2019

Dr. Strangeblock or: How I Learned to Stop Worrying and Love the GDPR

Kieran Ensor

Dr. Strangeblock or: How I Learned To Stop Worrying And Love the GDPR[1]

I. Introduction

As concern surrounding data collection, data privacy, and data protection increases exponentially around the world, we are fast realizing how steep a hill proper regulation presents.[2] Most significantly, the recent proliferation of data breaches[3] around the world has spotlighted the mass amount of data that is created, collected, stored, sold, and otherwise utilized on a daily basis.[4] Certainly, the collection of personal data points makes human existence easier in seemingly infinite ways, but when it leads a consumer to see an advertisement for an item she did not previously search for—but needs[5]—the creeping feeling of big-brother watching you sets in.[6] Such occurrences are no longer thought of as incidental,[7] and a new trend of what can be called "Privacy Nihilism" is emerging, where the belief is that the war for our data is lost and resistance seemingly futile.[8]

On the other side of this data privacy coin sit those who believe all is not lost and the war can yet be won through the means of regulation. One notable example is the European Union and

[1] *See* DR. STRANGELOVE OR: HOW I LEARNED TO STOP WORRYING AND LOVE THE BOMB (Columbia Pictures 1964) (a satirical take on the cold war and the fear of mutually assured destruction as a deterrence for all-out nuclear war).

[2] *See* Ian Bogost, *Welcome to the Age of Privacy Nihilism*, THE ATLANTIC (August 23,2018) https://www.theatlantic.com/technology/archive/2018/08/the-age-of-privacy-nihilism-is-here/568198/

[3] *See infra* note 42.

[4] For example, it is estimated that 2.5 quintillion bytes of data are created daily. *See* Bernard Marr, *How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read*, FORBES (May 21, 2018, 12:42 AM), https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#6b46bfd160ba.

[5] "[a] woman has a bottle of perfume confiscated at airport security, and upon arrival sees a Facebook ad for local perfume shops", Bogost, *supra* note 2.

[6] George Orwell, NINETEEN EIGHTY-FOUR (1949).

[7] Bogost, *supra* note 2.

[8] *Id.* ("There is no escaping the machinery of actual life, no matter how many brows get furrowed over or tweets get sent about it . . . the opponent in the data-privacy invasion is not a comic-book enemy of fixed form, one that can be cornered, compromised, and defeated. Instead it's a hazy murk, a chilling, Lovecraftian murmur that can't be seen, let alone touched, let alone vanquished.").

the General Data Protection Regulation (GDPR).[9] Article 1 of the GDPR states: "[t]his regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".[10] Regardless of the perspective, it is clear that the need for data protection is now at the forefront of conversation and will not disappear anytime soon.

The GDPR's expansive view on data protection raises many questions concerning its practicality. Take, for instance, Article 17 of the GDPR.[11] Known more commonly as the "Right to Erasure" or "The Right to be Forgotten", this provision allows an EU citizen to request deletion of personal data collected by any business that serves or collects information on citizens the Union.[12] But what happens when this protective measure clashes with a technology that renders the erasure of data collected impractical or even impossible? That is the focus of this paper. Though the GDPR is in its nascent stage—having come into effect on May 25, 2018—an inevitable clash with another fast-growing technology is imminent.[13] That technology is blockchain. Because a fundamental principle of blockchain is immutability,[14] the idea that data stored on a blockchain can be deleted, in compliance with Article 17, is idealistic at best. Inevitably, then, legal disputes will arise out of this incompatibility. This paper will discuss: blockchain technology and Article 17 of the GDPR; analyze the issues of justiciability surrounding the conflict; and suggest a method to resolve this type of dispute. To highlight the issue, this paper will use a hypothetical scenario that presents a common instance where the overarching problem will occur— credit card

[9] 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, and repealing Directive 95/46/EC (General Data Protection Regulation) [hereinafter GDPR], 2016 O.J. L 119/1.

[10] *Id.* at art. 1.

[11] *Id.* at art. 17.

[12] *Id.* This is true but subject to some exceptions. *See infra* notes 147–160.

[13] *See* Stephanie De Smedt and Valerie Verstraeten, "Blockchain and GDPR: is a clash really inevitable?", LEXOLOGY, August 2, 2018, https:/www.lexology.com/library/detail.aspx?g=2d91e00d-b434-4301-80ed-c5c69d92b8e#.

[14] *See* Primavera De Filippi & Aaron Wright, BLOCKCHAIN AND THE LAW: THE RULE OF CODE 2 (2018) ("Blockchains are, in many ways, [] 'tamper-proof boxes'").

transaction verification.

Assume that an American commercial entity uses a blockchain-driven transaction verification service that operates on the Ripple platform.[15] In a transaction between an EU citizen and the American entity, the EU citizen becomes displeased with his purchase and seeks to rid himself of all memory of the transaction—including the transaction log containing his credit card number and other personal information (e.g., name and address). The citizen requests that the data be deleted through invocation of his right under Article 17 of the GDPR.[16] Disgruntled to learn that the information cannot be deleted, the EU citizen seeks relief. The issue, though, is how can this be resolved?

Section II of this paper will discuss: (1) blockchain technology and how it can be used in transaction verification; and (2) the GDPR broadly and Article 17, specifically. Section III will re-introduce the hypothetical and offer current views on how to deal with this situation. Section IV will analyze the application of the GDPR to this conflict, explain why the two philosophies are incompatible, and propose alternative dispute resolution as a means of resolution. Section V will conclude with why a mutually assured destruction of both the GDPR and blockchain by each is avoidable and unnecessary to resolve the conflict.

[15] Ripple is a blockchain platform which focuses its use of blockchain technology to assist in expedited transaction verification for financial entities like banks. *See* Ripple, *Use Cases*, https://ripple.com/use-cases/banks/.
[16] GDPR, *supra* note 9, at art. 17.

