COMMENTARY TO PROFESSOR BAKER'S PRESENTATION

Gary Pulsinelli[*]

I first want to thank Prof. Baker for her very interesting presentation on moving banking to the cloud.[1] As she noted, one of the major issues in such a move is how to preserve data security and prevent fraud and theft. In the current environment, the thing that immediately springs to mind in the context of cloud data security is, of course, blockchain. However, the use of blockchain is on a course to collide with another area of considerable contemporary concern: data privacy. At a key collision point, one of blockchain's greatest strengths becomes a weakness: the area of data deletion.[2]

I do not intend here to get into the details of blockchain and its uses (indeed, I lack the expertise to do so).[3] For present purposes, it suffices to make the general point that one of the main purposes of blockchain is to save data in a way that makes it virtually impossible to change that data.[4]

[*] Associate Professor of Law, University of Tennessee-Knoxville. The author would like to thank Prof. Baker, the organizers of *Business Transactions: Connecting the Threads III*, and the editors of *Transactions* for their assistance in this commentary.

[1] Colleen Baker, David Fratto & Lee Reiners, *Banking on the Cloud*, 21 TENN. J. BUS. L. 381 (2020).

[2] This discussion builds on papers written by students in my Law, Science, & Technology seminar, particularly Bruce Shank and Will McManus. *See* T. Bruce Shank II, The Data Privacy Revolution: How the Era of the General Data Protection Regulation Impacts Tennessee Businesses (2018) (unpublished manuscript); Will McManus, *Recording the Future: Problems and Solutions Concerning Blockchain Medical Records* (2018) (unpublished manuscript).

[3] For a brief overview of blockchain and its uses, *see, e.g.*, *What is blockchain technology?*, IBM BLOCKCHAIN, https://www.ibm.com/blockchain/what-is-blockchain (last visited Jan. 12, 2020), and links therein; s*ee also Blockchain*, WIKIPEDIA, https://en.wikipedia.org/wiki/Blockchain (last modified Jan. 23, 2020), and links therein; Eric Jeffery, *Blockchain beyond cryptocurrency*, BLOCKCHAIN PULSE: IBM BLOCKCHAIN BLOG (Dec. 9, 2019), https://www.ibm.com/blogs/blockchain/2019/12/blockchain-beyond-cryptocurrency/.

[4] *See, e.g.*, Bruce Bennett et al., *The GDPR and Blockchain*, COVINGTON: INSIDE PRIVACY (July 24, 2018), https://www.insideprivacy.com/international/european-union/the-gdpr-and-blockchain/.

Such data immutability can be useful in many contexts, and the cloud banking security context Prof. Baker discussed is one of them.

However, that permanence can also create problems, and one place in which that happens is in the privacy arena.[5] Currently, the U.S. lags behind Europe in this regard, but (1) as Prof. Baker noted, banking is an international business, and most (if not all) U.S. banks will need to comply with European Union law because they will deal with European clients with European institutions;[6] and (2) many commentators and others are pushing for the U.S. to follow the EU's lead (and many states are already taking steps in that direction). Thus, it would behoove the industry to think about the upcoming collision before it happens and address it proactively.

The precipitating force for privacy's collision with blockchain security is likely to be the EU's General Data Protection Regulation ("GDPR"), which went into effect on May 25, 2018.[7] The GDPR is a comprehensive regulation[8] governing the use and protection of personal data in the EU. The GDPR declares that "the protection of natural persons in relation to the processing of personal data is a fundamental right"[9]—that is, citizens own their private data (a term that the GDPR defines very broadly), rather than the entity that holds the data.[10]

While the GDPR is a creature of EU law, applying to EU citizens and institutions, it will also apply to U.S. entities when they offer goods or services to EU citizens.[11] This means it will cover most U.S. banks of any

[5] *See id.*; *see also* David Pollock, *How Can Blockchain Thrive in the Face of European GDPR Blockade?*, FORBES (Oct. 3, 2018, 4:07 AM), https://www.forbes.com/sites/darrynpollock/2018/10/03/how-can-blockchain-thrive-in-the-face-of-european-gdpr-blockade/.

[6] Baker, *supra* note 1.

[7] 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), OFF. J. EUR. UNION L. 119/1 (Apr. 5, 2016) [hereinafter "GDPR"].

[8] Under EU law, a Regulation is directly binding legislation in all EU countries, requiring no legislative action by those countries and trumping any domestic legislation.

[9] GDPR, *supra* note 7, Preamble Para. 1.

[10] The GDPR is the reason that web sites are suddenly notifying customers about their cookies and other data-gathering techniques and requesting their consent to such activities.

[11] GDPR, *supra* note 7, art. 3 ("Territorial Scope . . . 2. This Regulation applies to the processing of personal data of 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)

size, which will almost certainly have EU clients, or at least indirectly gain access to data from EU citizens. Thus, any cloud-based banking scheme, whether it uses blockchain or not, will have to take into account the requirements of the GDPR.[12] And U.S. institutions ignore the GDPR at their peril: The GDPR allows the imposition of some fairly hefty fines for noncompliance. For particularly egregious offenses against "core" rights, the fines can be up to €20M (~$22M) or 4% of the violator's total worldwide annual turnover from the previous financial year, whichever is higher.[13]

Complying with all of the myriad requirements of the GDPR will present a significant challenge to banks with EU-based customers, and that challenge will only increase as banks move to a cloud-based system. However, for present purposes, I would like to focus on three key provisions: the minimalization requirement, the right to rectification, and the right to be forgotten.

