Payment Systems and Privacy

Charles M. Kahn

Privacy in payments is desired not just for illegal transactions, but also for protection from malfeasance or negligence by counterparties or by the payments system provider itself. Proposals to abolish cash take inadequate account of these legitimate demands for privacy. While central banks can play a useful role in setting standards for payments privacy, they are unlikely to have a comparative advantage at providing privacy. Therefore the replacement of cash by central bank electronic money is likely to spur demand for alternative means of payments to solve specific privacy problems. (JEL G23, E50, E59)

Federal Reserve Bank of St. Louis *Review*, Fourth Quarter 2018, *100*(4), pp. 337-44.
https://doi.org/10.20955/r.100.337-44

Two opposing forces are coming to a head for central banks and payments systems regulators: increased awareness of and concerns about threats to privacy in payments systems and increased pressure to move away from cash and toward new electronic payments arrangements.

Concerns about privacy have grown relentlessly as data security breaches have become commonplace. Policymakers now fully recognize the importance of privacy considerations in financial infrastructure, including payments arrangements. This article contrasts the demand for privacy by transactors with central banks' ability (and inability) to provide privacy, with particular reference to recent e-money proposals. It concludes with implications for how privacy may be provided in emerging payments arrangements.

DEMAND FOR PAYMENT PRIVACY

The demand for payment privacy has several distinct sources. The obvious one is the desire to engage in illegal transactions: cash payments for purchasing illegal drugs or to avoid

Charles M. Kahn is a research fellow at the Federal Reserve Bank of St. Louis; an emeritus professor in the departments of economics and finance, University of Illinois, Urbana-Champaign; and a visiting scholar at the Bank of Canada. This article is based on a keynote address for the conference "Financial Market Infrastructure Conference II: New Thinking in a New Era" at De Nederlandsche Bank, Amsterdam, June 7-8, 2017 (published as Kahn, 2018).

tax on unreported income; bitcoin payments to ransom hijacked computers or people; offshore bank accounts for bribing corrupt officials. Cash is not the only method for making illegal transactions, but it makes these transactions easier, through either direct payment or the process of money laundering, where a cash stage in the series of disguising transactions (so-called "layering") helps to foil attempts to trace the ultimate sources of payments.[1]

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 tend to favor abolition of this kind of privacy.[2] This is a position staked out by many philosophers and political thinkers and regularly by some (though not all) economists.[3] 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. (Notable recent examples are Sweden and India.)

However, there are other sources of demand for privacy. Individuals sometimes desire privacy not for protection from government scrutiny, but for protection from the other party to the transaction. Suppose, for example, that I wish to make a transaction with a stranger but wish to ensure that there are no unpleasant ramifications down the road. It is not hard to think of examples where the information about the 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 (certain medications, for example). More prosaically, making a purchase on the internet involves the revelation of identity in ways that make you subject to spam or harassment. In short, sometimes we want the ability to ensure that others cannot use the information in the history of our transactions against us.

Demand for privacy in this respect is the everyday commercial equivalent of the desire for a "right to be forgotten," a desire that is underappreciated in current economic theory. We recognize the importance of the ability to build reputations. We *want* these reputations to have ramifications in the future: Our good behavior and fair dealing today lead to trust in our actions in the future. More importantly, the fear of the consequences of a bad reputation is a strong, credible motivator to engage in good behavior today.[4] 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 those contracts. Also valuable are the technologies that facilitate the recording and implementing of these arrangements. Sophisticated insurance arrangement and complex investment projects would be impossible without adequate record keeping and enforcement.

The demand for privacy is an important flip 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 is closely related to 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 have led to more and more cases where the payment is not as final as we thought: clawbacks, extraterritorial rulings, new forms of product liability. Therefore we include clauses in these contracts that provide insurance, state what will happen in the event of disputes, and specify who has authority to raise objections or undo the arrangement in

which circumstances and who has jurisdiction to make the judgment. 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. Blockchain and smart contracts may eventually solve the problem for parties with the ability 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.

The ability to make a transaction without revealing your identity is therefore useful even when the transaction is legal. Cash is a simple way to make that possible. Kahn, McAndrews, and Roberds (2005) argue that an important role of cash is its ability to protect the purchaser's identity[5] and therefore a system allowing cash transactions can be welfare improving. All that is necessary for this conclusion is the existence of a moral hazard problem linked to the revelation of the counterparty'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 payments arrangements based on credit and deposit accounts, cash would survive.

Of course one 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.

Thus 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.

The third source of demand for privacy is for protection from the payments 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. The temptation to use information arises at both the wholesale and retail levels of payment. Patterns of retail purchases are 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. And with ready examples of breaches at all levels, the concern about this type of privacy is real.

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?

Of course governments already provide privacy-protecting payments arrangements in the form of physical central bank notes. But many central banks are currently contemplating providing an alternative—an electronic money that 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-money. One key difference between some of the new proposals and the existing electronic arrangements lies in their inherent privacy.