II. Blocks, Chains, and the GDPR

A. Blockchains

Fundamentally, a blockchain is a type of distributed ledger technology that uses blocks and chains to store transaction records.[17] A distributed ledger is an umbrella term for any transaction type that is decentralized and distributed amongst parties.[18] The participants in a blockchain system coordinate to keep this ledger up to date.[19] A block can be a single transaction or a collection of transactions that also contains reference to previous "blocks", and an answer to a complex mathematical puzzle used to validate the data associated with the "block" itself.[20] The method through which transactions are validated is referred to as "proof-of-work",[21] where users on the platform, known as nodes,[22] are tasked with solving a complex and computationally intensive mathematical equation.[23]

Once a transaction involved in a block is verified by a majority of nodes, the block is added to the chain.[24] A chain is a collection of blocks connected by hashes which are encrypted strings of data which contain references to the transactions within the block, reference to the hash of the previous block,[25] and a timestamp.[26] Notably, all data on a blockchain ledger is redundantly stored

[17] Stephanie De Smedt and Valerie Verstraeten, *supra* note 11.

[18] *Id.*

[19] Scott J. Shackelford and Steve Myers, *Block-by-Block: Leveraging the Power of Blockchain Technology to Build Trust and Promote Cyber Peace*, 19 YALE J. L. & TECH. 334, 342 (2017)

[20] Aaron Wright & Primavera DeFilippi, *Decentralized Blockchain Technology and the Rise of Lex Cryptographia*, SSRN 48–49 (Mar. 12, 2015), http://papers.ssrn.com/sol3/papers/cfm?abstract_id=2580664 (last visited Dec. 4, 2018).

[21] Elizabeth Sara Ross, *Nobody Puts Blockchain in a Corner: The Distruptive Role of Blockchain in the Financial Services Industry and Current Regulatory Issues*, 25 CATH. U. J. L. & TECH. 353, 364 (2017).

[22] *See Id.,* n. 84.

[23] *Id*.

[24] Note that an attempt to manipulate a blockchain would need to go through the process of this majority approval mechanism. Known as a "51% attack", this is an arduous and nearly impossible undertaking.

[25] "[this] ensures that preceding blocks are not altered, and a new block is a logical addition to the previous blockchain". Max Danzmann, *Asset Transfers Through Blockchain Applications*, (2018) 4 JIBFL 238 (2018).

[26] Primavera De Filippi & Aaron Wright, *supra* note 12, at 22–23.

by all nodes—meaning that each node has an exact copy of the ledger which will be accessible at any time.[27] When changes are entered in one copy, all other copies update simultaneously.[28]

Additionally, there are two general types of blockchains: public and private. A public blockchain is best described as a ledger where access to the network is unrestricted—meaning any user may view the ledger and act within the system.[29] Yet, this access can be subject to permissions that may require the user to follow an identification procedure to view or act within the blockchain.[30] The other blockchain type, private, is often a closed network where access and participation will be subject to specific conditions like invitation to access the blockchain.[31]

With a basic outline of what a blockchain is and how it works, to best understand the hypothetical this paper discusses, an explanation of how blockchains can and are used in financial transactions is necessary. Private blockchains allow for only certain users to access the platform and undertake verification of transactions to be added to the ledger. Financial institutions, for instance, are investing in the use of private blockchains with limited and trusted counterparties and finding that transaction costs are decreasing. [32] Such investment is undertaken because traditional transaction verification is a complex and time-consuming process.

Take consumer credit card purchases as an example. When a person swipes their credit card at a merchant, they are one of five parties involved in the processing of the purchase.[33] In addition to the consumer and merchant, there is the issuer bank that funds the consumer's purchase

[27] Max Danzmann, *Asset Transfers Through Blockchain Applications*, (2018) 4 JIBFL 238 (2018).
[28] Marco Iansiti and Karim R. Lakhani, "The Truth About Blockchain", HARVARD BUS. REV., (Jan.-Feb. 2017), https://hbr.org/2017/01/the-truth-about-blockchain.
[29] Max Danzmann, *supra* note 23, at *3.
[30] *Id.*; To that end, though, a blockchain can be designed in a manner that is anonymized or pseudonymized, meaning the identity of the user can be masked or completely unknown.
[31] *Id.*.
[32] Marco Iansiti and Karim R. Lakhani, "The Truth About Blockchain", *supra* note 25.
[33] *See* David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*¸ 75 MARYLAND L. REV. 935, 940 (2016).

from the merchant, and an acquirer bank that receives the payment.[34] Both banks have a contractual relationship with a card network, e.g., Visa, whose services they pay for through annual membership dues and per-transaction fees.[35] When the consumer swipes her card, the merchant then transmits the information to the acquirer bank that in turn enquires about the consumer's credit through the card network to the issuer bank.[36] If the credit is satisfactory, the approval of the transaction from the issuer bank is communicated to the acquirer bank through the card network.[37] This set-up is typical, but not exclusive.[38]

Regardless of the system, though, there is still a card network through which the two parties communicate. What if, however, there was a method of using an intermediary to verify this transaction type without the membership dues and transaction fees? Scholarship and blockchain research and development suggest that this can be done.[39] Enter, Ripple—"One frictionless experience to send money globally".[40] With blockchain-driven software that facilitates transaction settlement by connecting different networks on an open and neutral protocol, what it calls the "Interledger Protocol",[41] Ripple serves as the quintessence of disruption to the traditional means of transaction verification.[42] Ripple directs its services at global payments and aims to reduce institutional payment processing time to instantaneous verification—thereby reducing transaction

[34] *Id*.
[35] *Id*.
[36] *Id*.
[37] *Id*.
[38] *Id*. at 941 ("[there are] networks in which the issuer bank is the same as the acquirer bank").
[39] *Compare* Max Danzmann, *supra* note 23, at *3–*4 (arguing that blockchains can replace intermediaries if it is possible to settle transactions within a specific category of legal transaction without physical exchange of performances directly between parties) *with* Ripple, *Solutions Guide*, https://ripple.com/files/ripple_solutions_guide.pdf at 11 (accessed ____) (discussing that Ripple's software connects siloed networks though a protocol which will efficiently facilitate financial settlement through real-time settlement).
[40] Ripple, *Solutions Guide*, https://ripple.com/files/ripple_solutions_guide.pdf ; *see* Ripple, *Ripple*, https://ripple.com/.
[41] *Id.*
[42] *Id.* ("enabl[es] real-time settlement . . . [and] includes data-rich messaging between all transacting parties—delivering a real-time payment experience to end users").

costs significantly.[43] There is also added security to using a blockchain because of the encryption and tamper-proof foundation that a blockchain has when compared to traditional record-keeping systems.[44] Yet, Ripple is simply one example and one application of blockchain to the financial industry, with a plethora of possible solutions either available or in development.[45] It cannot be doubted, though, that blockchain technology is increasing in its popularity because it offers convenience in many important aspects of life.

