When Financial Intermediation Turns into Data Intermediation: New Risks and the Need for New Policies

Karen Petrou
Managing Partner
Federal Financial Analytics, Inc.
info@fedfin.com
www.fedfin.com

Remarks Prepared for Delivery at the

Online Lending Policy Summit

Washington, D.C.

October 9, 2018

It is an honor to moderate this distinguished panel on the privacy and data-security challenges arising as online finance heads to the stratosphere. To kick things off, I'll try to set the overall strategic context that each panelist's remarks will address. In short, privacy and data security have taken on a far different dimension as traditional financial intermediation – gathering deposits and making loans – is morphing into data intermediation – a business in which profit is earned not by transforming other people's money into macroeconomic growth engines but instead from watching what other people do with money and using these data to redefine finance into a business based far more on knowledge than net interest margin or related fees. Intermediating other financial transactions – e.g., buying stocks and bonds – has also become a data game via new technologies such as robo-advice and algo trading. Payment, settlement, and clearing services are no longer black boxes into which transactions seamlessly flow, now they are transactions from which data for the provider is gleaned at every turn to redesign the product offerings for which the payment transaction is just one part.

The transformation of finance into a data-driven business has tremendous potential, but one fraught with risks not only due to the usual mistakes made in the discovery process, but also the result of regulatory asymmetry that quickly drives transactions to less- or even-unregulated firms regardless of underlying comparative advantage. Now, competitors – some of them the biggest and most powerful tech companies in the world – are far outside the reach of traditional safety-and-soundness regulation. A recent paper from my firm goes into these issues in more detail, but I'll lay out two of them to start our discussion today.

1) Conflicts of Interest

The U.S. financial system is unique among all other major nations in that banks are barred from commerce and even from many financial services that, if allowed at all, must be in ring-fenced holding-company subsidiaries isolated from the bank with inter-affiliate transaction and other barriers. Numerous conflict of interest rules also apply so banks may not use their financial power or even just control of a customer's information to entice or force retail and business customers to obtain products that they do not need or do so at prices that take advantage of the need for banking products and services.

Turn this on its flip side and look at commercial and non-traditional – i.e., fintech and platform – companies. Many engage in extensive commercial activities – retailing, advertising, even manufacturing – and are allowed seamlessly to integrate finance into each of these commercial ventures. There is no barrier to a non-bank using every bit of data in its possession modelled through all of its AI and ML to offer financial products as a condition of access to desired services or from changing its own product offerings or to advertise based on proprietary data on a customer's ability to pay, price tolerance, and other possessions, family-member choices, or similar factors wholly unknown to financial intermediaries until the world went wired.

Is this a privacy problem? Yes in that it involves the use of personally-identifiable information for purposes unknown to the customer that are not necessarily in the customer's best interest.

But, it's more than a privacy problem. This is a structural rethink of finance we must understand from the get-go as we proceed to talk about what type of state, federal, or global standards make sense in this new world.

2) Infrastructure Risk

Turning to our other topic: data-integrity and security, we'll hear today that the shift from financial to data intermediation poses an array of structural risks. Last Tuesday, all of the federal banking agencies' top officials were united in their top systemic fear: cyber-security. They should be.

But, they should also worry at least as much about the enemy from within – operational risk at key nodes in the financial payment infrastructure as about the risk of outside evil-doers. The U.K. has already seen a series of wide scale systems outages at banks that wreaked havoc with affected customers. U.S. banks are so far experiencing only small-scale versions of these problems, with this largely due to the far more stringent U.S. framework for operational resiliency at the largest banks. No such standards apply to non-banks.

Systems are quickly becoming far more complex and inter-connected between regulated banks an unregulated entities with dubious internal controls or risk-management capabilities. Computing is heading to the cloud through just one or two service providers also exempt from redundancy, resiliency, and resolution standards.

Concentrated operational-infrastructure power create a systemic risk to global financial infrastructure which the Financial Stability Board and other global entities are just beginning to reckon. U.S. policy-makers are just now starting to think about what these changes mean, moving ponderously through complex analyses designed to balance the benefits of innovation with structural risks and coming up so far only with ambiguous papers committed to thinking more about all this.

I think we all know each day we pick up our phone or look at a laptop that time is not on the side of procrastination. A long, long time ago, I wrote a master's thesis showing that California only dealt effectively with earthquake risk after each major earthquake and only then to fix what fell down in the proceeding quake. The state's inability to grapple with seismic risk is evident every day on which San Franciscans look up at that 58-story skyscraper and see it titling fifteen inches to one side.

Today's panelist all are working hard to craft privacy, data, and security standards to more policy ahead of risk. So, let me turn now to each of them for expert advice and opinion.