The Threat of Privacy

By Charles M. Kahn[1]

Like artists, we academics want to believe that if one of our works doesn't get enough attention it's because we're ahead of our time. I'd like to pretend that everything I've written is pathbreaking, and will eventually be recognized for its true importance. But I have to admit that there are really only a couple of cases where I can say with hindsight that something I wrote has been ahead of its time.

One of them[2] is a paper written with Jamie McAndrews and Will Roberds, published in 2005, and titled "Money is Privacy." We wrote it partly as a response to Narayana Kocherlakota's famous paper "Money is Memory," which could be taken as arguing that cash is essentially a record-keeping device, tracking who was a net creditor and who a net debtor to society with respect to resources provided or consumed. The implication was that if it became easy to keep credit records directly, cash could wither away.

In our paper we argued instead that a key role of cash was its ability to protect the purchaser's identity. So we predicted that, even while the reductions in costs of record keeping and increases in the speed of data transmission were expanding the usage of credit- and deposit-account- based payments arrangements, cash would survive. Because the desire for privacy would always generate demand for cash, it would be a mistake—and ultimately futile—to attempt to abolish it. At the time, people were attuned to many of the problems of privacy, but there had not yet been a clear recognized link between the value of privacy and the role of payments systems. (Remember, bitcoin was only released in 2009).

---

[1] Keynote address at "Financial Market Infrastructure Conference II: New Thinking in a New Era" at De Nederlandsche Bank, Amsterdam, 7-8 June 2017.

[2] The other was my dissertation, back in 1980. It was on liquidity and the pricing of illiquid assets. At that time, no one thought this was an important issue in finance: financial markets were liquid; everybody "knew" that. So the work went nowhere. Oh well.

In the intervening years, the concerns about privacy have grown relentlessly, as data security breaches have become commonplace. Policy makers now fully recognize the importance of privacy concerns in financial infrastructure, including payments arrangements—so much so, in fact, that in this talk I'm going to focus, less on the threats TO privacy in the modern world, and more on the threats OF privacy—that is, the problems that the demand for privacy imposes ON central banks and payments regulators and providers.

Therefore I will begin by discussing the sources of demand for privacy in payments. Then I'll talk about central banks' ability (and inability) to provide privacy, with particular reference to recent e-money proposals, and finally make some tentative predictions about what one might pretentiously call "the emerging privacy ecosystem" in payments. While much of what I say will focus on retail payments, an important portion will be applicable to wholesale arrangements and financial market infrastructure more generally.

DEMAND FOR PAYMENT PRIVACY

The demand for privacy in payment has several distinct sources. The one that comes to mind first, I suppose, is the desire to engage in illegal transactions: Cash payments for purchasing illegal drugs, or in order to avoid tax on unreported service income; bitcoin payments to ransom hijacked computers or people; offshore bank accounts for bribing corrupt officials. While cash is not the only method for making illegal transactions, its existence certainly makes the transactions easier, either through direct payment, or through the process of money laundering, where a cash stage in the series of disguising transactions (so-called "layering") helps to break the ability to trace the ultimate sources of payments.

Now, your attitude to this kind of privacy will ultimately depend on whether you think the transaction being hidden is one which ought or ought not be illegal in the first place. In a country where sale of female contraceptive devices is illegal, you might be more sympathetic to the continued existence of a privacy-

preserving means of payment. The bottom line with regard to this kind of privacy is that "I" am always in favor of privacy for myself, since I would only use it to break bad laws, and opposed to this kind of privacy for other people, who might use it to break good laws. Nonetheless if you live in a country where the classification of activities as legal or illegal is generally in accord with your own moral standards, then you'll favor abolition of this kind of privacy. This is a position staked out by, for example, Ken Rogoff in his celebrated book *The Curse of Cash.* And it is in line with actions taken by various central banks around the world to abolish large-denomination notes, and otherwise discourage large holdings of cash.

But sometimes the privacy desired is not for protection from government scrutiny, but for protection from the other party to the transaction. There are cases, not that rare really, where I wish to make a transaction with a stranger, where the transaction is perfectly legal, but the stranger is not trusted. I have a used car to sell; I provide the car (and title) in return for cash. This is not uncommon in the US and I believe it is in fact the norm in several other countries. Norm or not, the possibility provides the basic idea: there are desirable transactions in which the transactors wish for the deal, once consummated, to have no ramifications down the road.

