Robert Tann

Discussion of "Digital Impact on Payments, Credit and Financial Risk Management: New Ethical Questions?" by José Manuel González-Páramo

1. In his paper, Professor González-Páramo has given us a thought-provoking review of some of the key ethical questions arising in our connected, digital economy. I would like to add some thoughts as a private citizen rather than an expert, and I hope they are not too simplistic.

Professor González-Páramo's insistence that financial institutions, and especially banks, must maintain a humanistic vision of their rôle in the economy and of their reason for existing is all the more important as it is so infrequently heard today. The algorithms which support and facilitate the new credit platforms leave no space for a "humanistic vision" and the sponsors of these ventures are also silent on the subject. Professor González-Páramo rightly reminds us that traditional bank lending brings with it an enormous impact and a heavy responsibility - in providing credit, retail banks are investing in human capital and helping individuals bring their projects to fruition. But in the digital marketplace, this is at best a side effect, rather than the guiding ambition of a credit scoring process.

2. The use of Big Data by banks is defended as a powerful tool for uncovering new correlations and for predicting customer behaviour. Certainly, credit institutions already have very valuable information about their customers' spending habits and spending intentions, and advanced data analysis has opened up far-reaching new uses for this information. The cross-filtering of customers' transactional data with other information, especially information about their on-line activity which may have been "offered" freely to service providers, then collated, "anonymised" and sold to third parties, is particularly revealing. Advertising agencies expend much energy in arriving, with the help of overlapping filters, at the granularity that banks can easily obtain. All this is undeniably positive for the banks, but less so for their customers, and we may be too late to change it.

3. This brings us directly to the ethical questions of privacy and trust highlighted in Professor González-Páramo's paper.

It goes without saying that in the digital world, all business models are built on trust and privacy, and that banks, perhaps more than other service providers, must ensure that customer information is held securely even as hacking methods - and marketing tactics - improve. National and supranational regulators have a clear mandate to enforce this security with forward-looking standards. However, today's digital giants such as Google and Facebook owe their success precisely to their ability to extract, retain and monetize customer information in the teeth of any concerns about privacy and trust. All this has been achieved with the simple use (or misuse) of the concepts of "consent" and "permission". Faced with a monetary incentive, or with the threat of a service being witheld, most customers willingly hand over their right to privacy, without qualification and without compensation. It is the customers themselves who opt out of privacy protections, and they do it in a way that actually binds them more closely to their service providers.

Some of these issues have been tested recently in American courts, where plaintiffs have alleged (for example) that their messages were scanned even though their email addresses were with a different provider, or that a social media service was reading e-mails, using photos and accessing personal address books without permission. Earlier cases saw claims thrown out because the plaintiffs could not prove they had suffered harm, but more recently courts have ruled that companies were not disclosing enough details of how they intended to use extracted information in their (lengthy) consent wordings. So far, penalties awarded appear to have been only in the tens of millions of dollars, which is hardly a strong deterrent in the context of annual on-line advertising revenues in excess of $42 billion.

4. It seems incredible but it is true that before being caught in the act, some Google Street View cars with their 360 degree cameras were not only taking pictures of all the residential and commercial districts they visited, but were also extracting personally identifiable data from unencrypted Wi-Fi connections as they went along.[1]

Gmail itself could be viewed as a supremely effective tool for invasive profiling, as Yasha Levine has argued:[2] "All communication was subject to deep linguistic analysis; conversations were parsed for keywords, meaning, and even tone; individuals were matched to real identities using contact information stored in a user's Gmail address book; attached documents were scraped for intel - that info was then cross-referenced with previous email interactions and combined with stuff gleaned from other Google services, as well as third-party sources"… [Google then created profiles on Gmail users, based on] "concepts and topics discussed in email, as well as email attachments [including] the content of websites that users have visited; demographic information - including income, sex, race, marital status; geographic information; psychographic information - personality type, values, attitudes, interests, and lifestyle interests; previous searches users have made; information about documents a user viewed and or edited by the users; browsing activity; previous purchases." With your permission, this is the value exchange for your free email account.

