50 shades of financial privacy

By Riccardo Spagni

18 Apr 2019

Privacy is widely held as a fundamental human right and is recognised in the UN Declaration of Human Rights, the International Covenant on Civil and Political Rights and in the Constitution of nearly every country in the world.

Riccardo Spagni

Privacy is becoming a growing concern as the world continues its mass digitisation. As we move more of our day-to-day business and personal communications and interactions online, the trail of personal data breadcrumbs we leave behind grows.

Take something as simple as an online transaction: when the average consumer pays a merchant in Europe via their PayPal account, their data goes to as many as 600 different companies. The consumer has zero visibility over any of the companies involved. The amount of metadata about our lives is staggering - and we have no control over any of it.

Financial privacy and its malcontents

Regulators have tried to resolve some of the issues around data privacy and use of personal information by businesses. The European Union's General Data Protection Regulation is a far-reaching piece of legislation that aims to protect EU citizens from unwanted or unauthorised personal data use. Although the upper limits of its sanctions still need to be tested, GDPR promises fines of up to €20m to organisations that compromise the personal data of any EU citizen.

But for most transactions, consumers and businesses remain at the mercy of a vast network of interlinked companies that process and distribute our personal metadata across the globe. A lot of this is driven by convenience: when cash was still the preferred payment method, people enjoyed a fair amount of privacy as cash transactions can be concluded away from any prying eyes.

With the introduction of electronic payment methods such as wire transfers, Swift, credit cards and mobile payments, privacy has been sacrificed for convenience. The amount of Know-Your-Customer (KYC) and Anti-Money Laundering (AML) processes in place means consumers have little in the way of financial privacy as financial services firms are bound by law to constantly analyse transactions for any irregularities and report them to authorities where appropriate.

Shining a light on criminality

Financial crime is a massive problem. A 2018 Thomson Reuters survey of 2,373 respondents in 19 countries - including South Africa - found that the aggregate lost turnover as a result of financial crimes amounted to $1.45trn, or 3.5% of their total global turnover. In Europe, on average one in every 200 transactions reviewed by bank compliance officers lead to a criminal investigation, but only 1% of criminal proceeds generated in the EU are confiscated by authorities.

But financial privacy is not only important to criminals; it is a critical safety measure for every digital citizen. Without financial privacy, personal and financial safety can be compromised by criminals who could, for example, see the value of a purchase that someone made - as well as their personal details - and use that information to target them with criminal activities. As a business, financial privacy keeps intimate business details such as salary information, profit margins and revenue away from unwanted eyes.

Cryptocurrencies often come into the firing line for their anonymity and lack of regulatory oversight. High-profile examples of illicit purchases on the dark web using cryptocurrencies have made regulators wary of their potential for driving criminal activity.

Not all cryptocurrencies are made equal

A large part of the appeal of cryptocurrencies is that they are more discrete than mainstream payment methods. And while this is partly what makes them attractive to criminals, it is unfair to assume all discrete transactions are criminal. We all make purchases we would rather other people not know about, for fear of embarrassment or judgement. Anonymity also has its benefits: who hasn't suddenly seen a spike in advertisements related to something you once searched for online, or saw similar products to one you've just bought advertised on sites you visit?

Privacy enhancing cryptocurrencies are built on five pillars, namely:

- Unlinkability, which conceals where transactions are going to;
- Untraceability, which conceals the origins of transactions;
- Cryptgraphically valueless, which hides the value of a transaction;
- Passively hidden, which conceals the transaction from other internet users; and
- Optionality, which maximises the privacy set while still enabling you to reveal information should you need to.

But not all cryptocurrencies are created equal. And not all have the privacy of their users as a primary concern. That's why I'd add a sixth pillar to the above, namely Ideology. Since cryptocurrencies involve thousands - even millions - of people, it is critical that the cryptocurrency is managed according to a strict set of privacy-enhancing guidelines.

There's a popular argument that honest people don't need privacy since they have nothing to hide. But that's fallacy. As Edward Snowden put it, "Arguing that you don't care about the right to privacy because you have nothing to hide is no different to saying you don't care about free speech because you have nothing to say."

Financial privacy is a fundamental human right. Technology can be both the greatest inhibitor or promoter of privacy. The

responsibility rests on all of us who participate in the new world of cryptocurrencies to ensure we protect the privacy of our users.

ABOUT THE AUTHOR

Riccardo Spagni is the lead maintainer at the Monero Project