Economics Bulletin

Volume 39, Issue 2

Some economic consequences of the GDPR

Darcy W E Allen
RMIT University, RMIT Blockchain Innovation Hub

Alastair Berg
RMIT University, RMIT Blockchain Innovation Hub

Chris Berg
RMIT University, RMIT Blockchain Innovation Hub

Brendan Markey-Towler
RMIT University, RMIT Blockchain Innovation Hub

Jason Potts
RMIT University, RMIT Blockchain Innovation Hub

Abstract

The EU General Data Protection Regulation (GDPR) is a wide ranging personal data protection regime of greater magnitude than any similar regulation previously in the EU, or elsewhere. In this paper, we outline how the GDPR impacts the value of data held by data collectors before proposing some potential unintended consequences. Given the distortions of the GDPR on data value, we propose that new complex financial products—essentially new data insurance markets—will emerge, potentially leading to further systematic risks. Finally we examine how market-driven solutions to the data property rights problems the GDPR seeks to solve—particularly using blockchain technology as economic infrastructure for data rights—might be less distortionary.

Citation: Darcy W E Allen and Alastair Berg and Chris Berg and Brendan Markey-Towler and Jason Potts, (2019) "Some economic consequences of the GDPR", *Economics Bulletin*, Volume 39, Issue 2, pages 785-797
Contact: Darcy W E Allen - darcy.allen@rmit.edu.au, Alastair Berg - alastair.berg@rmit.edu.au, Chris Berg - christopher.berg@rmit.edu.au, Brendan Markey-Towler - brendan.markeytowler@uqconnect.edu.au, Jason Potts - jason.potts@rmit.edu.au.
Submitted: October 21, 2018. **Published:** April 03, 2019.

1. Introduction

Personal data is an economic good that may be valuable, and when linked to other data may create further value. Data assets held by firms have economic value. That value can be changed by public policy targeted at the use or protection of that data. This paper examines the potential economic consequences of the European Union (EU) General Data Protection Regulation (GDPR). The GDPR provides for a range of regulatory controls on data access, rectification, the right to withdraw consent, erasure, and portability. This is a regulation of significant scope that provides for far greater data protections and penalties than competing jurisdictions, including the United States (see Safari 2016).

The GDPR is a wide ranging personal data protection regime that came into effect in late May 2018. The territorial scope of the GDPR is significant, with the regulation applying to the "processing of personal data of data subjects who are in the [European] Union", (Council of the European Union 2016, 110) no matter where the processing of data takes place. In effect, this means that the GDPR applies to vastly more data collection activities than its predecessor, the Data Protection Directive, which was applied as based on the location of the data processing, rather than the location of the data subject (Voss 2017). In addition, the EU has taken an 'omnibus' approach to privacy law and data protection, in stark contrast to the multitude of relevant regulations and agencies in the United States (Safari 2016). The penalties to be applied for infringements of the regulation are equally significant, ranging up to EUR20 million or four per cent of global revenue, whichever is higher (Council of the European Union 2016, 246). The GDPR law tries to use regulatory powers to create a high-powered threat incentive to induce firm behaviour in the direction regulators intend, based on their interpretation of voter preferences. Voters want privacy and control of their data, and so European regulators have sought to enact that wish.

The GDPR changes the value of personal data assets collected by firms who have previously sold that data to third parties. Data subjects will now in effect hold a zero strike price call option over that data because they can withdraw the right of data collectors to use their data. Thus the value of that data asset the collector holds now depends on the existence of continued data subject consent. This creates an economic incentive for data collectors to hedge the risk associated with holding that data asset with novel financial instruments that can be exchanged on secondary markets. Therefore we argue a potential economic consequence to that well-meaning regulatory action—through its distortive impact on the value of data property rights—is the creation of secondary insurance data markets. These new markets may themselves have second-order and disruptive consequences, including issues of systematic stability, analogous to financial markets. Using the terminology of Baumol (1990) this is a form of 'unproductive

entrepreneurship' in response to the blanket distortions introduced by the GDPR. We suggest that alternative market-based approaches to data property rights problem—including though the use of blockchain—might be comparatively less distortionary, enabling a more contract-based approach. Using blockchain technology as an infrastructure for the transaction of data property rights might more organically address privacy concerns and data protections. Organically developed solutions might provide better solutions to similar problems that the GDPR attempts to address while avoiding some distortionary consequences.