B. The GDPR and the Right to be Forgotten

Like blockchain's revolutionary impact on the world of technology, the GDPR, which became effective on May 25, 2018, also shocked the status quo. To comprehend the regulation in its present form, an understanding of how data privacy came to be designated as fundamental in the eyes of the European Union (EU) is necessary.[46] Generally, the right to privacy in EU countries extends to private and public data processors and to all industries.[47] The right to privacy in the EU originated as a right of individual consent and subsequently the individual right to participate in society.[48]

[43] *Id*. at 16; *see also* Marco Iansiti and Karim R. Lakhani, "The Truth About Blockchain" (Retailers that offer [blockchain-based gift cards] can dramatically lower costs per transaction").

[44] *See, supra,* notes 14–20; *contra, e.g., Remijas v. Neiman Marcus Group, LLC*, 794 F.3d 688 (7th Cir. 2015) (class-action complaint alleged that system maintaining transaction histories which included consumers credit card information was inadequately secured); *see also* FTC, "The Equifax Data Breach: What to Do", (September 8, 2017) https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do (discussing potential dissemination of sensitive personal information of 143 million Americans stemming from inadequate maintenance of record-storing system).

[45] *See* Max Danzmann, *supra* note 23 at *5–*6 (discussing use of blockchain-driven applications for collateralization purposes); *see also* Sara Elizabeth Ross, *supra* note 19, at 368–373.

[46] GDPR, *supra* note 9, at art. 1 ("This regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data"); *See also* Charter of Fundamental Rights of the European Union art. 8, 2010 O.J. C 83/389, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF.

[47] Michael Rustad and Sanna Kulevska, *Reconceptualizing The Right to be Forgotten to Enable Transatlantic Data* Flow, 28 HARV. J. LAW & TECH. 349, 356 (2015).

[48] *Id.*

Multiple vehicles exist in addition to (and even prior to the drafting, passage, and implementation of) the GDPR through which the EU protects citizens' right to privacy and even personal data.[49] In 2013, the Organisation for Economic Co-operation and Development ("OECD")[50] revised its privacy principles, first implemented in 1980, to recognize: " . . . that more extensive and innovative uses of personal data bring greater economic and social benefits, but also privacy risks". [51] Yet, the revisions did not recognize a specific right for the data to be forgotten.[52] However, the EU announced in its Charter of Fundamental Rights of the European Union[53], broader privacy for the individual in Article 7 of the charter.[54] Article 8 of the same lists personal data protection as fundamental.[55]

The final piece of legislation, and the one which governed privacy law in the EU prior to the GDPR, was Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (Data Protection Directive).[56] That this piece of legislation was a directive indicates how data privacy, though of concern to the EU, was not pressing enough in 1995 to make it uniformly EU law.[57] Said another way, the adoption of the

[49] *Id.* at 357–62 (discussing the privacy principles outlined by the Organisation for Economic Co-operation and Development (OECD), the Charter of Fundamental Rights of the EU, and the Data Protection Directive of 1995).

[50] The OECD is an international organization whose "[] mission [] is to promote policies that will improve the economic and social well-being of people around the world" *See* Organization for Economic Co-Operation and Development [hereinafter "OECD"], *About the OECD*, http://www.oecd.org/about/ (last visited Dec. 4, 2018).

[51] *Id.* at 357 (citing OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* ch. 1, 11 (1980), http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf.

[52] *Id*. (citing Rick Mitchell, *Revised OECD Privacy Guidelines Focus on Accountability, Notification of Breaches*, BLOOMBERG BNA (Sept. 16, 2013), http://www.bna.com/revised-oecdprivacy-n17179877087).

[53] Charter of Fundamental Rights of the European Union, 2010 O.J. C83/393, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:083:0389:0403:en:PDF.

[54] *Id.* at art. 7.

[55] *Id.* at art. 8. It also imposed the same level of data protection throughout the EU. *See* Michael Rustad and Sanna Kulevska, *supra* note 45, at 358.

[56] Council Directive 95/46 on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. L 281/31.

[57] Treaty on the Functioning of the European Union [hereinafter "TFEU"] art. 288, 2012 O.J. C 326/47, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012E/TXT&from=EN.

directive required member states conform to a minimum level of protection through enactment of legislation under their national that met or exceeded what the directive provided.[58] With the Data Protection Directive, the goal was two-fold: promote the free-flow of data; and to protect fundamental human rights.[59] Important aspects of the directive also included the view that processing of data by a party in a third country cannot inhibit the protection for EU citizens under the directive,[60] and that processing personal data must be done with consent from the individual—except where in the scope of ordinary and legitimate business activities, the data may be disclosed.[61] Importantly, too, the Data Protection Directive's Article 12(b) contained, though not explicitly, what can be considered the first version of what Article 17 of the GDPR provides outright—the right to be forgotten.[62]