This is, I believe, an aspect of transactions which is underappreciated in current economic theory. We recognize the importance of the ability to build reputations. We <u>want</u> these reputations to have ramifications in the future: good behavior, fair dealing today, leads to trust in our actions in the future—and more importantly the fear of the consequences of a bad reputation keeps makes it credible that we will engage in good behavior today. For this reason arrangements that facilitate individuals' ability to build reputations are an important driver of economic development, and that is the reason that programs such as India's Aadhaar ID card have such potential. Similarly, the theory of contracting provides innumerable examples where long-term arrangements, and contracts containing large numbers of contingencies can create value for the parties to the contracts, and so technologies which facilitate the recording and implementing of these arrangements provide economic benefits: think of trying

to sign a sophisticated insurance arrangement, or finance any complex construction project, in a world without adequate record keeping and enforcement.

But there is another important, less recognized side to the story—sometimes we want our arrangements not to continue for the long term, but to have an end point, beyond which we do not have to worry about further contingencies.

In the world of payments, this notion arises in the concept of "finality"—ideally we want to be able to state with certainty that at some point the payment has been made, the debt has been expunged, and the funds are secure. But developments in law and increasing powers to track activities begin to delineate more and more cases where the payment is not as final as we thought: clawbacks, extraterritorial rulings, new forms of product liability. So we want to write into contracts insurance against these possibilities, extra clauses stating what will happen in the event of disputes, who has authority to raise objections or undo the arrangement in which circumstances, and who has jurisdiction to make the judgement. And then comes the additional uncertainty about which of these clauses will be enforced by the courts and which overturned. As the problem becomes more and more complex, parties to the transaction are no longer able to support the lawyers' fees necessary to uphold the arrangement. Now, blockchain and smart contracts may eventually solve the problem for parties with the savvy and resources to use them. But in the meanwhile, for individuals without legal and IT departments at their beck and call, it becomes more and more tempting to forestall the problem entirely by making it impossible for the transactors to find each other after the deal goes through—that is, by instituting anonymity in the transaction. Cash is a simple way to make that possible.

The ability to make a transaction without revealing your identity is therefore useful even when the transaction is legal. Jamie's Will's and my paper showed that a system that allows this possibility can be welfare improving; the key ingredient for this to be the case is a moral hazard problem linked to the revelation of the counterparty's identity. In the paper we used a fairly silly example—we imagined that the purchase was of an asset which was susceptible

to theft, and that if the purchaser revealed his identity to the seller, the seller being able to find out where he lived, might use the information to steal it back. While it is hard to think of examples of individual goods where this is a serious concern, it is not so hard to think of examples where the information about purchase of a good makes the individual vulnerable: a purchase indicating that the individual has high wealth, or a purchase that may be embarrassing, even if perfectly legal—lots of medications, for example, fall into that category. More prosaically, making a purchase on the internet involves the revelation of identity in ways that make you subject to spam or harassment. Think of this as the everyday commercial equivalent of the desire for a "right to be forgotten." In short, sometimes we want the ability to ensure that others cannot use the information in the history of our transactions against us.

Of course we might hope that effective laws would provide a protection against these difficulties. Privacy is not necessary if there is no way for your counterpart to take advantage of the information he gets. But the whole point of the moral hazard problem is the inability (of individuals or governments) to perfectly control the "hidden actions" of others. Privacy is the means to deprive them of the information they need to carry out these hidden actions.

So there is a legitimate market for privacy of transactions. Bitcoin is in this market. The providers of stored value cards are in this market. To a certain extent, Paypal is in this market as are the credit card companies with their tokenization programs for internet transactions. And government-provided currency is also in this market.

And here appears the third source of demand for privacy—protection from the payments privacy providers themselves. In other words, one aspect of the public's demand for privacy is demand for security and safety in the payments systems they use. What does security and safety mean in the context of payments? Simply that the information in my payments records not be exploited to my detriment—either by the management of the payments system itself or by an outsider breaking into the system.

Note, by the way, that at this level the issue of privacy becomes important not only for the retail payments systems on which I have been focusing, but also for the wholesale systems and transactions infrastructure. Indeed the potential problems are analogous. Both retail and wholesale payments operators might be tempted to exploit the information derivable from the transaction history—in the retail context the patterns of purchases will be of value to marketers; in the wholesale or central counterparty context, the pattern of trades may reveal valuable, hard-earned information about the financial assets being exchanged.

In all financial infrastructure the more direct concern, of course, is the possibility that through neglect or incompetence the operator might allow others to get at the payments information thereby providing fraudulent access to users' identities and to the deposits in their accounts. The concern about this type of privacy, if payments systems can be hacked, is real—again, with ready examples of breaches at all levels. So for a variety of reasons, there is plenty of unmet demand for privacy in payment.

GOVERNMENT AS PRIVACY PROVIDER?

If the government cannot prevent the ill effects from the absence of privacy, perhaps the government can provide the privacy itself. So there is the question: should government entities merely regulate privacy standards in privately-provided payments arrangements? Or should the public entities (in particular, central banks) be providing privacy-protecting payments arrangements?