Section 2 examines some of the main regulatory implications of the GDPR, including the right to erasure of personal data. Section 3 examines the effect the regulation may have on data markets, including the creation of novel financial instruments that data collectors might create to rationally hedge regulatory risk. Section 4 examines market-based alternatives to the GDPR using blockchain technology. Section 5 concludes.

2. What does the GDPR do?

The GDPR uses a broad definition of personal data which relates to any "identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person" (Council of the European Union 2016, 111). Interesting to note is that while the regulation encourages the pseudonymisation of personal data where applicable, that data is still considered personal data under the regulation (Council of the European Union 2016, 16). This has implications for personal data which has been pseudonymised using cryptographic hash functions, such as SHA-256.[1] Similarly, public and private keys, used in asymmetric cryptography as utilised by public blockchains such as Bitcoin and Ethereum, are expected to be considered personal data for the purposes of the GDPR (Schwerin 2018).[2]

---

[1] Asymmetric cryptography, also known as public key cryptography, uses a pair of keys – one private and one public – to sign transactions and receive payments in the transaction of cryptocurrencies like Bitcoin and Ethereum. A private key is used to prove ownership over funds and sign transactions, while a public key, derived from the private key, is used to generate an address with which users can receive payments (Antonopoulos 2017).

[2] SHA-256 is a hash function used in the Bitcoin cryptocurrency protocol. A cryptographic hash function takes a data string of arbitrary length and converts it into an output of fixed length. The properties of hash functions that make them useful for cryptocurrency protocols, as well as pseudonymisation, are that each arbitrary input string produces a unique output, while it is computationally infeasible to calculate an input with a given output (see Narayanan et al. 2016).

The regulation has as its objectives the establishment of "rules relating to the protection of natural persons" and the "fundamental rights and freedoms of natural persons" as they relate to personal data, as well as "the free movement of personal data" (Council of the European Union 2016, 108). To this end, a number of rights and responsibilities are established as they relate to data subjects, as well as data controllers and processors respectively. A complete audit of personal data rights as set out in the GDPR is beyond the scope of this paper, however the rights of data subjects include that of data access, rectification, the right to withdraw consent, erasure and portability. The right to erasure is one of the more well-known aspects of the GDPR, and is also known as the right to be forgotten in the regulation. When exercised, this right requires data processors to take steps to erase personal data collected from data subjects "without undue delay" (Council of the European Union 2016, 140). It should be noted that some of these rights are not absolute, with the regulation stating that the protections of personal data must be "considered in relation to its function in society" (Council of the European Union 2016, 3). This statement refers to requirements such as 'know your customer' (KYC) obligations in the financial services industry, and other public protection measures which are carried out in the "general interest" (Council of the European Union 2016, 17).

The responsibilities of data controllers and processors as set out in the GDPR include technical and organisational requirements of data protection by design, the "lawfulness, fairness and transparency" (Council of the European Union 2016, 117) of data processing, the processing of data only for the purposes for which it was collected, and the protection of personal data "against unauthorised or unlawful processing" (Council of the European Union 2016, 118). In addition, it is the responsibility of data controllers and processors to obtain explicit consent, including the communication to data subjects of the purposes for which personal data is collected. Finally, data controllers and processors are obliged to designate a data protection officer (DPO) who shall "monitor compliance with this Regulation" (Council of the European Union 2016, 173), and act as a point of contact in the event of a data breach.

