Can a cashless society be compatible? with data protection? (2021)

Dr. Francis Graydon

Oct 2021

The debate about cash circulating in society has intensified in recent years. Rogoff (2016)[1] argues for the removal of large denomination paper currency implicated in serious criminal activity e.g. illegal drug activity and terrorism.[2] While the elimination of cash may reduce criminal activities, loss of financial privacy is a major concern.[3] In a cashless EU and UK, greater reliance on the GDPR[4] would become critical in protecting personal data and regulating data processing. Data protection authorities would certainly have to ensure that the GDPR was enforced robustly.

In assessing the compatibility of the cashless society with data protection, I will examine: (i) the nature of cash and a cashless society; (ii) the challenges of digital and electronic financial transactions for data protection; and (iii) consider the adequacy of the GDPR in the cashless society.

Cash and the Cashless Society

Cash refers to money (banknotes and coins) used continuously.[5] Cash transactions are private and privacy preserving. Firstly, they are peer-to-peer in nature and do not require intermediary involvement (e.g. banks). Secondly, they are also "permissionless".[6] The cash bearing party transacts freely without requiring permission.

[1] Kenneth S. Rogoff, The Curse of Cash (Princeton: Princeton University Press, 2016)

[2] C. Berg 'Financial Privacy'. In: The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change. Palgrave Studies in Classical Liberalism. (Palgrave Macmillan, Cham 2018) https://doi.org/10.1007/978-3-319-96583-3_11

[3] Karin Thrasher, 'The Privacy Cost of Currency' (2021) 42 Mich J Int'l L 403

[4] Regulation (EU) 2016/679 of the European Parliament and of the Council 27 April 2016

[5] J. Brito 'The Case for Electronic Cash Report' (Coin Center 2019) < https://www.coincenter.org/the-case-for-electronic-cash/#conclusion> accessed on 19 Oct 2021

[6] Stan Sater, 'Financial Privacy in a Cashless Society' (April 3, 2019) p 1 Available at SSRN: https://ssrn.com/abstract=3367610

Thirdly, cash allows for financial transactions with absolute anonymity.[7] Given these features, it is unsurprising that cash remains the most widely used payment instrument[8] and individuals seeking anonymity in financial transactions favour it.[9]

Electronic payments do not offer equivalent privacy. They are however pervasive, and in some EU Member States favoured over cash in day-to-day financial transactions.[10] The transactional nature of electronic payments is different and typically requires personal data (e.g. name). Electronic payments are completed using debit or credit cards and intermediated payment services relying on digitally based technology[11] such as mobile wallets (e.g. Apple Pay) and P2P systems (e.g. PayPal).[12]

The notion of a cashless society is an economic model in which *every* financial transaction will involve some digital data transfer.[13] One significant feature of this model is that an intermediary will be involved every time. They will keep records of every financial transaction a person ever makes. This likely exacerbates tensions over increased risks to data protection and the loss of financial privacy.

[7] Société Universitaire Europenne de Recherches Financieres ["SUREF"], 'Do We Need Central Bank Digital Currency?' Economics, Technology, and Institutions, 2018/2 SUERF Conf. Proceedings 28 (2018).

[8] G45 World Cash Report 4 (2018)

[9] ECB Crypto-Assets Task Force, Crypto-Assets: Implications for Financial Stability, Monetary Policy, and Payments and Market Infrastructures (Occasional Paper Series, No. 223/ May 2019).

[10] EDPB Guidelines 06/2020 on the interplay of the Second Payment Services Directive and the GDPR Version 2.0 Adopted on 15 December 2020, 18.

[11] W Donohue, Z Afridi, K Sokolyuk, T Bedwell, E York & A Salman, (2020). 'Cashless Society: Managing Privacy and Security in the Technological Age,' 1-6, 1 DOI:10.1109/SIEDS49339.2020.9106653

[12] Supra n 6, p 13.

[13] Supra n 11, p 1.

Challenges of electronic financial transactions for data protection

The financial data processed in electronic and digital transactions gives any party with access to it incomparable levels of personal and sensitive information about a person's life. This includes employment information, personal preferences, very sensitive health data, and sexual preferences.[14] Every time an electronic or digital payment is made a "digital financial trail"[15] is left, providing a ready-made data base. Anonymized financial records and credit card metadata have been used to re-identify shoppers 90% of the time[16]. This exemplifies the increased risks to data protection with one form of cashless transaction.

