Small company, big ethics

Ralph T O'Brien discusses the practicalities of privacy in the developing world where fingerprint identification is used due to lack of formal IDs.

I don't often get to share my client's privacy management activities, as confidentiality is key, so it is an honour to talk through one of my smaller customer's challenges due to their unique situation. Small customer, big data challenges. I am now finding that you don't have to be a big organisation to hold lots of data, and I am now often finding that technology solutions in the cloud allow organisations, though small in numbers, to execute big ideas across millions of data subjects.

This customer in particular is contributing to making a difference in people's lives, in areas where privacy can sometimes be less of a concern than simple survival. Individual's rights in the developing world are often forgotten. One of the biggest problems in the developing world is identity. The World Bank estimates that over 1.1 billion people do not have formal ID, excluding them from basic services such as healthcare, education, and finance. People that aren't issued government identity documents are made very vulnerable in terms of access to basic services. It makes distributing aid and education really difficult, in terms of ensuring that the aid gets to the right places, or the right people gain access to basic services taken for granted in the western world.

Fingerprint identification

But everyone does have unique characteristics. By connecting a custom-built device and software connected to a phone, a Cambridge-based company, Simprints, is seeking help to solve some of these problems. The idea sprang from a university project and the team are young, dynamic and idealistic. Their business uses fingerprints to verify identity and partner with other organisations in the third sector space to deliver their services, by using people's biometrics to accurately link them to records, empowering NGOs, businesses, and governments to reach their most marginalized beneficiaries. As a company in the aid space, Simprints also realised that privacy and data ethics are key to ensuring the safety of these vulnerable people, and to ensure they get granted the most basic of human rights in the treatment of their information.

Alongside this comes difficult data ethics decisions. Sebastian Manhart, Chief Operating Officer of Simprints, said; "Privacy is often treated as an afterthought in international development. We believe that it has to be the starting point of any project. If we cannot safeguard the data of the individuals we are trying to serve, we shouldn't be collecting it in the first place. Our stance is simple: adhere to the highest available privacy standard – the GDPR – no matter where you operate. While this is very hard, particularly from an operational perspective, it creates invaluable privacy gains for some of the most vulnerable people on the planet. Privacy is not a nice-to-have, it is a fundamental human right."

Established in the UK, Simprints is subject to the GDPR, even if its data subjects are not in the European Economic Area. Biometric fingerprint data used for establishing identity is classed as special category data, on a large scale, and they may operate in any part of the globe, often in countries with poor human rights records or offering citizens few privacy rights. Biometric data is highly sensitive. Your fingerprint is the same when you are born and when you die. So if someone gets hold of your fingerprint and your name, your identity is compromised for life. Simprints decided never to store any raw images of fingerprints. Instead, they convert images into interoperable biometric templates – basically an anonymous long string of numbers – and then create a random 16-digit code to form a link to third party databases. This pseudo-anonymisation, coupled with encryption, ensures that the privacy of the individual is safeguarded.

Controller or processor?

The firm's own legal status raised some questions at the beginning. Traditionally their partner organisations would be considered a data controller and Simprints a data processor – as a supplier of identity services. This isn't enough for this company, however, as they were concerned with any rights the data controller may have to access the biometric data, and believe that it is in the best interest of individuals and partners alike to entrust a specialised, ethical, highly capable organisation with the safeguarding of the data, given that even many large organisations simply do not have the resources to manage the data effectively. Simprints also want to collect separate datasets for research purposes of their own to improve their products, and therefore consider themselves as much of a controller as their partner. This of course means they have to be transparent and educate the individuals using its services. But providing detailed GDPR privacy notices in the field is not something that comes easy given the conditions and urgency of aid.

In terms of their legal basis to hold the data, it would be tempting to rely on reasons such as public interest/health given the nature of the work, but an individual's choice was important to the company, and they have therefore decided on the very high standard of explicit consent. This means they must collect specific consents separately for operational use and for research, achieve separate consents to their partner organisation as a separate data controller, and offer separate ways to verify identity if they refuse. This policy makes the consents freely given and not a barrier to accessing the aid offered.

Similarly, individual rights are hard to deal with. The individual data subjects do not have access to technology and may be illiterate, so ensuring individuals their rights (such as access and erasure) is really difficult in the remote areas, such as Zambia, Bangladesh, Uganda, Kenya, Nepal, where they live, or the conditions in which they live.

