Risk and Privacy Implications of Consumer Payment Innovation in the Connected Age
Commentary

Alessandro Acquisti

It is always a pleasure to read a new paper by Professor Anderson. There is always something new to learn. Especially in this case. Mobile payments are not my research focus. My research focus is the economics and behavior economics of privacy. When you have a hammer, everything looks like a nail. So, I will focus my remarks on the privacy angle in Professor Anderson's arguments. First, however, I will briefly summarize what I thought were the main key points in the paper.

There exist dominant players in the payments industry—no doubt. But there are many challengers, too. Therefore, complexity is growing and governance is becoming more difficult. Innovation in this area may increase fraud—but that may be a price worth paying, considering the welfare benefits that more mobile technologies can bring.

Therefore, Professor Anderson's recommendation is: "Do not be afraid of innovation. In fact, foster innovation. Try indeed to create some formal central reporting of fraud, as has been happening in other countries."

Among these points, perhaps the conclusions which I found most interesting were the predictions Professor Anderson makes—and I find them reasonable predictions: with mobile payments, we probably will see an uptick in fraud and an uptick in complexity. I found that reasonable to expect; I am in fact going to push the envelope here, and consider other cases where fraud may become more common and other reasons why complexity could cause more fraud. But then, I will also try to invert the cards, and discuss an alternative scenario where, in fact, these technologies are going to bring less fraud and less complexity. Then, I will twist the cards once more, to suggest that less fraud and less complexity are not necessarily always a good thing.

Bear with me. Hopefully, I will get there, and hopefully I will be clear.

So, let me start with more fraud. There is a stream of academic research which combines computer science, psychology, cognitive research and usability studies, and which focuses on the security and the usability of security systems—for instance, how people respond to security warnings. It is a fairly recent literature—the first paper in this area was from 1999. Alma Whitten, at the time at Carnegie Mellon University (she now is director of privacy at Google), wrote a paper with a very catchy title, "Why Johnny Can't Encrypt." She ran some experiments with smart students—of course, they were CMU students—giving them encryption technologies to protect their data, only to find out that the students believed they had protected their data, but in fact they had not. This is the worst-case scenario—people believing they are protecting themselves and therefore acting under that belief—when in fact they are not protecting themselves.

This stream of research is recent, only 10 years or so old. There is an even more recent stream of research, which focuses on usability of security and privacy on mobile devices. Security and privacy on mobile devices represent a worst-case scenario, in the sense it is already hard to properly display security information on desktops (many security signals are hard to comprehend unless you have a computer science background. Figure 1 is a typical message telling the consumer or the Internet user: "Aw, there is something not so good about the website where you are about to go." It then proposes a number of choices the average Internet user may not be equipped to choose among. Well, when you translate these signals into the mobile world, you have a seemingly different problem. You now have messages which succeed in being simultaneously very terse and ominous.

Figure 2 is an example of another—PhotoSpy, which wants to access your photos. You do not know exactly what PhotoSpy will do with your photos. But you are there, using your device, probably doing something else under a state of cognitive load (because maybe you are driving, maybe you are in a store, and you are not paying much attention). The "OK" button, which is the one highlighted, is big. So you click on it—maybe even when the messages are even more ominous. I would say that, in this sense, the more we will be using mobile payments, the more we will face these kinds of challenges.

The good thing about mobile payments is that they should be really easy to use—seamless to use. Otherwise, why not use credit cards? But the more seamless and invisible they become, the less attention they require from the user. That also means, however, that the more vulnerable they leave us to social engineering attacks (which tend in fact, to focus on user inattention).

A second problem Professor Anderson was referring to is the fragmented payment ecosystem. There are up to 300 different electronic payments systems listed on Wikipedia. The ecosystem is very fragmented—and the problem is that, as economic historians know very well, the best technology does not always win. For instance, consider a very significant problem—the fact that many payment systems still use passwords confusing together identification and authentication. Identification is a

Figure 1

Figure 2

process through which you tell a system who you are. Authentication is a process through which you prove you are who you claim to be. When you are using credit cards, you are providing to the entity which receives your credit card number the information needed for impersonating you. If another party just has your credit card number and the three digits on the back of your card, they can impersonate you (authenticate themselves as if they were you).