GDPR Art. 5.1 spells out limitations on data holders: "Personal data shall be . . . (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed . . . ."[14] This provision essentially requires that entities holding private data of EU citizens must delete such data when they no longer need it (sometimes called the 'Minimalization Principle').[15]

GDPR Arts. 12-23 provide rights to data subjects. Art. 16 provides the "Right to rectification": "The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her."[16] This provision thus provides the right to have erroneous data corrected. Banks are certainly subject to having erroneous information, and thus they must have the capability to fix that problem. Art. 17 provides one of the most important provisions

the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union . . . .")

[12] This discussion omits considerable nuance—the GDPR is a very complex set of rules containing a host of subtle definitions about who is covered (on both the citizen and entity sides), what data is affected, and what rules apply. However, generally speaking, U.S. banks with EU customers will have to comply with the GDPR.

[13] *See* GDPR, *supra* note 7, art. 83.5.

[14] GDPR, *supra* note 7, art. 5.1.

[15] *See* GDPR, *supra* note 7, art. 5.1.; *see also* Manuel Grenacher, *GDPR, The Checklist for Compliance*, FORBES.COM (June 4, 2018 7:00 AM), https://www.forbes.com/sites/forbestechcouncil/2018/06/04/gdpr-the-checklist-for-compliance/.

[16] GDPR, *supra* note 7, art. 16.

of the GDPR, the "Right to erasure ('right to be forgotten')": "The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay . . . ."[17] This provision gives the data subject the power to require an entity that holds his or her data to erase that data, which is a very powerful tool. However, the right is not unlimited in that it requires erasure only in certain specified situations[18] and is subject to certain exceptions.[19] Nevertheless, in at least some instances, a bank customer will likely be able to meet these requirements and force the bank to delete the customer's data.

All of these provisions will thus require changes to data in the bank's possession. In the current complex, interconnected data environment, that is likely to be a hassle for the bank, but this hurdle is not insurmountable. In a cloud environment, the exercise is likely to become more challenging. In a blockchain environment, it may prove impossible. The entire purpose of blockchain is to make sure that the integrity of data is not compromised, using technology that throws up a big red flag if any past data is changed even slightly.[20] Any correction or deletion of data will certainly have that effect. The users of blockchain will then be required to investigate each flagged event to determine whether it was due to a legitimate correction or deletion, or rather to the actions of a malefactor—effectively defeating the whole purpose of using blockchain in the first place (as one of my students put it in his paper, "[W]hile the GDPR and blockchain are compatible in their ideals, they conflict in almost every way in practice."[21]).

Furthermore, the problem is expanding as it moves to the United States. The California Consumer Privacy Act of 2018 ('CCPA'),[22] which

[17] GDPR, *supra* note 7, art. 17.1.

[18] *See* GDPR, *supra* note 7, art. 17.1 (specifying situations in which such erasure is required, such as "the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed," "the subject withdraws consent on which the processing is based," or "the personal data have been unlawfully processed").

[19] *See* GDPR, *supra* note 7, art. 17.3 (providing exceptions such as processing "for exercising the right of freedom of expression and information," "for compliance with a legal obligation," or "for reasons of public interest in the area of public health").

[20] *See supra* sources in note 3.

[21] Shank, *supra* note 2; *see also* Pollock, *supra* note 5 ("It is a direct clash of function, but, on ideological grounds, the aim of both the GDPR and blockchain is the protection of data").

[22] Assemb. B. 375, 2017 Assemb., Reg. Sess. (Cal. 2018) (adding Title 1.81.5, the California Consumer Privacy Act of 2018, to the California Civil Code).

went into effect on January 1, 2020,[23] similarly gives California residents the right to have their data deleted.[24] Thus, even if a bank somehow avoids EU customers and the GDPR, it will still have to worry about California customers and the CCPA.[25]

I am far enough outside my areas of expertise that I do not have a solution to the problem, but it is nevertheless an important issue—one that the banking industry should keep in mind as it moves into its cloud-computing future.[26]

[23] *See* NPR, *On Jan. 1, California's Consumer Privacy Act Goes into Effect*, NPR.ORG (Jan. 1, 2020 5:09 AM), https://www.npr.org/2020/01/01/792821108/on-jan-1-californias-consumer-privacy-act-goes-into-effect (transcript of Morning Edition interview with Stuart Brotman).

[24] *See* Kristen J. Mathews & Courtney M. Bowman, The California Consumer Privacy Act of 2018, PROSKAUER: PRIVACY L. BLOG (July 13, 2018), https://privacylaw.proskauer.com/2018/07/articles/data-privacy-laws/the-california-consumer- privacy-act-of-2018/ (discussing the contents of the Act).

[25] *See id.* (noting that "Both the [CCPA] and the GDPR apply to companies located outside their borders, emphasize some of the same broad themes (such as the importance of access and transparency), and—perhaps most importantly—will require companies to expend a great deal of effort and resources to achieve compliance." before discussing the differences between the laws).

[26] For some suggestions along these lines, see Bennett et al., *supra* note 4 (suggesting, among other things, pseudo-anonymization of data using encrypted keys, and also discussing reconciliation discussions taking place in the United Kingdom and at the European Commission); Pollock, *supra* note 5 (suggesting that the GDPR and blockchain share a "ideological common ground," and quoting blockchain expert Thomas Power, a board member at Blockchain Industry Compliance and Regulation Association (BICRA), as saying that "First they [GDPR and blockchain] will battle and challenge, then they will harmonize because they are not enemies, rather Frenemies.").