In terms of security, Simprints has to educate and train their partner organisation's staff using their solution. They have to ensure the devices themselves are rugged and can operate in difficult

circumstances, and often must store data in areas where there is no signal coverage so the data has to be uploaded later. This means devices must be programmed to wipe themselves clean, and the users need to authenticate to them securely, whilst the data is uploaded and downloaded from cloud storage partners with carefully managed access to the data itself. The systems are designed so that no one in the field should gain access to the back-end data, just the functionality required.

Data sharing issues arise

The data collected then has a further value of its own. The third sector wants more and more data to achieve insights and carry out valuable services, and both academic and aid organisations around the world know that these data sets of collected biometrics will be valuable research tools. Simprints were surprised at the state of the third sector's information sharing practices and found that most organisations simply attach personal data to emails and send it out to third party volunteer researchers and students using their personal devices, without controls or care for what and how they were sending. Careful thought must therefore be taken to ensure that data can be anonymised where possible, the least amount of data sent that is required, with secure mechanisms such as data encryption for transfer and storage, and deleted when no longer required. Worse, they have found it very difficult to get other organisations in the sector to commit to the standards required to handle the data, and found them less than opaque in how they can prove they can follow equivalent high standards of information protection.

The organisation is young, but has established retention periods for this data, and put in place plans to ensure data quality, limitation and deletion of the data as appropriate.

The company wants to go above and beyond in its obligations. Despite its small size – far less that of the legal requirement to perform one (250 people) – it has completed a data inventory. They are recruiting a privacy specialist and will complete privacy impact assessments for each project, which they post publicly on their website for transparency. In addition, they have to manage the other data they use, such as for business to business contracts and their own staff data.

New projects are even more cutting edge, establishing biometric technology in schools, education and even at neo-natal level. This means parental consent will need to be documented and children's data managed with even stricter rules and safeguards.

For me as a consultant, this organisation is a fascinating case study, and so different from my larger corporate clients. The company may be small, but is managing big data, and making a big difference in the world. The GDPR presents a big overhead to an organisation of this size. Simprints demonstrates a genuine refreshing appetite for ethical behaviour and the safeguarding of its data subjects, set against environments that the law just wasn't written to handle. The situations forces me as a consultant to come up with innovative approaches in response to unique challenges. I've drunk the "Kool-Aid", and am completely in love with their outlook and ethics. I look forward to continuing to help this organisation deliver its services, and protect their stakeholders' privacy as they continue to make changes to individuals' lives into the future.

AUTHOR

Ralph T O'Brien is Principal at REINBO Consultancy.
Email: robrien@reinboconsulting.com

Italy nudges closer to implementing the GDPR

On 17 October 2017, Italy's Parliament approved a specific European Delegation Law for 2016-2017, Law no. 163/2017, delegating the Government to officially transpose the GDPR in Italy by adopting legislative decrees within six months from 21 November 2017. The current "Privacy Code" 2003 will be modified according to the provisions of the GDPR. Specifically, the legislative decrees require the Italian Government to:

1. expressly repeal the provisions of the Privacy Code incompatible with the provisions of the GDPR;
2. amend the Privacy Code as strictly necessary to implement the provisions of the GDPR not directly applicable;
3. coordinate the existing provisions regarding personal data protection with the GDPR;
4. require, where necessary, specific implementing and supplementary measures to be adopted by Italy's Data Protection Authority (the *Garante*) for the purposes of the GDPR;
5. adapt the existing criminal and administrative sanctioning system to conform with the provisions of the GDPR.

In exercising its powers conferred by the European Delegation Law, the Council of Ministers approved on 21 March 2018 a draft decree implementing the GDPR in Italy's data protection regulatory framework and amending the Privacy Code (the "Draft Decree").

In the light of evaluations carried out for the Draft Decree, it was found out that the majority of provisions set forth by the Privacy Code should be expressly repealed because they are incompatible with the provisions of the GDPR that are directly applicable in the EU Member States.

At the time of writing (5 June), the Draft Decree has not yet been definitely approved. On 22 May 2018 the *Garante* published its Opinion on the Draft Decree, in which the Authority required several amendments to be made (for example, in relation to the retention of telephone and traffic data, processing of special categories of personal data in the public sector, child's consent, etc.).

Therefore, the Draft Decree still needs to be finalised. However, the appointment of the new Government should speed up the process, expected to be ongoing until July/August 2018.

AUTHOR

Reported by Daniele Vecchi, Partner, and Anna La Mura, Associate, Gianni, Origoni, Grippo & Partners, Milan, Italy.
Emails: DVecchi@gop.it
ALamura@gop.it