MINDING THE GAP: FINANCIAL TECHNOLOGY, SECURED TRANSACTIONS AND THE FUTURE OF COMMERCIAL FINANCE LAW

AALS 2020 "Innovations Connected to Fintech Lending"

Jonathan C. Lipson*

My interest in financial technology ("fintech") reflects an ongoing effort to understand the relationship between legal institutions, on one hand, and technological and transactional innovation, on the other.[1] Nearly twenty years ago I somewhat naively wrote that: "The laws of information technology and commercial finance speak, but not to one another."[2] I focused then, as now, on how this communication gap plays out in secured transactions involving fintech.

In 1997, Nick Szabo coined the term "smart contract," denominating the ur-fintech. Although legal academics were quick to point out that the things Szabo had in mind may have been neither "smart" nor "contracts," these skeptics tended to ignore the fact that at least one of his examples—the so-called "kill switch"—was codified in Article 9 of the Uniform Commercial Code (UCC 9-609(a)(2)), which governs secured transactions in personal property and fixtures. The kill switch, known in less Tarentino-esque fashion as a "starter interrupter," is a mechanism that enables a car lender to stop a borrower's car from starting (or, in theory, to turn it off) if the borrower breaches the loan agreement.

The kill switch is controversial because, among other reasons, when engaged, we may worry that: (i) the borrower did not actually breach (the lender could be wrong; the switch could have been hacked); (ii) if the borrower breached, this is an excessive penalty (the UCC permits self help only if there is no "breach of the peace"); or (iii) others may be harmed (Szabo said killing the car when in motion would be "rude," which seems scarily understated). But, as anyone who has watched car-repo-reality shows knows, the kill switch might be an improvement on sending a crew of toughs to bully the borrower into handing over the keys.

In a fintech world, it is easy to imagine more expansive and creative analogues to the kill switch. The technologies Szabo contemplated could, in principle, extend to many types of collateral (e.g., data and cryptocurrencies) and to the design and governance of secured transactions involving them (e.g., digital documentation; remote breach detection and enforcement, etc). If so, these technologies could affect every step in the legal analysis and design of a fintech secured transaction.

Take the question of scope. Under what conditions are various fintech transactions considered secured transactions? Is the electronic escrow of cryptocurrency in connection with an initial coin offering (ICO) a secured transaction within the scope of UCC Article 9? Maybe, but only if cryptocurrency is "property" that secures payment or performance of an obligation. If so, is it "located" somewhere that the UCC applies? Who knows? Similar questions dog other elements of the analysis (e.g., the attachment, perfection, and priority of fintech secured transactions).

---

* Harold E. Kohn Professor of Law, Temple University-Beasley School of Law.

[1] As to technology and secured transactions, see Jonathan C. Lipson, *Financing Information Technologies: Fairness and Function*, 2001 WIS. L. REV. 1067 (2001) ["*Financing*"]; Jonathan C. Lipson, *Remote Control: Revised Article 9 and the Negotiability of Information*, 63 OHIO ST. L.J. 1327 (2002); Jonathan C. Lipson & Steve O. Weise, *The Business Lawyer at 75 and Secured Transactions Under Article 9 of the Uniform Commercial Code,* 75 BUS. L. __ (forthcoming, 2020) As to institutional design and choice, see Jonathan C. Lipson *Against Regulatory Displacement: An Institutional Analysis of Financial Crises,* 17.3 PENN. J. BUS L. 673 (2015). As to transaction design and lawyering, see Jonathan C. Lipson, *Price, Path & Pride: Third-Party Closing Opinion Practice Among U.S. Lawyers (A Preliminary Investigation)*, 3 BERKELEY BUS. L.J. 59 (2005); *Re: Defining Securitization*, 85 S. CAL. L. REV. 1229 (2012).

[2] *Financing, supra* note 1, at 1068.

These are specific and perhaps prosaic examples of more general questions that many others, notably Lawrence Lessig, have explored: How are we to understand the gap between law and technology? If "code is law," what does that imply for legal institutions and practice? Earlier approaches to these questions were largely institutional, focusing on control and governance ("Code 1.0"). While those remain critical (#deFacebook, anyone?), disciplinary questions are also important, perhaps coextensive with the institutional ones, even though they have enjoyed less attention among those who think about the law and lawyering of fintech transactions.

Consider a basic question: Should lawyers know something about the computer code underlying fintech transactions? Recent studies of ICOs suggest that lawyers may know little about it. Secured transactions involving fintech are unlikely to be different. In either case, if computer code anticipates and determines the outcome of disputes, it would displace not merely law, but also lawyers.

Observers have, at different moments, lauded (e.g., John Perry Barlow) or lamented (e.g., the Susskinds) the possibility that robots will replace lawyers, but I think both enthusiasms should be curbed. Law and lawyering can be understood, in part, as complex conflict management systems: we anticipate and prevent conflict through contract (e.g., a security agreement); provoke it to vindicate rights; and resolve it through litigation or negotiation (e.g., the loan workout). Fintech depends upon a world in which we are more interconnected in more complex and contingent ways, so the future is likely to produce more, not fewer, moments of actual or potential conflict that could involve legal actors and institutions.

So understood, fintech would spell not the end of law or lawyering, but instead a change in the supply of and demand for law, and in the nature of lawyers' work. Law as it pertains to fintech transactions (including secured transactions) is, as Lee Fennell might say, "lumpy": it sometimes goes too far, and other times not far enough. UCC provisions on collateralizing electronic chattel paper (ECP), for example, were enacted before there was much ECP, so the supply of that law outstripped the demand (but maybe it "primed the pump"?). The question whether (or how) securities laws affect cryptocurrencies, by contrast, may bespeak unmet demand, since the SEC, itself, seems unsure of the answer.[3] Many would say we need legal clarity here, but legal institutions have yet to provide it.

Legal disequilibrium can be scary. Legal institutions and actors are, by design and social preference, not nimble, and so adjust to change slowly, if at all. The hard questions will involve our commitments to understanding and addressing this disequilibrium: What does equilibrium look like, and how do we get there? What should we study and teach, and how should we do so? Should we learn (or teach) code? If so (or if not), then what? That these questions are difficult does not make them less interesting or important.

I may not mind the gap between law and technology—but I do worry about it.

---

[3] On September 30, 2019, the SEC announced that it had settled an enforcement action involving an initial coin offering by Block.one. See Press Release, SEC Orders Blockchain Company to Pay $24 Million Penalty for Unregistered ICO, available at https://www.sec.gov/news/press-release/2019-202. The next day, the SEC issued a letter to Cipher Technologies stating that it could not register as closed-end fund because the SEC "disagree[s] with your conclusion that bitcoin is a security." See Letter dated Oct. 1, 2019 in re Cipher Technologies Bitcoin Fund, available at

https://www.sec.gov/Archives/edgar/data/1776589/999999999719007180/filename1.pdf