One consequence of shifting to a cashless society will be the recording and storage of everyone's personal data for every transaction throughout their entire life. This would be un-precedented and it is doubtful whether GDPR data subjects would tolerate the totality of their financial life being processed in this way. Their anonymity would be lost. However, this is what lies ahead in the cashless society. The violation of financial personal data "clearly involves serious impacts in the data subject's daily life"[17] and includes the risks of payment fraud. A continuous concern will be the risks caused by commercial attempts to commodify the financial personal data for profit previously carried out in "surveillance capitalism".[18]

[14] Supra n 2, p 181.

[15] Ibid.

[16] Yves-Alexandre De Montjoye, Laura Radaelli, and Vivek Kumar Singh, 'Unique in the Shopping Mall: On the Re-identifiability of Credit Card Metadata' (2015) Science 347 no. 6221.

[17] Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01 endorsed by the EDPB.

[18] Shoshana Zuboff. 'The age of surveillance capitalism: the fight for the future at the new frontier of power' (Profile Books 2019)

Adequacy of the GDPR

Recital 1 of the GDPR[19] highlights that protection of natural persons in relation to the processing of their personal data is a fundamental right. "Under Article 8(1)[20] of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1)[21] of the Treaty on the Functioning of the European Union (TFEU) *everyone* has the right to the protection of personal data concerning him or her".[22] Within the EU and UK, the operation and enforcement of the GDPR will become critical in a cashless society. However, it is not possible to say whether sector specific regulation will need to be strengthened further.

The EDPS identifies three "foreseeable" data protection challenges that lie ahead in a society that relies less on physical cash.[23] These are based on (i) the proposed introduction of a "digital Euro" or Central Bank Digital Currency (CBDC) by the European Central Bank (ECB) for cashless payments and (ii) the development of cryptocurrencies by private companies like Facebook. Firstly, there will be greater risks due to an increased number of intermediaries offering payment services and digital wallets.[24] Secondly, there will be an increase in the amount of personal data collected.[25] Thirdly, poor design in the underlying technological infrastructure may worsen the data protection issues that already exist in the "digital payment landscape".[26]

[19] Supra n 3, Recital 1.

[20] Charter of Fundamental Rights of the European Union, art. 8, Dec. 18, 2000, 2000 O.J. (C 364) 10

[21] Consolidated versions of the Treaty on European Union and the Treaty on the Functioning of the European Union (TFEU) [2016] OJ C202/1

[22] Supra n 4, Recital 1.

[23] European Data Protection Supervisor 'Central Bank Digital Currency' https://edps.europa.eu/presspublications/publications/techsonar/central-bank-digital-currency_en (accessed on 19 Oct 2021)

[24] Ibid.

[25] Ibid.

[26] Ibid.

In particular, the personal data from transactions may be used illegally for cross-selling enterprises and credit assessments.[27] Companies using any cashless payment method (e.g. digital coins or cryptocurrencies) are legally obligated to comply with Article 25 (Data protection by design and by default)[28] of the GDPR and implement "appropriate technical and organisational measures".[29] This is the starting point, and it is unclear whether compliance with these specific principles in the GDPR will be achieved.

CONCLUSIONS

Technological developments and changes in society will always alter the stability and limits of data protection in compound and erratic ways. In a cashless UK & EU, the GDPR gives citizens a baseline framework to safeguard their data protection rights. The regulation of electronic payments will inevitably have to be more robust and comprehensive. This will have to include at least three elements: (i) better design in the technological infrastructure that underlies the financial payment system; (ii) separate and more comprehensive enforcement of the financial sector by data protection regulators; (iii) greater guidance from the EDPB on how concepts should be applied with new technologies.[30] It is not possible to say that a cashless society can ever be compatible with data protection. There are clear tensions and vulnerabilities in the relationship and no clear signs that they are reconcilable in the short term.

[27] Ibid.

[28] Ibid.

[29] Supra n 3, Article 25

[30] Ibid Article 25(1)

[31] B.S. Jiménez-Gómez, 'Risks for Blockchain for data protection: a European approach' (2020) Santa Clara High Technology Law Journal, *36*(3), 281-343. https://www.proquest.com/scholarly-journals/risks-blockchain-data-protection-european/docview/2404652578/se-2?accountid=10673