The introduction of the GDPR should be seen in the context of two recent high profile legal cases involving Google and Facebook, which addressed the right to be forgotten and the nature of the consent given to data collectors and processors (see Safari 2016). The GDPR should also be considered from the perspective of recent public discourse about data collection and its use in elections and marketing, such as that seen in the use by Cambridge Analytica of Facebook data during the 2016 United States Presidential Election. Equally important to note in the context of this new regulation is the development of market driven technology solutions which may allow data subjects to have greater control, ownership and portability as it relates to their personal data. The concept of self-sovereign identity is being actively explored by firms who are examining how emerging technology, including blockchain and other distributed ledgers,

can address privacy concerns and data protections in the market, rather than through distortionary regulation (see Section 4).

3. How the GDPR creates data markets

The regulatory interventions of the GDPR are not costless. The interventions shift the risk profile of firms worldwide who manage personal data and operate in data markets. The GDPR might not only cause organisations to reduce their product offerings to European citizens, but also incentivise new financial products to mitigate the risks (the operational risk of individuals exercising their new right to be forgotten or erasure).

Consider the business model of organisations who collect the data of customers in the course of their operations. In some circumstances firms will collect personal data from customers for commercial purposes, seeking to ascertain some level of assurance over a debtor's ability and willingness to repay in a credit relationship for example. Similarly, firms in regulated industries must collect personal data from customers to satisfy legislative and regulatory requirements, such as KYC obligations in the financial services industry. Both commercial and regulatory reasons endogenous to the transaction instigate the collection of the personal data of individuals. However, circumstances of firms collecting data which is exogenous to the transaction also abound. Zero-price online services for the user are paid for primarily by the collection of the personal data of users which is then sold to third parties. This data exogenous to the transaction is personal data which firms place a positive value on. This personal data is regularly part of the mutually beneficial relationship between firms and customers. While there is uncertainty surrounding the value of this data—it is an entrepreneurial effort for data collectors to bundle that data and sell on to third parties—there is a further distortionary uncertainty that the GDPR has introduced that those companies did not previously face.

The GDPR creates a new economics of privacy regulation in personal data markets. Previously, firms who collected personal data derived positive value from said data, such as in the form of advertising revenue. The collection of personal data from users—such as social media users—allowed third party organisations to gain insight into their personalities, past experiences and purchasing habits (Howells and Ertugan 2017, Tuten and Solomon 2017). This personal data in turn creates the ability for targeted advertising which creates revenue. The introduction of a right to be forgotten or of erasure in the GDPR or similar regulations significantly shifts the value of that personal data by requiring it to be erased on request at any time.

The GDPR creates an option-like instrument that can be exercised by data subjects. The data subject is generally able to exercise the option to purchase data assets as collected by firms at

no cost; this is analogous to a zero strike price call option held by the data subject.[3] Therefore the value of personal data assets as collected by firms will be derived from the actions of the data subject who acts in accordance with their rights as set out in the GDPR. Personal data collected during business may have value for a firm if data subjects act in some way, but may have zero, or even negative value if they act in another.

Consider an example where personal data has some positive value from the perspective of a data collector. During a transaction, a data subject may consent to have their personal data collected and used for the purposes of marketing; they agree to have their personal data passed on to third parties who may use it for market research, or for targeted advertising. Given the GDPR, the data subject, up until a (unknown) point in time when the data subject may choose to exercise this zero strike price call option and withdraw consent to their personal data being used, that personal data holds value for the organisation that is acting as a data collector. The GDPR therefore has distorted the property rights in a previously voluntary relationship between data subjective and collector.

