ESTABLISHED 1987

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

EU-US Privacy Shield is invalid says European Court of Justice

Although Standard Contractual Clauses remain valid, the decision creates uncertainty for companies which have been relying on the Shield for their EU-US transfers. By **Laura Linkomies**.

The EU-US Privacy Shield was declared invalid by the Court of Justice of the European Union (CJEU) on 16 July. The court said that the agreement does not provide equivalence of protection to EU citizens due to access to personal data by the US surveillance community, and that there are faults in the US Ombudsman system. The US Department of Commerce, which administers the programme, was

Continued on p.3

Jamaica adopts a post-GDPR data privacy law

Graham Greenleaf asks whether Jamaica's law is strong enough to mark the start of a different direction for data privacy in the Caribbean.

Jamaica's Data Protection Act 2020[1], enacted on 19 May but not yet in force, provides for a transitional period of two years. The Jamaican Information Commissioner, once appointed, should be influential in the region, at least within the anglophone Caribbean.

There are now 15 Caribbean data privacy laws: the Bahamas (2003), St Vincent & Grenadines (2003), BES Islands (the Netherlands municipalities

Continued on p.5

Issue 166 **AUGUST 2020**

Buying and selling personal data directly from consumers

Are data marketplaces the wrong direction for data privacy? Selling one's personal data is OK as long as there is revocable consent, says **Sanna Toropainen** of Muna.io.

Personal data markets stir conversation, with different intermediaries such as Clture and Citizen.me already providing a possibility for consumers to exchange their data for discounts or cash. However, the legal consequences of selling one's data are not clear – do you still have your right to privacy after selling your data? (*PL&B UK* July 2013 p. 19).

In the US, Clture pays consumers for access to their Netflix video streaming information. The data is sold on the company's business intelligence site to other companies. In Europe, Citizen.me pays users £0.08 for behavioural metadata, and £0.12 per company specific question answered on the Citizen.me application. Citizen.me positions itself as an ethical consumer insights company, sourcing the data directly from the consumers and compensating them for answering questions on their platform.

Personal data markets are based on the premise that consumers should be active participants in the data economy and that they can assess privacy related risks and weigh them against the benefits. Consequently, when they consent to selling their personal details such as home address and age, they do it knowingly and willingly, fulfilling the requirements for valid consent under the General Data Protection Regulation[1].

David Taylor, the Data Protection Officer of an intergovernmental organisation in life sciences, says however that you should not sell your data because a right to privacy is a fundamental human right, and "any commodification of human rights is an anathema to human rights, for a good reason". *Christopher Tonetti*, a macroeconomist at Stanford University understands that people are worried about financial incentives eroding privacy, but in his view, they should be allowed to make the choice, "which data is worth selling for the price they would receive".[2]

This article examines the legitimacy of the personal data trade and gives recommendations on the key considerations for a company to answer when buying personal data directly from consumers.

Legitimacy of personal data trade

It is necessary to highlight that the GDPR does not address data monetization. The regulation does not explicitly cover situations where individuals sell or exchange their data for benefits. The same lack of reference is found throughout EU legal instruments in general. Only in the preamble of the Digital Content and Digital Services Directive, it is said that since individuals have a fundamental right to privacy, personal data "cannot be considered as a commodity".[3] In the same vein, the European Data Protection Supervisor has commented that there should not exist a market for personal data, just like a market for human organs should not exist.[4]

The Digital Content Directive has been in force since 2019, and regardless of the comments made by the EDPS, it also recognizes situations where data is the *de facto* counter-performance (or consideration) of a contract. Article 3(1) of the Directive states "where the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader." The directive thereby enables individuals to rely on contractual remedies and data protection rights even after they have given their personal data in exchange for free access to social media platforms like Facebook. This should also be comparable to a situation when an individual sells his or her data to retailers and manufacturers, but their data protection rights remain protected.

Furthermore, *Václav Janeček* and *Gianclaudio Malgieri*, legal researchers from the University of Oxford and the Free University of Brussels, reasoned that there is no explicit prohibition on the sale of personal data in EU law.[5] Consequently, it is allowed, as long as the consumer consent fulfills the conditions set in the GDPR, and data subject rights are enabled. Janeček and Malgieri compare article 3(2) with article 7 and 8 of the Charter of Fundamental Rights of the European Union, noting that while article 3(2) prohibits making "human body and its parts as such a source of financial gain", there is no prohibition on personal data monetization. Albeit, the researchers conclude "commerce in some data is, and should be, limited by the law because some data embody values and interests (in particular, human dignity) that may be detrimentally affected by trade."[6]

The fallacy of data ownership

The discussion around personal data markets mixes up two different, equally important topics – data ownership and data monetisation. The former is about whether personal data can be an object of property law and the latter, whether an individual should sell their personal data and how they can exchange personal information for profit. The problem is that data ownership is still only conceptual. You can market data trade solutions with slogans like "it's your data, now get paid for it" (Clture) and "control and own your data" (Wibson – a data market), but legally you cannot own data, at least, not yet.