5. The EU has been hard at work to strengthen the regulation of digital services and to protect the privacy of the consumer. The draft regulation, released on 10 January, updating the EU's ePrivacy law will supplement the General Data Protection Regulation, enacted last May and entering into application on May 25, 2018. The draft regulation is a high-quality and forward-looking instrument, requiring manufacturers and retailers to respect consumer privacy and requiring service providers to seek prior consent for many of their most profitable activities. It introduces a duty-of-care requirement to have user-friendly hardware and software default settings (for example, do-not-track settings) on the part of manufacturers and retailers of connected devices. It also brings up to date rules regarding spam, cookies and location-based services, and it allows providers to withold content from users who browse with an ad-blocker. But in all these cases, the Achilles' heel of the proposed regulation is that users can choose to lose their privacy rights when asked to opt in or out. When the alternative is paying for a service that is otherwise free, or having a valued service witheld, experience shows that consumers vote for "transparency" instead of privacy. I suspect that if prior-consent wordings were less helpful to the service providers, they would respond with outright money offers to "purchase" user consents.

---

[1] John W. Whitehead, The Rutherford Institute, 12 May 2014

[2] ibid.

6. In short, consumers have already lost the battle for privacy, and if we look at where the internet is going, we may well conclude that this defeat cannot be overturned.

Consider the vision of the connected future reflected in the public utterances of Eric Schmidt of Alphabet and Mark Zuckerberg of Facebook, companies with market values of $565 billion and $370 billion respectively. The stock market puts quite a value on their ability to extract customer data.

a). The convergence of search, location and social is the next big narrative. Schmidt says that people who "opt in" to the system will begin experiencing a much richer relationship with technology, aided by their computerised "personal assistant".
"We still think of search as something you type," Schmidt said. "Perhaps a decade from now, you will think, well, that was interesting, I used to type but now it just knows. How does it know? Well, on mobiles we know where you are, down to the nearest foot. You've chosen to log in, with your permission, and it knows where you are and it can provide a personalised service … Technically, with your permission, we know where you are, we know your history, we can do data extraction and look at what it tells us."[3]

b). "One day, I believe we'll be able to send full rich thoughts to each other directly using technology. You'll just be able to think of something and your friends will immediately be able to experience it too, if you'd like. This would be the ultimate communication technology … We're working on Virtual Reality because I think it's the next major computing and communication platform after phones...I think we'll also have glasses on our faces that can help us out throughout the day and give us the ability to share our experiences with those we love in completely immersive and new ways that aren't possible today."[4]

"First, people are gaining the power to share in richer and richer ways. We used to just share in text, and now we post mainly with photos. In the future video will be even more important than photos. After that, immersive experiences like virtual reality will become the norm. And after that, we'll have the power to share our full sensory and emotional experience with people whenever we'd like. Second, people are gaining the power to communicate more frequently. We used to have to be with someone in person. Then we had these bulky computers at our desks or that we could carry around. Now we have these incredible devices in our pockets all the time, but we only use them periodically throughout the day. In the future, we'll have augmented reality and other devices that we can wear almost all the time to improve our experience and communication."[5]

Not everyone perceives these pictures of the future as preserving human dignity or protecting a humanistic vision of society. To me they seem like its opposite, but no less inevitable for that. Professor González-Páramo aptly quotes Michael McFarland: "Losing control of one's personal information is to a large extent losing control of one's life and one's dignity". I fear the future that inescapably awaits us is one of "rich and immersive serfdom".

---

[3] Eric Schmidt, interview with Kamal Ahmed (Daily Telegraph), World Economic Forum, January 2011

[4] Mark Zuckerberg, Facebook Q&A, 1 July 2015

[5] ibid

7. We still use the phrase “in the privacy of your own home”, but in reality, this expression is already antiquated. Today there is almost nothing private about your own home, thanks to mobile phones, smart devices and and internet tracking. Robert Shrimsley of the FT jokingly quotes the head of Scotland Yard’s Digital Forensics Unit as saying that your refrigerator might one day keep you out of jail (by providing your alibi and proving your innocence), but it is equally possible that your washing machine will prove your guilt and lead to a conviction.[6]