In contrast, personal data may have zero, or even negative value, from the perspective of a data collector. As in the example above, a data subject may consent to their data being collected and subsequently used by third parties. Again, the data subject holds a zero strike price call option on that data; at any point, they have the option to withdraw consent to that data being sold to third parties. If the data subject exercises this option-like instrument—effectively purchasing a data asset at no cost—the value of that data may be zero, or even negative, from the perspective of the data collector. The data collector can no longer sell the data asset to a third party. The personal data may even have some negative value because the organisation has the obligation to erase the personal data, and faces substantial penalties if they do not do so in accordance with the regulation, as well as the previous contractual relationships they have made in data markets based on their perceived value of that data.

Some simple reasoning illustrates that the GDPR may have the unintended consequence of incentivising the expansion of financial markets by the extension of risk-sharing services to the collectors of data.

---

[3] In effect this would mean that this is an American option, as the option can be exercised any time prior to some expiry data. This is in contrast to a European option which can only be exercised at the expiry date (see Black and Scholes 1973).

Suppose that a given data has value v to a collector of data if used and the cost of its collection is c. Suppose also that the value of not collecting data is simply zero. Suppose further, without great loss of generality, that preferences over data collection are linear in these two objects. If this is so, then there is an incentive to collect this data if and only if $v \geq c$.

The GDPR introduces uncertainty into these preferences by granting the subject of collected data an option to withdraw consent to the use of their data at any time. For simplicity, we might imagine that this transforms preferences over the collection of data to a standard von Neumann-Morgenstern utility function over two possible states. For simplicity also, we will consider only the right to withdraw consent to the use of data and not the right to have all data collected erased.

If the option to withdraw consent to the use of data is exercised with a subjective probability $1 - p$, then we might say that the value of that collected data being zero is associated with a subjective probability $1 - p$. The value v of the collected data can then be realised only with a probability p. If the cost of collecting that data is constant relative to the exercising of the option to withdraw consent to use that data, and preferences are of a standard linear von Neumann-Morgenstern form in these objects, then there is an incentive to collect data if and only if

$$p \geq \frac{c}{v}$$

Since $p \in [0,1]$, the GDPR will disincentivise the collection of data because the costs of data collection must now be a smaller proportion of value obtained to provide an incentive for that data to be collected than otherwise. This might be an unintended consequence of the regulation in some quarters and not in others, but it is fairly obvious. There is another, less obvious, consequence of the GDPR which is almost certainly unintended. Let us suppose that the condition above is indeed met and there is an incentive to collect data. If this is the case, then there may be an incentive to take out insurance on the use-value of collected data. Suppose that insurance may be taken out on the value of data at premium i which pays out v if consent is withdrawn by the subject of the data collected. This has the effect of removing the uncertainty of realising value v from linear preferences over collecting data, though adding to the cost of collecting that data. In this case, there is an incentive to take out insurance on the use-value collected data if and only if

$$v - i - c \geq pv - c$$

Where, by assumption, we have that $pv - c \geq 0$. So, rearranging, there is an incentive to take out insurance on the use-value of collected data if and only if

$$(1 - p)v \geq i$$

which is a standard insurance condition. There is an incentive to take out insurance on the use-value of collected data if and only if it costs less than the expected loss of value if consent to use collected data is withdrawn.

Now suppose an insurer believes that the probability for consent for the use of data being withdrawn and the value of the data being paid to the collector thereof is q. Let us assume they are a standard profit maximiser and the value of not providing insurance in this particular is simply zero. There will be an incentive to supply insurance to data collectors subject to the right of veto created by the GDPR if and only if

$$i \geq qv$$

Opportunities for mutually beneficial exchange—opportunities for market exchange—will therefore exist, and a market is likely to arise, if there is a divergence of beliefs about the likelihood that consent will be withdrawn for the use of collected data

$$(1 - p) \geq q$$

Now note that this market is only strictly (as opposed to weakly) feasible if and only if the right of veto over the use of data collected is given to the subject of that data (for only then is it the case that $p \leq 1$). Therefore, the GDPR has the capacity to facilitate an expansion of financial markets into the provision of risk-sharing services to data collectors. As this market develops, we can expect the insurance premium to converge at the margin toward the fair premium $i = (1 - p)v$ and the market toward equilibrium such that $(1 - p) = q$ at the margin.