Prior to the enactment of GDPR, the Court of Justice for the European Union (CJEU) decided a case in 2014 in which it found a right to be forgotten within the Data Protection Directive. In *Google Spain SL v. Agencia Española de Protección de Datos* (AEPD) ("*Google Spain"*),[63] the CJEU found that a EU citizen possessed a right to be forgotten under the Data Protection Directive.[64] In *Google Spain*, a Spanish national, Mario Costeja González filed suit against the AEPD, Google Spain, and *La Vanguardia Ediciones SL* (a publisher of daily news in Spain).[65] González alleged that when end users typed his name into a Google search, it showed links to *La Vanguardia* newspaper articles with announcements for a real estate auction related to

[58] *Id*.
[59] Beata Safari, "Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection", 47 SETON HALL L. REV. 809, 813 (2017) (citing Council Directive 95/46, *supra* note 54).
[60] *Id.*
[61] *Id.*
[62] *Id.* (citing Council Directive 95/46, *supra note* 54, at art. 12).
[63] *Google Spain SL v. Agencia Española de Protección de Datos*, Case C-131/12, 2014, http://curia.europa.eu/juris/document/document.jsf?text=&docid=152065&doclang=EN.
[64] *Id.* ¶¶ 1–4.
[65] *Id*. ¶ 14.

attachment proceedings stemming from González's failure to pay social security debts.[66] He further argued that despite the accuracy of the articles, they nonetheless injured his reputation and invaded his privacy.[67] González demanded that the newspaper erase the articles because the proceedings concluded ten years previously and were no longer relevant.[68] After the newspaper refused, citing instruction from the Ministry of Labour and Social Affairs to publish the articles,[69] González demanded that Google remove the link to the stories to eliminate association with them to his name.[70]

Procedurally speaking, the AEPD first reviewed the dispute and deemed Google responsible as a data controller for removing results about the plaintiff from its search platform.[71] Next Google brought the case before the *Audencia Nacional*, the court of last resort in Spain, which in turn referred the case to the CJEU.[72] Advocate General Niilo Jääskinen issued his advisory opinion on June 25, 2013, and found that Google held no responsibility to remove any links on its search engine stemming from a privacy claim.[73] His reasoning was that the suppression of legitimate and legal information already in public would undermine the freedom of expression and objectivity of information on the Internet.[74]

In its judgment, the CJEU rejected the opinion of Advocate General Jääskinen and instead recognized a wide-ranging right to be forgotten under Spain's implemented analog to the Data

[66] *Id.*
[67] Michael Rustad and Sanna Kulevska, *supra* note 45, at 363 (citing Dave Lee, *What Is the "Right To Be Forgotten?"*, BBC (May 13, 2014), http://www.bbc.com/news/technology-27394751).
[68] *Google Spain SL*, *supra* note 61, at ¶ 15.
[69] Opinion of Advocate General Jääskinen, Google Spain SL v. Agencia Española de Protección de Datos , Case C-131/12, 2014, ¶ 19, http://curia.europa.ed/juris/document/document.jsf?text=&docid=138782&doclang=EN.
[70] *Id.*
[71] *Google Spain SL*, *supra* note 61, at ¶ 17.
[72] *Id.* ¶¶ 18–20.
[73] Opinion of Advocate General Jääskinen, *supra* note 67 at ¶ 138.
[74] *Id.* ¶¶ 120–34.

Protection Directive.[75] The Court reasoned that because Google was an indexer of information, it processed personal data and was subject to the obligations of the Data Protection Directive that related to data controllers.[76] Citing to articles 12(b) and 14(a) of the Data Protection Directive, the Court held that Google owed a duty to erase information from its search index.[77] The Court determined that search engines enable users to obtain information about a EU citizen by simply typing in the individual's name,[78] and that given their role in organizing data, Google was far more likely to interfere with the individual's right to privacy than an original website publisher.[79] Thus, data subjects in Europe gained the right to demand Google delete links to websites that appear when searching for their names unless legitimate reasons not to remove them existed—even if the original website had not taken down the content and the data is truthful and otherwise lawful.[80]

With this brief history of the predecessors to the now fear-inducing regulation[81] outlined, a brief description of the GDPR itself, but specifically Article 17 thereof is critical to piecing together the conflict between blockchain technology and the regulation's fundamental protection for data protection. Below is a brief outline of how the GDPR came into being and a description of Article 17 and what it lists.

The GDPR was first proposed by the European Commission (EC) in January 2012 and its main purpose was to update data protections in light of rapid changes in technology that occurred

[75] *Google Spain SL*, *supra* note 61.
[76] *Id.* ¶ 41.
[77] *Id.* ¶ 82.
[78] *Id.* ¶ 80.
[79] Note, too that the Court used this reasoning to reject Google's argument that this imposed duty violated proportionality and any removal questions should be directed to the original website publisher. *Id.* at ¶¶ 63, 94.
[80] Michael Rustad and Sanna Kulevska, *supra* note 45, at 365, n. 101; *see also Google Spain SL*, Case C-131/12 at P 94.
[81] This regulation can be fear inducing because, for example, infringement of rights under Article 17 of the GDPR can lead to fines of €20 million or 4% of the previous financial year of the culprit company. *Cf.* Beata Safari, *supra* note 56, at 825; *see also* GDPR art. 83.

subsequent the passage of the Data Protection Directive.[82] The GDPR is a regulation which means it is EU law and self-executing and does not require the adoption of analogs on national level to have effect.[83] The explicit recognition of a right to be forgotten beyond the confines of a search engine was included in the version introduced by the EC in January 2012 and approved by the Civil Liberties, Justice and Home Affairs Committee of the European Parliament ("LIBE").[84] The version passed by the European Parliament in April 2016 repealed and superseded the Data Protection Directive.[85]

Article 1 of the GDPR states: "This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data".[86] Article 3 outlines the territorial scope of the regulation: "This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not."[87] It is important to note that these two articles highlight that: (1) the right is fundamental; and (2) it application is not restricted to the boundaries of the European Union.