Consider Alexa, available with Amazon’s Echo, a metal tube containing speakers and microphones which connects to the cloud, acts as a personal assistant, answers questions, streams music and orders things for you on-line, activating whenever it hears “Alexa”. Echo’s microphones *are always listening* unless physically switched off. The data collected is analysed and used for targeted advertisements and “an enhanced service”. It may be sold to third parties without the speaker’s knowledge. As journalist Rory Carroll points out, *all* of the recorded data is uploaded and stored in the cloud, once the Alexa trigger word is spoken.[7] A few days after Rory’s private discussion at home with his wife about babies, his Amazon Kindle device offered him unprompted adverts for diapers. When questioned, Alexa couldn’t explain how that had happened. Anyone familiar with Stanley Kubrick’s “2001” knows where this leads.

Mobile devices give away our location and our activities. Even when we change our system settings to turn off location services, our devices show approximately where we are, and we might discover that the location function has been restored, for example with an app update. Mobile phones can be activated remotely to record what we say, whether or not they are switched off.

Moreover, to quote Edward Snowden[8], “Something that people forget about cellphones in general, of any type, is that you’re leaving a permanent record of all of your physical locations as you move around. … The problem with cellphones is they’re basically always talking about you, even when you’re not using them. … Are you carrying a device that, by virtue of simply having it on your person, places you in a historic record in a place that you don’t want to be associated with, even if it’s something as simple as your place of worship?”

Today, to guarantee privacy you should be taking a Faraday Cage for your mobile phone to the confessional, but in the future you will have too many personal devices for you to confess in privacy.

8. Credit provision and financial risk management are affected directly by the digital revolution. In traditional banks, credit scoring, risk profiling and portfolio modelling have become more sophisticated, bringing the theoretical benefits of better resistance to market disruptions and lower minimum capital requirements. However, only another financial crisis will prove whether these advantages are effective, and there are good reasons for caution. Many experts agree with Warren Buffett that risk management in banking should not be a bureaucratic dialogue between internal compliance resources and the regulatory authorities, but on the contrary, it should be the direct responsibility of the CEO, because it always involves critical business judgements, which cannot be delegated or bypassed.

---

6 Financial Times, 6 January 2017

7 The Guardian, 21 November 2015

8 The Intercept, 12 November 2015

As John Kay observed, “Risk management decisions are among the most important matters of business judgement in financial institutions. The devastatingly negative consequences of regulatory prescription in these areas is that such prescription has undermined business disciplines and the risk management responsibilities of senior executives”.[9]

Better analytics from the application of Big Data and advanced algorithms will not by themselves reduce the risk of another systemic financial crisis. Banks which were Too Big To Fail in 2008 are still Too Big To Fail in 2017, notwithstanding all the regulatory changes designed to avoid this outcome. Italy did not allow MPS to collapse in 2016, and I am sure Germany would not allow Deutsche Bank or Commerzbank to collapse if market conditions changed. In 2015 the combined gross notional derivative exposure of JP Morgan, Citi, Goldman Sachs, Bank of America, Morgan Stanley and Wells Fargo was more than $278 trillion - more than 28x the size of their combined assets and 15x the US national debt. Nobody knows the total gross notional amount of derivative exposures worldwide, but one estimate ranges from $630 trillion to $1,200 trillion. Warren Buffett famously called these instruments “financial weapons of mass destruction carrying dangers that, while latent, are potentially lethal”.[10]

Since the 2008 financial crisis, the Bank for International settlements in Basel has led efforts to increase the proportion of OTC derivative contracts which must be centrally cleared, introducing higher capital and margin requirements. In the interest rate derivatives market, it is estimated that three quarters of all contracts are now standardised, but this still leaves an enormous number of non-standardised and illiquid contracts which are easily sufficient to undermine the banking system in any future financial crisis. A better way to prevent another banking meltdown might be to have international agreements (or tax incentives) to force banks gradually to close out most of their contractual exposures rather than merely carrying the notional net and gross amounts, and to introduce an unambiguous obligation on banks to ring-fence their retail activities, and to prevent managements from using their retail balance sheets to finance or backstop their speculative trading positions. Any serious attempt to contain this pervasive risk will require an attack on the “scourge of rehypothecation” and it will see the world’s major retail banks become more like regulated utilities, which is no bad thing.