Kahn and Roberds (2009) emphasize the importance of the distinction between arrangements that connect a transaction with the transactor's identity and those that leave it anonymous. That work considers the fundamental distinction between two systems: (i) "account-based systems," in which the system provides an account for each user and payments are made by transferring funds into or out of a user's account once the user has been identified, and (ii) "token-based systems," in which payment is effected by transferring a "thing" without the need to identify transactors.[6]

An account-based system may offer its users anonymity relative to their counterparties (to a limited degree this is possible in PayPal, for example) 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.

In terms of this 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. Many new proposals for central bank e-money are token-based systems, as opposed to the account-based reserve balances central banks already issue.

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 will not be an effective provider of electronic privacy services.

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 payments 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 about their customers; the temptation to misuse such data is 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 experience having members of the public as direct customers. Given this unfamiliarity and the general suspicion of financial institutions post-crisis, central banks are convenient bogeymen 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 that information, governments are also tempted, only 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 in the current political environment that 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 computer code does what it advertises it does and *only* what it advertises. 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. Generating trust in the privacy promises of a public payments authority's new electronic money will be an extremely tall order.

PROSPECTUS

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

As seen, the demand for privacy, like the demand for other aspects of payments services, is multifaceted. We should expect different types of systems to handle different kinds of privacy. After all, they serve different market niches. We should also expect different types of systems to offer different degrees of privacy protection; they are, after all, subject to differing dependency on regulatory institutions and place differing values on their own long-term reputations.

The prospect of some privacy-poor systems is not necessarily a bad thing. 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 with sufficient incentive and

sufficient means. The homeowner's goal is to make it so expensive that the typical burglar won't find it worth the effort.

Transactors will in the end adopt a variety of payments media specialized to particular needs. And so we can expect that agents will use low-security systems when the concerns are insignificant and higher levels of privacy protection, despite their cost and inconvenience, when the stakes are sufficiently high. There is really nothing new in this sort of arrangement: Individuals who have felt themselves to be vulnerable have long used legal structures to maintain privacy in major transactions—think of real estate trusts to hide ownership.

In fact, we should expect an increase in the number of systems that enact a marketing strategy that emphasizes their 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. As these costs become lower and as people become more aware of the pervasiveness of the vulnerabilities, more and more individuals will turn to payments technologies for privacy protection in specific transactions.

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.

Finally, because of their comparative strengths, we can expect both public and private institutions to play a role in payments provision. All institutions, public or private, are likely to be untrustworthy—they are just going to be untrustworthy in different ways. Citizens are not really interested in an absolute guarantee of privacy; we simply want it to be sufficiently difficult to violate privacy that it can be done only 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.

Is there still a role for 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 either 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, the reputation of their funds would not be an issue, but the regulatory burden of anti-money laundering and know-your-customer rules 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 golden age 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. Taking on the role of privacy regulation will open central banks to regular criticism from a new, vocal constituency—but less criticism than if they tried to provide privacy services themselves. ■

NOTES

[1] For an introduction, see Masciandaro, Takáts, and Unger (2007).

[2] On the other hand, if you want to hide an activity that you believe should not be illegal in the first place, you'll favor this kind of privacy for yourself, since you would use it only to break "bad" laws. But you still might oppose this kind of privacy for other people, since they might use it to break "good" laws.

[3] For example, this position was taken recently by Ken Rogoff (2016) in his celebrated book *The Curse of Cash*.

[4] 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.

[5] Our article was written partly in response to the important work of Kocherlakota (1998), who argues that money is primarily a record-keeping device.

[6] This distinction was first noted by Ed Green (Green, 2008), 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.

REFERENCES

Green, E.J. "Some Challenges for Research in Payments," in S. Millard, A. Haldane, and V. Saporta, eds., *The Future of Payment Systems*. Routledge, 2008, pp. 57-67.

Kahn, C.M. "The Threat of Privacy." *The Journal of Financial Market Infrastructures*, 2018, *6*(2/3), pp. 21-30.

Kahn, C.M.; McAndrews, J.J. and Roberds, W. "Money is Privacy." *International Economic Review*, 2005, *46*(2), pp. 377-99; https://doi.org/10.1111/j.1468-2354.2005.00323.x.

Kahn, C.M. and Roberds, W. "Why Pay? An Introduction to Payments Economics." *Journal of Financial Intermediation*, 2009, *18*(1), pp. 1-23; https://doi.org/10.1016/j.jfi.2008.09.001.

Kocherlakota, N.R. "Money Is Memory." *Journal of Economic Theory*, 1998, *81*, pp. 232-51; https://doi.org/10.1006/jeth.1997.2357.

Masciandaro, Donato; Takáts, Előd and Unger, Brigitte. *Black Finance: The Economics of Money Laundering*, Edward Elgar Publishing, 2007.

Rogoff, K.S. *The Curse of Cash*. Princeton University Press, 2016; https://doi.org/10.1515/9781400883219.