Well, we have had much better authentication (and payment) technologies than that for many, many years. Let me give you an example. Figure 3 depicts a very well-known protocol to those of you who have a CS background. It may be less known among economists: It is a blind signature. The blind signature was a protocol developed in the 1980s by David Chaum. It then was transformed by Stefan Brands into anonymous credentials, which can be used for anonymous payments, in which you have at the same time authentication separated from identification. The idea is analogous to making a carbon copy. Do you remember carbon copy paper, through which you can write something on the first sheet, and that something transfers down as you press onto the second sheet? Imagine that you put a piece of paper together with carbon paper inside an envelope and you give the envelope to the bank together with a payment for $1. The bank receives the $1 from you, knows who you are, puts a stamp signature on the outside of the envelope and gives you back the envelope. The signature, because there is a carbon copy, has now been copied onto the sheet of paper inside the envelope, which the bank has never seen. So, now you can open the envelope and you have a document, signed by the bank, worth $1. While the bank can recognize the document as a valid $1 bill, it cannot recognize it as your bill, so you can spend it at any merchant—achieving full authentication (complete payment) but no identification (anonymity). Arguably, this is a more secure method than just passing a password. But do we have an existing payment system using this technology? Not really. In the United States only one bank was providing this payment—it was called eCash—only for a few years, because this technology did not go anywhere.

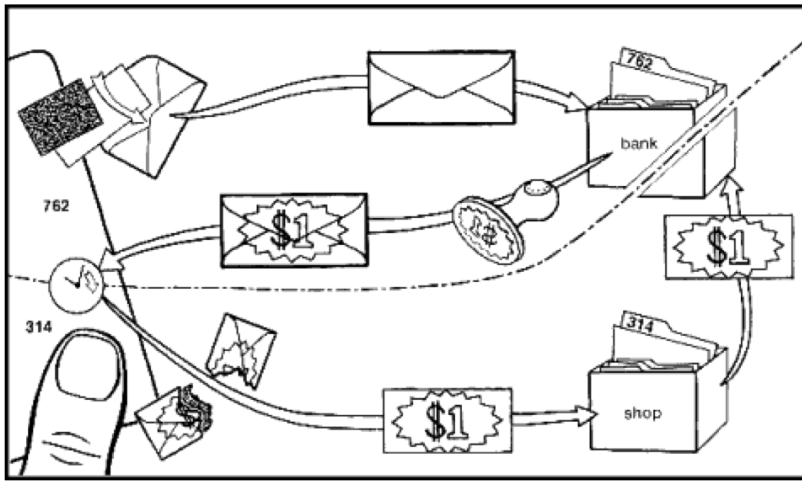
So, yes, I agree that we can have more fraud and more complexity with mobile payments. However, I also wanted to propose a different angle—the angle from which we have less fraud and less complexity. And then I will also mention, why I do not think this would necessarily always be a good thing.

In order to explain that, I would like to invoke two buzz words—one of them "social" has already appeared many times today. The other appears at any conference on privacy nowadays—so I guess I will be guilty of being the first to bring it up today: "big data." So we have "social" and "big data"—the two buzz words.

Of course, companies involved in mobile technologies have an interest in going social, in entering social networks (either coordinating with existing ones like Google+, Facebook, or creating their own). The two buzzwords (big data and social), reinforce each other, in the sense that the larger the social network you have,

Figure 3

Blind Signature and Electronic Cash



the more social data you can create. The more data you can create, the better your social network becomes. The better your social network becomes, the better you are able to target marketing information, products, and so forth.

This is good. In fact, it can create less complexity, in the sense that, as you can imagine, social networks and big data are inherently about network externalities—economies of scale and economies of scope. Facebook and Google+ are the prototypical network goods: You do not want to be in a network where no one else is! However, these networks may also suffer from negative network externalities: The moment when your grandmother is on Facebook, may become the moment you start moving your profile elsewhere (in reality, Facebook has succeeded in passing this threshold somehow unscathed). The success of the network also creates economies of scope, in that once you have so much data about people, you can start creating lots of new products. No longer only the social network itself; you can start innovating in mobile payments, too.

It is possible however, that in the future this virtuous cycle between social and big data—big data and social, social and big data—will also lead to concentration and standardization in the mobile payment industry.