The impact of the GDPR on data collectors is substantial uncertainty over the value of the assets they hold. They may be incentivised to mitigate this risk. Data collectors who have purchased personal data from users—including through providing zero-price or discounted services—are incentivised to buy new insurance contracts because some of their data assets will have a zero or negative value in the future. It logically follows that new financial products might then be developed to hedge that risk. Indeed, third parties will be incentivised to create new markets because of new potentially mutually beneficial trades to be captured. Most

generally, this might include insurance contracts which will pay out in the event data subjects exercise their rights set out in the GDPR.

There are several different ways to interpret these unintended consequences of the GDPR in the form of new financial instruments to offset risk. First, while third parties may be incentivised to create new markets to offset risk, these are not data markets. Those new financial markets would be a form of 'unproductive entrepreneurship' (Baumol 1990) in the sense that they are the result of distortionary changes in the 'rules of the game' that shift entrepreneurial endeavour from 'productive' entrepreneurial activities to 'unproductive' ones. Second, there may be more complex financial markets that evolve due to incentives to take out reinsurance and diversify exposures. Data-Backed Securities (DBS) are one possible innovation in financial products that could be developed to both manage risk, as well as create immediate revenue streams for data collectors. An uncertain series of future revenue streams is in this way converted to a single certain source of revenue. Risk is then transferred from the data collector to another party via a DBS market. Collateralised Data Obligations (CDO) may also emerge, with data 'originators' packaging personal data into tranches of varying risk of consent withdrawal. The risk of consent withdrawal, and therefore the pricing of DBS and CDO products, will presumably be derived from actuarial pricing of consent withdrawal, in addition to exogenous shocks to the secondary data market. Such as it is we have the incentives for the creation of secondary data derivative markets. Together, these interpretations suggest the need to examine alternative institutional solutions to the problems the GDPR seeks to solve.

4. Market alternatives to the GDPR

The GDPR principles of privacy by design, disclosure minimisation and portability are largely analogous to those which inform organisations developing, and advocates for, self-sovereign identity solutions (see in particular Allen 2016, Loffreto 2012, Searls 2012). Such market derived solutions to enhance individual privacy and data protection should be compared to government interventions such as the GDPR due to the potential for unintended and destabilising consequences. In addition to the potential consequences set out above, privacy regulations might also be anticompetitive due to the inability of smaller firms to comply with their requirements. For instance obtaining consent to collect data from individuals disproportionately effects smaller firms (Campbell et al. 2015), and may allow companies like Facebook and Google to extend their dominance over smaller rivals (Cerulus and Scott 2018, Schechner and Kostov 2018).

Non-regulatory solutions allowing data protections and addressing privacy concerns should be examined, including the use of technology to allow data subjects greater control over how they

disseminate personal information. Market alternatives to the GDPR and other regimes have the potential to allow for privacy and data protections without the distortionary effects of a blanket approach to the preferences of individuals in how they trade their own data. Research into the concept of self-sovereign identity, and the use of blockchain and distributed ledger technology is one such promising avenue. As discussed in Berg et al. (2017) self-sovereign identity provides a way for the personal data of individuals to be cryptographically secured, and allows them ownership and graduated permissioning control over their personally identifiable information. In addition, such an identity model allows verifying parties confidence in the attestations of a counterparty (Mühle et al. 2018), while denying potentially malicious third parties from associating multiple transactions, and hence relating them to any particular individual (Der et al. 2017).