Article 17's title reads: "Right to erasure ('right to be forgotten')".[88] Paragraph 1 indicates that a data subject can request the erasure of personal data without undue delay by the data controller when one of the following applies: (1) the data is no longer necessary in relation to why it was collected;[89] (2) the data subject withdraws consent on which the processing of the data was

[82] Commission Proposal for a Regulation of the European Parliament of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation), COM (2012) 11 final (Jan. 25, 2012), Explanatory Memorandum § 1.
[83] TFEU, *supra* note 55.
[84] Michael Rustad and Sanna Kulevska, *supra* note 45, at 369, n. 112.
[85] *See generally* GDPR, *supra* note 9.
[86] *Id.* at art. 1.
[87] *Id.* at art. 3(1).
[88] *Id.* at art. 17.
[89] *Id.* at art. 17(1)(a).

permitted per Article 6(1)(a) or Article 9(2)(a), and when no other legal ground for the processing exists;[90] (3) the data subject objects to the data processing pursuant to Article 21(1) and no legitimate and superseding grounds exists to permit processing, or the subject objects under Article 21(2);[91] (4) the personal data was processed unlawfully;[92] (5) erasure is necessary for compliance with a legal obligation imposed by the Union or a Member state to which the controller is subject;[93] or (6) the personal data was collected in relation to the offer of information society services.[94]

Paragraph 2 discusses that controllers who make the personal data public must take reasonable steps to inform other controllers processing the data aware that a request for erasure was made on the data.[95] Paragraph 3 outlines exceptions to application of erasure.[96] The exceptions are: (1) when the processing is necessary for the exercising of the right of freedom of expression and information;[97] (2) compliance with legal obligation that requires processing imposed by the EU or a member state, or for a task to be undertaken in public interest, or in the exercise of official authority vested in the controller;[98] (3) reasons of public interest in the realm of public health;[99] (4) in furtherance of public interest in the fields of scientific or historical research or statistical purposes so far as erasure would render impossible or seriously impair the achievement of data processing;[100] or (5) establishing, exercising, or defending legal claims.[101]

Academics categorize the right to be forgotten as taking three forms: the right to have

[90] *Id* at art. 17(1)(b).
[91] *Id* at art. 17(1)(c).
[92] *Id* at art. 17(1)(d).
[93] *Id* at art. 17(1)(e).
[94] *Id* at art. 17(1)(f).
[95] *Id* at art. 17(2).
[96] *Id* at art. 17(3).
[97] *Id* at art. 17(3)(a).
[98] *Id* at art. 17(3)(b)
[99] *Id* at art. 17(3)(c).
[100] *Id* at art. 17(3)(d).
[101] *Id* at art. 17(3)(e).

information deleted after a preset period; right to have a clean slate; and the right to be connected to current information and delinked from the outdated information.[102] The first right describes the ability to have information erased by the entities who collect it.[103] The second and third rights describe a way forward with a fresh start.[104] Yet, confusion surrounds how controllers are to determine when the various provisions of paragraphs 1 and 2 of Article 17 apply when to follow them—for example, determining when data which is subject to a request for erasure is no longer necessary or where no legal basis for retaining it exists.[105] The same can be said about the application of the exceptions outlined in paragraph 3, like when a data request runs afoul of the freedom of expression.[106] Some believe this Article may have a chilling effect on various aspects of life such as journalism.[107] Some others argue that United States-based controllers will be more hesitant to deal with European citizens given the disparity in privacy protection laws and standards. [108] So, what happens when the data cannot be deleted?

III. Is Blockchain a Nuclear Bomb?

A. The Conflict

To illustrate the conflict between the GDPR and Blockchain technologies, a common-occurrence hypothetical suffices—an online credit card purchase. As illustrated above, the traditional method of credit card purchase verification can be complicated and time consuming, due in large part to the number of parties involved. [109] This exact issue is addressed by companies,

[102] Michael Rustad and Sanna Kulevska, *supra* note 45, at 368.
[103] *Id.*
[104] *Id.*
[105] *Id.* at 369–70.
[106] *Id.* at 371.
[107] *Id.* at 374.
[108] *See generally*, Paul J. Watanabe, *An Ocean Apart: The Transatlantic Data Privacy Divide and the Right to Erasure*, 90 S. CAL. L REV. 1111 (2017).
[109] *See* David W. Opderbeck, *supra* notes 30–35.

like Ripple, whose platforms seek to streamline the transaction verification process using blockchain technology.[110]

The question must be asked, then: what happens when an EU citizen purchases an item online from an American entity and then later decides he is unhappy and seeks to invoke his Article 17 right? Take the story of Haider, a Belgian-born EU citizen who decides to purchase a brand-new head-piece from Frank's Berets ("Frank's").[111] Frank's is an American-based company that employs a public, permissionless blockchain to verify its online transactions.[112] Given its business model, Frank's deliberately focuses its business strategy to non-EU citizens.[113] In search of a "new look", Haider scours the internet to find the hippest, trendiest item emerging from the United States. Haider finds Frank's website and discovers the "Setonia", the brand-new Fall 2018 beret. With rave reviews, and hand-selected New Zealand merino wool, the Setonia is the "hottest product in the United States". Convinced, Haider completes the purchase online and inputs his credit card information, as well as his billing and shipping address. Three weeks later, Haider receives his beret.

At first, Haider is enamored with his new purchase. However, after he is teased by his friends over his purchase, Haider decides he is unhappy with the beret. Understanding of his situation, Frank's employs its liberal returns policy and refunds Haider. Eager to place all of this behind him, Haider requests that Frank's delete all stored information it possesses relating to Haider, and his purchase. He invokes his right under Article 17 of the GDPR[114]. Unfortunately,

[110] *See* Ripple, *supra* note 13.
[111] The author would like to thank Frank X. Wukovits and Haider Gontier, two learned friends and brilliant legal minds, for serving as the inspirations for the parties in this hypothetical.
[112] *See* Ripple, *supra* note 13; Max Danzmann, *supra* note 28.
[113] Therefore, it does not voluntarily submit to EU jurisdiction under agreements such as Privacy Shield. *See* United States Department of Commerce International Trade Administration, *Privacy Shield Framework*, https://www.privacyshield.gov/welcome (last visited Dec. 4, 2018).
[114] *See* GDPR, *supra* note 9, at art. 17.

under certain obligations imposed upon Frank's, it must retain the transaction log.[115] When Frank's informs Haider of the impossibility of deleting the information because it is placed on a blockchain, an enraged Haider discovers the glaring conflict between the GDPR and Blockchain technology: immutability.[116] How can this issue be resolved?