Well, of course, they already are, in the form of physical central bank notes. But many central banks are currently contemplating providing an alternative, an electronic money which would be in this market as well.

As the central bank gets out of the business of cash provision, whether by choice or by increasing competition from private alternatives, it is natural for central bank governors to consider whether it might be desirable to enter the business of e-money provision. In one sense central banks already provide e-money: central banks' reserves on bank balance sheets are every bit as intangible and

computerized as e-moneys. The key difference between new proposals and the existing electronic arrangements lies in their inherent privacy.

In other work (Kahn and Roberds, 2009), Will and I have emphasized the importance of the distinction between arrangements that connect a transaction with the transactor's identity and those that leave it anonymous. We have done so by distinguishing between "account-based systems," in which the system provides an account for each user, and payments are made by transferring funds into or out of his account once he has been identified, and "token-based systems" in which payment is effected by transferring a "thing" without the need to identify transactors.[3]

An account-based system may offer its users anonymity relative to their counterparties (to a limited degree this is possible in PayPal) without keeping the users anonymous from the system itself.

On the other hand paper bank notes also maintain anonymity from the issuer (whether the issuer is a central bank or private bank). More precisely, the issuer may know the identity of the initial recipient of the note, but as the note is passed hand-to-hand, no one down the line need know the identities, and certainly not the initial issuer. One of the cool features of bitcoin is its ability to permit transactions across the internet while maintaining privacy from the bitcoin system.

Therefore in our dichotomy, a user of a token-based system need not be concerned with the competence of the issuer to maintain the user's privacy. Contrast this with the typical bank or credit card account where privacy is only as good as the ability of the bank to deliver that privacy. The new proposals for central bank e-money are largely token-based systems, as opposed to the account-based reserve balances central banks already issue.

[3] This distinction was first noted by Ed Green (Green 2004), and it cleanly categorizes most historical payments arrangements. While modern computer systems allow a variety of intermediate cases, the dichotomy is still a useful simplification for this discussion.

Both central banks and private institutions are capable of issuing e-money. Therefore an important factor in determining the desirability of an e-money arrangement is the question of whether the central bank or private parties have a comparative advantage in providing transaction privacy.

I think there are some important reasons that a central bank in the twenty-first century cannot be in the business of providing privacy services electronically.

First, it's hard to argue that the central bank will have greater technical skills in protecting privacy (at least in retail transactions; wholesale and infrastructure may be a closer call). The standard regulatory arguments for oversight of payment systems apply however: there is an easy case for a regulator to be in charge of setting and harmonizing standards for privacy protection.

On the issue of trustworthiness, the answer is more difficult: payments service providers amass large amounts of valuable data on customers; the temptations for misuse by them are huge. So it might seem that public providers could have an advantage in terms of trust. The only problem is that central banks are also not trusted institutions. The public has little understanding of what central banks do and central banks have little understanding of having members of the public as direct customers. Given this unfamiliarity, and given the general suspicion of financial institutions post-crisis, central banks are convenient bogey men for demagogues in need of scapegoats, further reducing trust.

But it is not merely a matter of perception. While private payments institutions have an incentive to use the information they amass, and a temptation to abuse the information amassed, governments would be no less tempted: just for different kinds of privacy invasion. Every twist and turn in politics provides an opportunity to justify an examination of one or another aspect of individuals' transactions. And it is not clear that in the current political environment, a central bank or a payments authority will be any stronger at pushing back on these intrusions than private institutions are.

Nor will transparency solve the problem. Paper money is transparent: the technology eliminates the ability of the issuer to monitor transactions, and "it is a

truth universally acknowledged" that paper money does so. No computer technology can have this degree of confidence. Only an infinitesimal proportion of people on this planet can verify that code does what it is advertised as doing, and nothing more. To believe that the CIA has imprinted paper currency with a technology enabling it to report hand-to-hand transactions is paranoia. To believe that spy agencies have backdoors to common computer programs is last week's news.[4] Generating trust in the privacy promises of a public payment authority's new electronic money seems to me an extremely tall order.

PROSPECTUS

So if we can't hope for the government to be the source of privacy for the electronic replacement to cash, what will the future be for privacy in payments?

First, expect different systems to handle different kinds of privacy. As seen, the demand for privacy, like the demand for other aspects of payments services, is multifaceted—we would expect that transactors will in the end adopt a variety of payments media specialized to particular needs.

In this respect, I am in awe of my college-aged daughter, who has on occasion attempted to explain to me the distinctions among the plethora of e-payment platforms she uses: why this one is most appropriate for collecting the rent from her roommates, and that one for certain kinds of internet shopping, and which she thinks are safe to link to her bank account and which not. In her mixture are both established financial institutions and upstart technology firms. We would expect different kinds of institutions to have different takes on privacy protection; after all they place differing values on their own long term reputations, and are subject to differing dependency on regulatory institutions.