The control over personal data, as well as its value for the individual with access to data markets has been of interest to researchers since before the advent of blockchain (Schull 2005). More recently, the technology has been examined in its use in enabling new classes of financial assets (Corbet et al. 2018, Phillip et al. 2018, Urquhart 2017), as well as for its potential in providing greater privacy and anonymity in the context of financial transactions (Conley 2017, Genkin et al. 2018). Our interest here is in the technology's use in data management in the form of self sovereign identity, and the potential for the emergence of new types of data markets. In general, self-sovereign identity allows for an environment where organisations who typically rely on the personal data of their users 'can't be evil' (Ali 2017). Blockchain technology, the class of distributed digital ledgers first developed for the cryptocurrency Bitcoin (see Antonopoulos 2017, Nakamoto 2008), is one of the innovations which may provide the technological foundations for data models which allow the individual control over, and potentially the option to monetize, their data (Catalini and Gans 2016).

Using blockchain technology, as well as allied technologies such as zero-knowledge proofs, individuals can prove some fact about themselves without revealing what that fact is (Swan 2015), preventing a counterparty from holding their personal data in the first place. For instance, an individual can prove they are old enough to purchase some restricted product, without revealing to a counterparty what their age actually is. Similarly, individuals can pass along 'just enough' personal information to allow a personal transaction to proceed, greatly reducing the amount of redundant information organisations typically hold about their customers. Such data models also allow for individuals to audit who is accessing their data, while relieving organisations of the responsibilities which are involved with the custody of personally identifiable information and preventing data breaches (Zyskind and Nathan 2015).

Compared to the regulatory approach of the GDPR—that attempts to solve issues of privacy and portability through regulatory direction, creating additional uncertainty for data

collectors—a more decentralised approach to the property rights of data markets may be preferable. Individuals who hold their own data property rights can decide under what conditions they wish (or otherwise) to sell those rights to data collectors. The contracts that are signed—perhaps through smart contracts—would provide greater certainty for data collectors to sign subsequent contracts with third parties, including because those contracts are not open to latter opportunistic behaviour. Rather than treating the preferences of individuals and their data rights evenly across the population, a more decentralised approach would focus on the contracts that individuals engage in and how they wish to execute their rights. To be sure, this market and contract-based approach is not costless—including the transaction costs of negotiating these individual contacts—but technologies such as blockchain may substantially lower the costs of deploying such data market contracts. It is an open question over the relationship between the GDPR approach and the market-based blockchain approach we have outlined here. It may well be that the GDPR spurs the creation of separate data markets based on decentralised governance of data property rights—but it may similarly be the case that GDPR-like regulations inhibit the ability of individuals to sell or lease their data.

We can see quite readily how this alternative approach might create data markets in which the creation of property rights for the subjects of data leads to mutually beneficial exchange. Again, if v is the value created by some data for a user thereof, and c the cost of its collecting, but now f is a fee which must be paid to the subject of that particular data for the transfer of property rights to it, the user has an incentive to collect that data as long as $v - c \geq f$. Supposing that the cost to the subject of the data of the decrease in their privacy is l, they have an incentive to sell their data as long as $f \geq l$. Hence there will be scope for mutually beneficial exchange, and data markets created by the allocation of property rights to the subjects of data as long as

$$v - c \geq l$$

Notice that where the effect of government intervention in the form of the GDPR was to introduce uncertainty and an incentive for unproductive entrepreneurship to emerge, the effect of this intervention, through blockchain-based *innovation*, is to create a market for mutually beneficial exchange. In particular, this approach recognises that the loss of privacy *does* create a cost for the subject of collected data, and then by allocating property rights ensures that they must be compensated for that cost. But further, it ensures that whether data is collected or not by potential users truly reflects the value of that data, for market exchange can only occur if the profit to be obtained from using data is sufficiently large to compensate the subject thereof for their loss of privacy. Where the effect of the GDPR is to create uncertainty which erodes the value of data, and incentives for unproductive entrepreneurship without offering subjects of data the opportunity to benefit from its transfer, the effect of blockchain-based innovation

which creates property rights is to create a market where data is transferred only when it is mutually valuable to all parties involved.