B. Perspectives

A recently published thematic report by The European Union Blockchain Observatory and Forum ("EUBOF"), entitled: "Blockchain and the GDPR", addresses this issue.[117] The EUBOF asserts that: "[t]here is no contradiction in principle between the goals of the GDPR and those of blockchain technology. Most GDPR requirements can be applied to *most* blockchain applications.[118] Yet, the report acknowledges a conflict in practicality.[119]An issue that the EUBOF brings forward in its report is one that could be important to the issue in the case of Haider and Frank's: accountability.[120] Addressing accountability, the Report asserts that who or what qualifies as the "data controller" , for purposes of the GDPR, is subject to debate and concedes that this remains open and inconclusively settled in the context of public, "permissionless" blockchains.[121] Members of the blockchain community differ on this point: with some seeking to exclude the protocol developers from liability[122]; others seeking to exclude validating or participating nodes[123]; and others still arguing the contrarian position—that validating or participating nodes are data

[115] Under industry standards, tax filing purposes, and possibly even federal regulation, company's may be required to retain transaction logs. *See, e.g.,* The Bank Secrecy Act, 31 U.S.C.S. § 5311 et seq. (2001).
[116] *Id.*
[117] This entity is an initiative of the European Commission and is tasked with publishing "thematic reports" on various blockchain topics. European Union Blockchain Observatory and Forum, *Blockchain and the GDPR*, (October 2018), https://www.eublockchainforum.eu/reports.
[118] *Id.* at 17 (emphasis added).
[119] *Id.*at 17–27.
[120] *Id.*
[121] *Id.*
[122] *Id.* at 18.
[123] *Id.*

controllers.[124]

The EUBOF report next discusses the concept of data anonymization.[125] Parties disagree about whether the cryptographic methods employed by most blockchains are exempted from GDPR coverage.[126] Under the GDPR, if the data processed by an entity is anonymized, it is not subject to the regulation.[127] Yet, the bar for what qualifies as anonymized is steep; it must be: (1) impossible to identify a natural person through any and all of the means "reasonably likely to be used"; and (2) irreversible.[128] The report concludes that the cryptographic methods employed currently do not meet the GDPR exemption, but "[promising areas of cryptographic research] are likely to play an integral role in how blockchain-based applications can be made compliant with the GDPR."[129] It further concludes that the uses of these cryptographic technologies will need to be done on a case-by-case basis.[130]

A final relevant topic in the report is the tension between blockchains and the GDPR over data minimization and the right to erasure.[131] The report re-affirms that a seeming clash between blockchains and the GDPR exists because: "data, once written to the chain, [cannot] be changed. This immutability is a key property of the technology."[132] The report next states that even if a data controller could be found on a public blockchain, it is impossible to delete or update the record of a transaction without destroying the chain.[133] It adds, further, that changing to a private,

[124] Supporters of this position reason that "through the act of actively downloading and running the software, nodes are indeed determining the purpose and means of processing", means and processing being criteria for qualifying as a data controller under the GDPR. *Id.*; *see also* GDPR, *supra* note 9, at art. 4 (7) (defining data controller).

[125] *Id.* at 19–24.

[126] *Id.* at 19.

[127] *Id.* (citing Article 29 Working Party, *Opinion 05/2014 on Anonymisation Techniques,* https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf).

[128] *Id.*

[129] *Id.* at 23.

[130] *Id.*

[131] *Id.* at 25.

[132] *Id.*

[133] *Id.*

permissioned blockchain will not necessarily resolve the issue.[134] The report offers the following solution: since the GDPR does not define erasure specifically, some encryption techniques paired with key destruction[135] can potentially be considered erasure even if not in the strictest sense of the word.[136] In its conclusion, the EUBOF offers four general principles to resolve the tension between Blockchain and the GDPR: (1) do you really need blockchain?; (2) avoid storing personal data on a blockchain and use other methods to anonymize data; (3) collect personal data "off-chain" or use a private blockchain if unavoidable; and (4) be clear and transparent with users.[137]

For one further perspective, consider an article written by Stéphanie De Smedt and Valérie Verstraeten from Loyens & Loeff entitled: "Blockchain and GDPR: is a clash really inevitable?"[138] Similar to the assertion of the EUBOF, the authors identify three privacy issues with blockchain and the GDPR: (1) who is the data controller; (2) how can data subjects exercise rights; and (3) can the two be reconciled?[139] Regarding data controllers, the authors argue that the it might be possible to identify a central administrator who is the data controller but on the public blockchains the answer would be either all nodes qualify as data controllers or none would.[140]

On the exercise of rights by data subjects, the authors write that amendment or erasure of data is technically impossible because the system is designed to prevent such action.[141] Thus, once data is added to a blockchain, it cannot be amended or erased and attempting this would require

[134] Not necessarily resolved is subject to the assertion that: "unless that network is designed in a way that each and every piece of data is readable by only the parties that absolutely need to . . ." *Id.*
[135] The translation mechanism that allows a party to view the otherwise encrypted data. *See* Marco Iansiti and Karim R. Lakhani, *supra* note 27.
[136] European Union Blockchain Observatory and Forum, *supra* note 113, at 25 (citing Commission National de l'informatique et des Libertés (CNIL), LA BLOCKCHAIN: QUELLES SOLUTIONS POUR UN USAGE RESPONSIBLE EN PRÉSENCE DE DONNÉES PERSONNELLES?, (September 2018), https://www.cnil.fr/sites/default/files/atoms/files/la_blockchain.pdf).
[137] *Id.*at 28–31.
[138] *See* Stephanie De Smedt and Valerie Verstraeten , *supra* note 11.
[139] *Id.*
[140] This is because the system on a public blockchain is operated by all its users in a peer-to-peer way. *Id.*
[141] *Id.*

adding a new block to the chain to record this change.[142] Yet, the initial data will always remain—leading the authors to question whether the immutability concept of blockchain technology can be reconciled with the right to erasure.[143]