Second, expect different systems to offer different degrees of privacy. Privacy is not an absolute—attempts to maintain privacy can always be undermined by sufficient digging. Any household security system can be thwarted by a burglar

[4] As Mr. Weasley admonished the children in the second Harry Potter book, "Never trust anything that can think for itself if you can't see where it keeps its brain" (Rowling, 1998).

with sufficient incentive and sufficient means. The homeowner's goal is to make it so expensive that the typical burglar finds it not worth the effort. And so we can expect that agents will use higher levels of privacy protection, despite their cost and inconvenience, when the stakes are high enough. There is really nothing new in that statement: the rich have long used legal structures to maintain privacy in major transactions—think of real estate trusts to hide ownership. And again, this is a prediction which *mutatis mutandis* applies to the rest of the payments infrastructure.

Third, expect increases in the number of systems emphasizing privacy advantages. Alarmists say privacy is disappearing. Cynics respond that we've never had privacy; it was only that the cost of thwarting privacy used to be high. The panic about privacy is really due to the dramatic reduction in the costs in recent decades of collecting and disseminating the vulnerable information. The fear Google arouses is not because the information wasn't already public; it was just sufficiently difficult to dig it from old court records and small town newspapers that no one would bother. So as these costs become lower and as people become more aware of the pervasiveness of the vulnerabilities then we would expect more and more individuals to turn to payments technologies for privacy protection in specific transactions.

Fourth, don't just expect, <u>embrace</u> creative tension. All institutions, public or private, are likely to be untrustworthy—they are just going to be untrustworthy in different ways. We are not really interested in an absolute guarantee of privacy; we simply want it to be sufficiently difficult to violate privacy that it can only be done in a publicly-observed and generally-agreed way. Using the differences in objectives of the private and public spheres becomes, it seems to me, a way of making this tension work for us: public regulation with pushback by private providers seems to me the more hopeful formula.

So where does this leave the role of a government e-money? There are still possibilities: a token system for large value settlement may have operational advantages when interacting with other infrastructure. Government e-money could serve as a convenient standardized unit for filling prepaid cards or e-wallets.

This could benefit start-up payments providers who would otherwise have to build a reputation to convince payees that they had the reserves needed to back their payments solutions, or depend on established major banks to provide the backing. For major banks reputation of their funds would not be an issue, but the regulatory burden of anti-money laundering rules and know-your-customer would be alleviated by the ability to offer depositors a way to pay someone without that payment turning into an account at some bank. In other words, the arrangement can offer a privacy loophole in response to overly expensive anti-privacy regulation—a second-best to refining the regulation itself.

CONCLUSION

Not all of the privacy provided by cash is bad, and if cash disappears we will need new ways of providing that privacy. Because privacy needs are different in type and degree, we should expect a variety of platforms to emerge for specific purposes, and we should expect continued competition between traditional and start up providers. We shouldn't expect e-cash to play all the privacy roles that physical cash currently plays. There will be a demand for systems providing counterparty anonymity, at least until the millennium of smart contracts arrives. While the central bank or a payments authority will need to regulate privacy protection, the use of token-based systems will help minimize dependence on the competence and high-mindedness of start-up payments arrangements.

When central banks first took on the job of note issuance they became privacy providers. As they try to get out of the paper money business, I think the future of central banks and payments authorities is no longer in privacy provision but in privacy regulation, in holding the ring as different payments platforms offer solutions appropriate to different niches with different mixes of expenses and safety, and with attention to different parts of the public's demand for privacy. For central bankers, the bad news is that a new, vocal constituency will be complaining about the job they are doing. The good news is that, if they were to

end up actually attempting to provide the privacy themselves the complaining would only have been worse.

REFERENCES

Green, E.J., 2004. “Challenges for research in payments,” invited lecture at The Economics of Payments, Federal Reserve Bank of Atlanta, March.

Kahn, C.M., McAndrews, J.J., Roberds, W. 2005, “Money is Privacy,” *International Economic Review,* Vol 46 issue 2, pp 377-399

Kahn C.M. and Roberds W. (2009) “Why Pay? An Introduction to Payments Economics,” *Journal of Financial Intermediation,* Vol 18 no. 1 pp 1-23.

Kocherlakota, N.R., 1998. Money is memory. *J. Econ. Theory* 81, 232–251.

Rogoff, K.S., 2016, *The Curse of Cash,* Princeton University Press.

Rowling, J.K., 1998, *Harry Potter and the Chamber of Secrets,* Bloomsbury.