5. Conclusion

Government intervention into what are deemed to be instances of market failure often has unintended consequences when rational market agents endeavour to offset the additional risks or costs the regulatory intervention imposes. A well-known instance of this is the Global Financial Crisis of 2007-08, and the role of Wall Street investment banks in this period is well documented by financial and economic historians. Accusations of greed, immorality and excess, and the effects of 'neoliberal deregulation' fill the pages of accounts of the period (Crotty 2009, Sykes 2010). However, what many of these accounts of the crisis fail to emphasise is the role of poorly designed capital requirements, which incentivised financial institutions to trade in significant amounts of poorly understood Mortgage-Backed Securities, Collateralised Debt Obligations, and related financial products (Friedman and Kraus 2011). Similarly, global KYC regulations designed to first combat drug related crime, and later to counter terrorism financing (Stanley and Buckley 2016) have seen financial institutions worldwide 'de-risk'; reducing their product offerings to certain individuals around the world, contributing to the massive amounts of 'unbanked' and 'underbanked' (Durner and Shetret 2015).

It seems entirely reasonable to suppose that the legislative endeavours of the GDPR, as it seeks to attain through regulatory intervention privacy-for-free by imposing constraints on activity and therefore costs on firms into their existing business models and capital investments, will induce a strategic counter-response as firms rationally (under competition) seek to offset or offload those imposed costs and burdens. We predict that one such response will be the creation of insurance products (i.e. new markets) to allocate that newly created risk to those most efficiently able to bear it. It would further follow that such products will become tradable (possibly securitised) financial instruments. Whether this growth in the financial sector induced by enactment and enforcement of the GDPR will ultimately be economically destabilising, or innovation chilling, remains to be seen, but past evidence of similar regulatory interventions suggests we ought to expect that this new EU regulation might be costly.

The potential distortionary impacts of regulations such as the GDPR should be compared institutionally to market-based solutions. Through the application of blockchain technology as new economic infrastructure for property rights, data subjects and data collectors may be able to better deliver privacy and data protections that individuals seek. There are potential benefits to such as blockchain-based system of data markets, including the bespoke nature of

contracting and more productive forms of entrepreneurial activity to discover mutually beneficial forms of economic exchange.

6. References

Ali, Muneeb. 2017. "Can't Be Evil: The Google-Inspired Case for Blockchain." *Coindesk*, 27 August 2017. Accessed 7 March 2019. https://www.coindesk.com/cant-evil-google-inspired-case-blockchain-tech.

Allen, Christopher. 2016. The Path to Self-Sovereign Identity. Accessed 12 February 2018.

Antonopoulos, A.M. 2017. Mastering Bitcoin: Programming the Open Blockchain: O'Reilly Media.

Baumol, William J. 1990. "Entrepreneurship: Productive, Unproductive, and Destructive." *The Journal of Political Economy* 98 (5):893-921.

Berg, Alastair, Chris Berg, S. Davidson, and Jason Potts. 2017. "The institutional economics of identity." *SSRN*.

Black, Fischer, and Myron Scholes. 1973. "The pricing of options and corporate liabilities." *Journal of political economy* 81 (3):637-654.

Campbell, James, Avi Goldfarb, and Catherine Tucker. 2015. "Privacy regulation and market structure." *Journal of Economics & Management Strategy* 24 (1):47-73.

Catalini, Christian, and Joshua S Gans. 2016. Some simple economics of the blockchain. National Bureau of Economic Research.

Cerulus, Laurens, and Mark Scott. 2018. "Europe's new privacy rules: 1 month in, 7 takeaways." *Politico*, 25 June 2018. Accessed 8 March 2019. https://www.politico.eu/article/gdpr-europe-new-privacy-rules-7-takeaways/.

Conley, John P. 2017. Blockchain Cryptocurrency Backed with Full Faith and Credit. In *Vanderbilt University Department of Economics Working Papers*: Vanderbilt University Department of Economics.