This, in turn, can decrease the risk of fraud in mobile payments—because it allows providers to switch from authentication of individuals to authentication of transactions. Once you have so much data about people, you can recognize their behavior. Each behavior is a signature, and you can calculate instantly what the probability is that this person making a purchase from this type of store at this time of day from this location is really Alessandro Acquisti.

Credit card companies are already doing it, of course. Now, imagine expanding what credit card companies are doing based purely on transactional data, to what they can do when social network data is also combined.

These are the good things. But there is also, let us call it, a "dark side" to concentration and standardization and network externalities. One of the dark sides is, potentially, a decrease in competition. As you have more data, more network externalities, and the ability to combine big data and social, you start facing the temptation also to expand your business into different areas. Indeed, many of the large players in the Internet industry in recent months—in fact in recent weeks—have been accused of doing exactly that.

As a little exercise, a couple nights ago, I simply went to Google and I typed a name of a large Internet or Silicon Valley player, and then added to that the word "forces," and then I looked at what responses I received, using Google's auto-complete. It turns out that, nowadays, everyone is being accused of forcing someone else to do something. Apple is being accused of forcing a PC maker to stop making Acer ultrabooks because they compete with Apple MacBook Air or the iPad. Microsoft is being accused of blocking computer hardware from booting competing operating systems. Google is being accused of pushing Android developers to only use Google Wallet. I have not forgotten about Facebook, by the way. I am getting there in a second.

In terms of privacy externalities, the second potential danger here is the fact that, if you believe the network externality story, you also must conclude, that for those who want to protect their privacy, the costs of doing so is becoming larger and larger. Let me give you an example. There are more and more newspapers in this country that use Facebook Connect for their own commenting systems. Before, if you wanted to comment anonymously on the *Los Angeles Times*, you could do so. Now you cannot, unless you deliberately violate Facebook terms of services (because to comment on *The Times* you must be member of Facebook, and under Facebook terms of services, you are supposed to join with a profile that uses your real first and last name. Not everybody does that, but now you are in violation of the terms of services if you do not).

You can export this challenge to the mobile payments story, and see how—as more and more people start using, for instance, Facebook Credits for payments—then, more and more merchants will start using that too. But then, people who do not want to use Facebook may not be able to buy from these merchants.

Another story. Privacy as control over personal information, or privacy as protection from the control others have over you, once they have information about you? Once again, it is about the power of networks: once they become larger, their ability to influence your behavior in other parts of your life increases.

Take, as an example, Facebook's recent change in policies. If you sign up now, you are agreeing not only not to use the term "Facebook" as a trademark, but also

not even the term "book" or the term "face." So, in this instance, a company tries to expand its claims over the right of its users, once it has reached a certain size and power.

So, bringing this all back to where we started: my point is that mobile payments are both the products and the drivers of acceleration in economic and social changes. We cannot fully predict where they will bring us. You can imagine science fiction scenarios (which are not that much science fiction any longer). You can imagine how—and we are already starting to see this—years ago we went on the Internet to search for information, but now we go there looking for suggestions (there are more and more tools, like Yelp, that provide you with suggestions about where you can go). And then from suggestions, we get into decisions. I was browsing the Internet just a few minutes ago, and I was checking out an application which can choose automatically the perfect seat on your next flight for you. You choose your settings once, and then this app checks with the airlines every four hours, to see whether a seat better matching your needs has popped up. It is good, because automatically it takes the pain of searching for better seats away from you. And then, the next, step, is that you can also get into automatic payments: eBay did something along those lines a few years ago, allowing users to structure bids so that a certain item could be automatically bid upon.

So, finally, you can imagine now a complete sequence in which the future of payment technology is its own disappearance, in that you no longer even need a mobile phone or a smart card. The system knows exactly what you want, before even you know it, and buys it for you. Is it science fiction, or are we just 10 years away from that?

And this can be good, too. It can increase welfare. But…welfare for which party exactly, and at what cost? The now obligatory mosquito bite analogy (to paraphrase Professor Farrell) is the following: in the case of privacy, privacy costs are the mosquito bite. They are very small. You may not even notice them. But over a large number of people, over a long enough period of time, the bites amount to a very, very large transfer of wealth. Thanks.