IV. Away From Mutually Assured Destruction

A. Does The GDPR Apply?

A threshold question here is: does the GDPR apply to Frank's? Article 3 of the GDPR outlines the territorial scope of the Regulation.[144] In relevant part, Article 3 provides: (1) "[the] Regulation applies to the processing of personal data in the context of the activities of an establishment of controller or a processor in the Union, regardless of whether the processing takes place in the Union or not"[145]; and (2) "[] to the processing of personal data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union."[146]

In a recently published report,[147] the European Data Protection Board ("EDPB") adopted guidelines for interpreting the meaning of Article 3.[148] Regarding Article 3(1), the EDPB recommended a three-prong analysis to determine "establishment" for purposes of the GDPR's coverage: (1) is there an establishment in the Union[149]; (2) if so, is there processing of personal

[142] *Id.*
[143] *Id.*
[144] GDPR, *supra* note 9, at art. 3.
[145] *Id.* at art. 3(1).
[146] *Id.* at art. 3(2).
[147] European Data Protection Board, "Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)", (November 16, 2018), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_en.pdf.
[148] *Id.*at 3.
[149] *Id.* at 4–6.

data carried out “in the context of the activities” of the establishment;[150] and (3) if the processor or controller are within the EU, the GDPR will apply regardless of whether the processing occurs in the European Union.[151]

Under the first prong, and relevant here, the EDPB states: “the degree of stability of the arrangements and the effective exercise of activities in [a] Member State must be considered in the light of the specific nature of the economic activities and the provision of services . . . this is particularly true for undertakings offering services exclusively over the Internet.”[152] It notes, too that the threshold for “stable arrangement” can be low when the focus of activities of a data controller concerns the provision of online services.[153] However, the EDPB also noted that “[i]t is not possible to conclude that the non-EU entity has an establishment in the Union merely because the undertaking’s website is accessible in the Union.[154]

Under the second prong, the EDPB indicates that “if a case by case analysis on the facts shows that there is an inextricable link between the activities of an EU establishment and the processing of data carried out by a non-EU controller, EU law will apply to that processing by the non-EU entity, whether or not the EU establishment plays a role in that processing of data.”[155] On this point, the EDPB recommends that all concerned organizations assess: (1) whether personal data are processed; and (2) analyze any links between the purpose of processing and the activities of any presence of the organization in the Union.[156] The third prong, lastly, indicates that controllers and processors located in the EU are responsible for GDPR compliance and obligations

[150] *Id.* at 6–8.
[151] *Id.* at 8–12
[152] *Id.*at 5.
[153] *Id.*
[154] *Id.* (citing *Verein für Konsumenteninformation v. Amazon EU Sarl*, Case C-191/15, (2016), ¶ 76).
[155] *Id.* at 6–7.
[156] *Id.*at 7.

regardless of the location of the data processing.[157]

Under Article 3(2), the EDPB provides that the absence of an establishment in the EU does not necessarily relieve a data controller or processor in a third-country.[158] The EDPB outlines a two-factor analysis for this provision: (1) does the processing relate to personal data of data subjects who are in the Union; and (2) does it relate to the offering of goods or services or to the monitoring of data subjects' behavior in the Union.[159] Regarding this section, the EDPB states that the processing of data alone is not sufficient to trigger application of the GDPR, there must be an element of targeting individuals in the EU by: (1) offering goods or services; or (2) monitoring their behavior.[160]

In the case of Frank's berets, there is a strong likelihood that the GDPR may not even apply. Under: Article 3(1); the guidelines provided by the EDPB; CJEU case law; and because Haider discovered Frank's website, that Frank's website is merely accessible within the EU on the internet may not meet this critical threshold.[161] Haider sought out Frank's website to purchase the beret. Frank's, assumedly, created its website for customers domiciled in the United States, only. Further under Article 3(2), Frank's only processed the data of Haider when the transaction was initiated and completed—it did not deliberately target nor monitor Haider.[162] Therefore, Frank's likely would be relieved of GDPR coverage and fulfilling any obligations thereunder.

[157] *Id.* at 8–12.
[158] *Id.* at 12.
[159] *Id.* at 13.
[160] *Id.* at 14, 17. the EDPB also discusses that factors such as tracking a natural person on the internet including potential subsequent use of personal data processing techniques which consist of profiling a person to make decisions about his or her preferences.
[161] *See* European Data Protection Board, *supra* note 150.
[162] *See* European Data Protection Board, *supra* note 156.

B. The Perspectives Applied

For the sake of argument, assume that Frank's is subject to GDPR coverage. Applying the above-mentioned perspectives[163], Frank's remains free from responsibility to Haider. In theory, the vision of the EUBOF to reconcile blockchain with the GDPR in general may occur one day; but it must be re-stated that in the absence of a specific definition for erasure, Article 17 of the GDPR and blockchain technology's immutability principle cannot, and realistically should not, be reconciled. Any change to the blockchain does not remove the content, but rather will alter the chain but retain the original information, regardless.[164] This does not solve any issues. Applying the four solutions outlined by the EUBOF to the present hypothetical further illuminates the conflict. The four solutions offered by the EUBOF are: (1) do you really need blockchain?; (2) avoid storing personal data on a blockchain and use other methods to anonymize data; (3) collect personal data "off-chain" or use a private blockchain if unavoidable; and (4) be clear and transparent with users.[165]

Returning to Haider and his concern: Frank's would argue the need for a blockchain to process its transactions. The reason is that a blockchain platform that simplifies and expedites the verification of credit card transactions is critical to cash flow—in that it will significantly decrease the time to receive the funds[166]—and save the company from membership fees to credit card networks.[167] Next, Frank's may assert that storing credit card transactions on a blockchain is the safest method of retaining the transaction logs and credit card information in light of the recent