Corbet, Shaen, Andrew Meegan, Charles Larkin, Brian Lucey, and Larisa Yarovaya. 2018. "Exploring the dynamic relationships between cryptocurrencies and other financial assets." *Economics Letters* 165:28-34.

Council of the European Union. 2016. Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). In *5419/16*, edited by Council of the European Union.

Crotty, James. 2009. "Structural causes of the global financial crisis: a critical assessment of the 'new financial architecture'." *Cambridge journal of economics* 33 (4):563-580.

Der, Uwe, Stefan Jähnichen, and Jan Sürmeli. 2017. "Self-sovereign Identity - Opportunities and Challenges for the Digital Revolution." *arXiv preprint arXiv:1712.01767*.

Durner, Tracey, and Liat Shetret. 2015. Understanding Bank De-Risking and its Effects on Financial Inclusion: An exploratory study.

Friedman, J., and W. Kraus. 2011. *Engineering the Financial Crisis: Systemic Risk and the Failure of Regulation*: University of Pennsylvania Press, Incorporated.

Genkin, Daniel, Dimitrios Papadopoulos, and Charalampos Papamanthou. 2018. "Privacy in decentralized cryptocurrencies." *Communications of the ACM* 61 (6):78-88.
Howells, Karen, and Ahmet Ertugan. 2017. "Applying fuzzy logic for sentiment analysis of social media network data in marketing." *Procedia Computer Science* 120:664-670.
Loffreto, Devon. 2012. What is "Sovereign Source Authority"? *The Moxy Tongue*.
Mühle, Alexander, Andreas Grüner, Tatiana Gayvoronskaya, and Christoph Meinel. 2018. "A survey on essential components of a self-sovereign identity." *Computer Science Review* 30:80-86.
Nakamoto, Satoshi. 2008. "Bitcoin: A peer-to-peer electronic cash system."
Narayanan, A., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*: Princeton University Press.
Phillip, Andrew, Jennifer SK Chan, and Shelton Peiris. 2018. "A new look at Cryptocurrencies." *Economics Letters* 163:6-9.
Safari, Beata A. 2016. "Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection." *Seton Hall L. Rev.* 47:809.
Schechner, Sam, and Nick Kostov. 2018. "Google and Facebook Likely to Benefit From Europe's Privacy Crackdown." *The Wall Street Journal*, 23 April 2018. Accessed 8 March 2019. https://www.wsj.com/articles/how-europes-new-privacy-rules-favor-google-and-facebook-1524536324.
Schull, Jonathan. 2005. "Predicting the evolution of digital rights, digital objects, and digital rights management languages." Proceedings of the 2nd International ODRL Workshop, Lisbon, 2005.
Schwerin, Simon. 2018. "Blockchain and Privacy Protection in the Case of the European General Data Protection Regulation (GDPR):A Delphi Study." *The Journal of the British Blockchain Association* 1 (1):1-75.
Searls, Doc. 2012. Sovereign-source vs. adminstrative identity.
Stanley, Rebecca L, and Ross P Buckley. 2016. "Protecting the west, excluding the rest: The impact of the AML/CTF regime on financial inclusion in the pacific and potential responses." *Melb. J. Int'l L.* 17:83.
Swan, M. 2015. Blockchain: Blueprint for a New Economy: O'Reilly Media.
Sykes, T. 2010. Six Months of Panic: How the Global Financial Crisis Hit Australia: Allen & Unwin.
Tuten, T.L., and M.R. Solomon. 2017. *Social Media Marketing*: SAGE Publications.
Urquhart, Andrew. 2017. "Price clustering in Bitcoin." *Economics letters* 159:145-148.
Voss, W Gregory. 2017. "European union data privacy law reform: General data protection regulation, privacy shield, and the right to delisting."
Zyskind, Guy, and Oz Nathan. 2015. "Decentralizing privacy: Using blockchain to protect personal data." 2015 IEEE Security and Privacy Workshops.