9. Separately, payment services are exposed to new risks as a result of the digital revolution. Although not so much discussed, the biggest of these is the risk of cyber warfare attacks by hostile governments. There have been many cyber attacks in recent years and some of them may well have involved state controlled hacking teams. Examples of successful recent hacks at banks and retailers include Global Payments (1.5 million credit cards), Target (40 million credit and debit cards), Tesco Bank (40,000 out of 136,000 checking accounts), and the Central Bank of Bangladesh theft of $100 million where apparently both SWIFT and the Federal Reserve of New York missed the red flags. The biggest customer data hack so far was the 2014 theft of 500 million user account details from Yahoo, also thought to be the work of a hostile state team. In future these attacks will only become more sophisticated (although good old-fashioned employee fraud has never disappeared) and two or three stage biometric authentication might be the only defence for banks when quantum computing allows hackers to undermine all today’s encryption systems.

---

[9] John Kay, “Narrow Banking” 11 November 2009

[10] Warren Buffett, Berkshire Hathaway Letter to Shareholders, 2002

Much has been made of the potential for gated blockchain technology to make payments systems more secure. Initiatives like the R3 Consortium and the Hyperledger Project show that the world's biggest banks are taking this possibility seriously.[11] Experts have predicted that the introduction of Digital Identity protocols will protect global payments systems and make financial markets more secure[12], while Distributed Ledger Technology will allow more rather than less rehypothecation (and by implication, more systemic leverage)[13]. In the background is the lingering concern that providers such as Google or Apple would sweep aside the traditional banks, if ever they turned their customer firepower towards full-on competition in payment and credit services.

10. Gunther Oettinger (when he was EU Commissioner for Digital Economy and Society) suggested in a WEF panel in 2011 that "we need a convincing global understanding, we need a UN agency for data protection and security." This is an interesting idea. What if national governments offered secure browsing and free e-mail addresses to all their citizens, with strong encryption and no possibility of data extraction? This might be a part of their digital welfare arrangements or their national digital taxpayer systems. Individuals could be encouraged or even forced to use safe on-line searching and browsing services, and safe e-mails as part of their personal digital identification. They would be no more exposed to government snooping than they currenly are, but better protected from the predatory extraction and onward sale of their personal transaction and location based information by third parties. Apart from the cost, there is no great practical difficulty in implementing this. The consumer would still be free to use any additional search engine or browser desired. This would cause uproar of course, and unless prevented by law, today's big service providers would find ways of "compensating" people, perhaps even with hard cash, to opt out of such services.

11. Another interesting idea is Professor González-Páramo's suggestion that the digital revolution opens up new possibilities for philanthropic initiatives. For the big retail banks, this could grow into a sizeable activity. Just imagine an initiative which used a bank's data mining capacity to flag up to potential job candidates forthcoming employment openings, in large or SME businesses, that the corporate employer does not yet realise exist, but that the bank already sees from its data analytics. Or where new public or private contracts are announced and a bank's algorithms instantly identify the best-suited applicants, and can help to match both sides. Or where it is the bank, before anyone working with the corporate customer, that can already see a company's new export opportunity from its payments data analysis, and perhaps even from its deep knowledge of the potential counterparty. Projects like these might even qualify for government assistance and funding. The biggest European banks could do this and more with their existing customer information, if they had the right incentives.

This paper has been prepared at the request of the Centesimus Annus pro Pontifice Foundation for a consultation organized jointly with Universidad Pontificia Comillas ICAI-ICADE and the BBVA Group in Madrid, January 26-27, 2017. The papers are circulated under the author's responsibility to elicit comments and to encourage debate; the views therein expressed are those of the authors and do not necessarily represent the views of the CAPP Foundation

---

[11] D.Tapscott and A.Tapscott, "Blockchain Revolution" 2016, p.69

[12] World Economic Forum, "A Blueprint for Digital Identity" 2016, p.17

[13] World Economic Forum, "The Future of Financial Infrastructure" 2016, p.27