[163] *See supra* Section III B.
[164] This is also known as a fork in the chain, where the original chain "forks" and a new chain is created by the change. Yet, there will still be a reference to the previous chain; *See also* European Union Blockchain Observatory and Forum. *See* European Union Blockchain Observatory and Forum, *supra* note 129.
[165] *See* Marco Iansiti and Karim R. Lakhani, *supra* note 133.
[166] *See* Stephanie De Smedt and Valerie Verstraeten, *supra* note 11.
[167] *See* David W. Opderbeck, *supra* notes 30–35.

slew of data breaches of companies retaining credit card information.[168] Third, the use of a private blockchain does not alleviate the problem. As the EUBOF admits, the information cannot be removed from the chain without altering it. Also, Frank's would point to a possible legal obligation for why it needs to retain transaction logs.[169] Therefore, Frank's would have a sound basis to argue the need for it to use a blockchain-driven storage platform.

C. A Call for Alternative Dispute Resolution

This paper has undertaken to explain the fundamental issue that proponents of both blockchain technology and those who champion the GDPR face: they are incompatible and practically irreconcilable.[170] Yet, it is against most rules of reason to say that an individual faced with a situation where his personally identifiable information is incapable of erasure should be without a form of relief.[171] For that reason, an alternative avenue of dispute resolution should be explored if and when an EU citizen who seeks to invoke the Article 17 right to erasure against an entity using a blockchain-driven technology to process the data.

In the absence of some form of resolution, the result is a chilling effect on the GDPR. Likewise, too strong a resolution, like a binding opinion of the CJEU, the chill may fall on blockchain technology itself. In Stanley Kubrick's cinematic classic, Dr. Strangelove or: How I Learned To Stop Worrying And Love The Bomb,[172] the film tackles the intriguing theme of restraint driven by a fear of "mutually assured destruction". Mutually assured destruction is

[168] *See Remijas v. Neiman Marcus Group, LLC,* 794 F.3d 688 (7th Cir. 2015) (class-action complaint alleged that system maintaining transaction histories which included consumers credit card information was inadequately secured).
[169] *See* Ripple, *supra* note 13.
[170] *See, e.g.,* European Union Blockchain Observatory and Forum, *supra* note 130.
[171] U.S. Courts have found that at least as pre-discovery motions on the pleadings are concerned, a potential harm stemming from an alleged misuse of personal data can survive pleading standards. *See, e.g., Attias v. CareFirst, Inc.*, 865 F.3d 620 (D.C. Cir. 2017) (holding that consumers who face a possible future financial harm stemming from a data breach, in which credit card numbers were disseminated, satisfy the threshold inquiry for Article III standing).
[172] *See* DR. STRANGELOVE, *supra* note 1

effectively a situation where both sides in a conflict possess the same capability to cripple or destroy the other once provoked by the other. The result is, then, that both sides will restrain from provoking the other—driven by the knowledge that it could not survive attacking the other.

In the context of the GDPR and blockchain technology, the institution of an action by a EU citizen in the CJEU seeking to invoke his article 17 right to erasure would lead to a "nuclear bomb" dropping on blockchain technology in the form of a binding decision. Likewise, refusing to delete or alter records on a blockchain without providing relief cripples the purpose of the GDPR's article 17 right—a right deemed fundamental by the EU.[173]

To avoid the fallout that a binding decision of the CEJU or refusal to delete causes, arbitration as the method of dispute resolution could prove to be the most efficient method of resolution. Arbitration prevents the CJEU rendering an interpretation of Article 17 and stifle the development of blockchain technologies. It also prevents commercial entities from weakening the GDPR. Arbitration is contractual in nature—allowing parties to bargain for the means and methods for resolving their issues. In the realm of complex and niche dispute resolution—as a conflict between the GDPR and blockchain would be—the parties could bargain to select a third-party neutral who is versed in both the GDPR and blockchain and he or she could provide a fair resolution that is non-binding on courts and could potentially fulfill the spirit of the GDPR—to uphold the fundamental freedom of protection for personal data.[174] One such forum competent to review this dispute type could potentially be the International Centre for Dispute Resolution ("ICDR-AAA"), a subsidiary of the American Arbitration Association.[175]

[173] *See* Charter of Fundamental Rights, *supra* note 52.

[174] *See* Charter of Fundamental Rights, *supra* note 52, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT.

[175] International Centre for Dispute Resolution, *About the AAA and the ICDR*, https://www.icdr.org/about (last visited Dec. 4, 2018).

The ICDR-AAA provides a service specifically for disputes brought under the Privacy Shield framework[176], so it is within reason to assume that it could be competent to assess and adjudicate the dispute between parties like those of Haider and Frank's Berets. Instead of compromising the validity of a revolutionary technology or a preeminent piece of personal data protection legislation, concerned parties should seek to find the middle path.

V. Conclusion

In the age where personal data protection finds itself in the spotlight, competing interests will undoubtedly seek to shape the future of data protection legislative efforts. This paper sought to explain what blockchain technology is, why it is useful in important aspects of commercial activity—notably in credit card transactions—and explain its fundamental incompatibility with Article 17 of the GDPR by using a hypothetical situation which will not be uncommon. The result, that the GDPR does not apply, is a matter of threshold; but applying an analysis to whether information stored on a blockchain could be "erased" to satisfy the rights afforded EU citizens under the GDPR showed how these two philosophies could produce a "Mutually Assured Destruction" and that to avoid activating a "Doomsday Machine"[177] parties should pursue alternative dispute resolution before a neutral well-versed in both blockchain and the GDPR.

[176] International Centre for Dispute Resolution, *Privacy Shield*, https://www.icdr.org/privacyshield (last visited Dec. 4, 2018

[177] DR. STRANGELOVE, *supra* note 1.