In the classical model of property law, the number of property rights is limited and so is the number of objects to which you can claim a property right (*numerus clausus* of legal objects).[7] The property rights are exercised against everyone, without a prior agreement, and for this reason need a stringent justification for the introduction of a new

right, in this case, the claim of ownership for personal data.

Sjef Van Erp, a private law professor at Maastricht University, uses Dutch law to give a simple example of why data cannot be an object of property law: "In Dutch law, ownership is defined as the most complete right concerning a physical thing. Consequently, if the thing is not physical, that particular object cannot be "owned". This does not mean that no primary right (in the sense of the maximum of powers, rights, privileges and immunities) exists, but it is not ownership, but entitlement."[8] Still, as seen from the Digital Content Directive, data can be a part of a contract and as such you do not need to own your data to share it or get benefit from it.

Talking about data ownership derails the conversation for two reasons. First, as explained, data ownership does not legally exist yet. As such, it gives false expectations to consumers. Second, it also gives the impression that once you sell your data, you would give away your right to privacy and data protection since property rights are transferable. If you sell your car, you will no longer have a right to that car. That is contrary to human rights that are inalienable and non-transferable. We would claim that similarly to the Digital Content Directive, selling data can be a contractual transaction, and as argued earlier, the right to privacy and data protection should remain intact after the sale of personal data.

Compliance in personal data trade

Annelies Moens, Managing Director of Privcore and Co-Founder of the International Association of Privacy Professionals Australia and New Zealand, also asserts that "companies and consumers cannot contract out of their legislative rights under data protection laws". Hence, companies working as intermediaries between consumers selling their data and companies buying the data, will need to make sure that they enable the data subject rights. Moens lists four questions for the intermediaries that highlight key factors for the GDPR.

First, she asks how do you enable data monetization that allows real choice and real privacy, and is not deceptive by design? The GDPR requires that valid consent is freely given, specific, informed and unambiguous (article 7). In addition to how a company requests consent for data processing, consumers also need to know who the data controller is. Consumers need to know which company buys the data, even when it happens via an intermediary, as well as the purpose of the data processing (preamble 42 GDPR).

The second question is, how to give consumers the opportunity to change their mind? Under the GDPR, the revocation of consent is a critical data subject right and helps give control back to consumers. Consent cannot be considered as freely given if the consumer is not able refuse or withdraw the consent "without detriment" (article 7, preamble 42 GDPR).

Thirdly, Moens poses the question how can an intermediary prevent the reselling of the consumer data. Companies could potentially resell data to another company with a higher profit. Is there a way to restrict this? Debbie Reynolds, US-based data protection expert, notes that aside from California, there are no legal limits to reselling data in the US. In her view, it is one of the biggest challenges for the personal data market. Even the purpose limitation clause in the GDPR, Article 5(1)(b), is easy to circumvent with broad descriptions of the purpose of data processing. Moens proposes to include "assurance clauses" in the data exchange contract to provide additional protection for consumers.

The fourth question is how do you handle consumer complaints? Intermediaries will need to continue to take responsibility even after the sale of personal data, and address consumer complaints. Under the GDPR, individuals in the EU have a right to complain to a supervisory authority, with some choice depending on where they reside, where they work or where the alleged issue arose. An individual can also choose a representative to complain on their behalf.

Lastly, Moens remarks that there are four main methods of data collection – direct, observed, indirect, and through inference. The most privacy risk occurs when data collection happens furthest from the consumer (i.e. through inference). Hence, sourcing data directly from the consumer poses the least privacy risk, as the consumer is most likely to be aware their data is being collected.

Conclusion

There is a lack of legal certainty on what happens when an individual sells his or her data in a personal data market, like Clture or Wibson. We would argue that since the EU privacy laws do not explicitly forbid the sale of personal data, it is allowed, as long as the conditions on freely given and revocable consent are met.

What creates confusion around data monetisation is the association with data ownership. An individual can transfer his or her right to property, but he or she cannot and should not transfer his or her right to privacy. Individuals should be able to sell their data by signing a contractual relationship with the buyer, and rely on the data subject rights to revoke their consent to data processing when needed.

It is important for intermediaries and companies who buy data from the individuals to assess how they ask for consent and how individuals can revoke it, how to prevent reselling of the data and how consumer complaints are handled.

AUTHOR

Sanna Toropainen is a legal researcher and co-founder at Muna.io, a Belgium-based company that is a data monetisation platform where consumers sell their data directly to companies in exchange for discounts or cash.

