the risk of seriously eroding trust in state authorities. The willingness of citizens to be transparent towards authorities depends crucially on their trust that public authorities function well and do not overstep their mandate. Depriving citizens of a simple tool to guard their privacy in financial matters can easily prove to be counterproductive: Feeling captive to public authorities – as opposed to being a citizen – would loosen the bond between people and government.

Cash empowers the individual through data protection

Wherever civil rights are not respected by the government, cash – much more than digital payments – helps opposition activists to protect themselves from the illegitimate use of public power, e.g. from surveillance and intimidation.

Cash empowers the individual

By providing a high degree of privacy in payments, cash helps to slow the growing information asymmetry between consumers and companies as well as between citizens and public authorities. As knowledge about your counterparty is power, privacy is crucial for individuals to safeguard their position when dealing with organisations which are more powerful than a single person.

[1] Ich weiß, was Du gestern gekauft hast, Zeit Online, June 20, 2018.
[2] So hinterlassen Sie jeden Tag eine riesige Datenspur, WirtschaftsWoche, May 24, 2018.
[3] "General Data Protection Regulation", Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (taking effect May 24, 2018).
[4] Data brokers: regulators try to rein in the 'privacy deathstars', Financial Times, January 8, 2019.
[5] De Montjoye, Yves-Alexandre et al, Unique in the shopping mall: On the reidentifiability of credit card metadata, Science, January 30, 2015.
[6] Google and Mastercard Cut a Secret Ad Deal to Track Retail Sales. Google found the perfect way to link online ads to store purchases: credit card data, Bloomberg, August 31, 2018.
[7] Dynamic Pricing. Warum online jeder einen anderen Preis zahlt, Bayerischer Rundfunk BR 2, April 16, 2019.