Omfido – Written evidence (FDF0039)

Onfido warmly welcomes the opportunity to respond to this call for evidence.

We are leaders in AI and biometric technology used to combat fraud, and recently issued a Fraud Report that looks at the issues being considered by the Committee.[1]

Below we have offered views on areas that have particular relevance to us. We would be very happy to discuss our response further, our Fraud Report, or the broader issues raised, if that would be helpful.

Emerging biometric technologies to tackle fraud

In the coming years remote identity verification and authentication using biometric technology will become ever more widely adopted across industry verticals. The pandemic has driven the market forward and stimulated hugely increased demand for such technology as customers across multiple sectors now look to onboard users remotely.

The benefits of this technology are now being embraced by established institutions as well as early-adopters in financial services and a wide range of other sectors. In addition to facial biometrics, other forms of biometric technology such as voice, behavioural and fingerprints will also continue to emerge as powerful and trusted forms of verification.

The reason that this technology will continue to grow in scale and importance is because it offers best-in-class performance for onboarding customers, from a security privacy and user experience perspective. It enables customers from large banks and fintechs to e-scooter providers to effectively combat fraud and prevent bad actors accessing services. Many financial services customers use providers offering such technology to help meet regulatory compliance requirements such as anti-money laundering and "know your customer" obligations. Such innovations need to be encouraged and incentivized by the regulatory and policy framework for digital and tech.

The difference between verification, authentication and identification

Identity verification, i.e. enabling the confirmation that a user is who they claim to be, is a key use case for biometric technologies. Such technologies are a powerful tool in combating fraud, as they allow users to be identified quickly and accurately.

We take this opportunity to set out the need for clarity and consistency on terminology. In particular there is a clear difference between identification, verification and authentication of individuals.

The need for clear distinction between these terms is important because it may have an impact on how regulators perceive the need to apply rules that govern their use. We have seen this issue arise recently in relation to the new EU AI Act proposals. Below we briefly explain the key differences between identification, authentication and verification.

[1] https://onfido.com/resources/insights/identity-fraud-report-2022

Identification

"Biometric identification" was defined in a EU Commission White Paper in February 2020 as "when the identities of multiple persons are established with the help of biometric identifiers (fingerprints, facial image, iris, vascular patterns, etc.) at a distance, in a public space and in a continuous or ongoing manner by checking them against data stored in a database."[2]

The understanding of biometric identification was further developed in a recent study for the JURI and PETI Committees of the EU Parliament[3], which defined "biometric identification" as a:

"'one-to-many' comparison where the persons identified do not claim to have a particular identity but where that identity is otherwise established – often without the conscious cooperation of these persons or even against their will – by matching live templates with templates stored in a template database."[4]

Authentication

The White Paper rightly makes a distinction between such identification systems and "authentication". It describes the latter as "a security process that relies on the unique biological characteristics of an individual to verify they are who they say they are".[5] It also suggests that "Authentication (or verification) [..] is often referred to as one-to-one matching. It enables the comparison of two biometric templates, usually assumed to belong to the same individual. Two biometric templates are compared to determine if the person shown on the two images is the same person."[6]

Verification

A further material distinction that needs to be drawn, which is between authentication and verification. Verification means the process of confirming that an individual is who they claim to be whilst authentication refers to the process of matching an identifier to a specific stored identifier in order to grant access to a device or service.

It is very important that policymakers understand the difference between these terms, because it may have a bearing on how services are deemed to be "high risk" and therefore regulated more strictly. This is currently a live debate in the EU - and while the UK may take a different approach, we consider it is vital that policy makers understand these nuances when considering how to regulate emerging technologies.

Onfido believes it is essential that technologies are not governed exclusively by reference to inflexible definitions but instead take into account use cases, as discussed. For example, it does not make sense to apply a "high-risk" label to technology used exclusively to combat fraud, and impose strict rules on its use.

---

[2]Footnote 52, p18

[3]https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2021)696968

[4]Page 20

[5]Footnote 52, p18

[6]https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf (footnote 56, p21)

How these technologies benefit individuals and the use of their personal data

Our technology and associated services directly benefit both individuals and businesses because they are a vital tool in the fight against fraud. Never has this fight against fraud been more important, with well over £4 billion of UK taxpayers money suspected of having been lost to fraud during the pandemic.[7]

As explained above, many financial services customers use Onfido services to help comply with their regulatory obligations associated with fraud prevention, in particular anti-money laundering and know-your-customer rules. Used as part of identity verification solutions, this technology has now become a key part of the wider consumer protection framework.

Onfido processes personal data in order to provide its services, and further uses this data to test and improve its technology, in particular the algorithms it uses. This use of data is fundamental to driving improvements and innovation that improve outcomes for both our customers and wider society by increasing trust and inclusion. For example, we use the data to help mitigate bias in our algorithms. It is therefore very important that such activities linked to important public interests are explicitly recognised as lawful in the legal framework.

We also conduct vital research in this area. In particular our Center of Applied AI conducts a rolling programme of research into AI bias mitigation and optimising algorithmic performance in order to continually improve our product. This ultimately enhances outcomes for both our customers and their end users. Our research is essential to driving innovation, and in turn improving the quality of the deterrent against fraud. This drives huge societal benefits and a better level of consumer protection for customers using our product.

Key regulatory challenges to deployment of the technologies

Data re-use

For companies that do not have a direct relationship with end users there is a greater reliance on customers to give notice to and collect consent from end users. This creates barriers under existing laws where, in Onfido's case, our clients may have to describe in detail how Onfido may use data for testing and research purposes. We need to see a greater level of flexibility in the legislative framework to alleviate some of this friction whilst maintaining adequate safeguards. We consider that it should be made clearer that user consent is not the only basis on which organisations should rely and that, subject to suitable safeguards, there may be other appropriate bases.

However there is also the wider question about the extent to which a data processor can even do this, i.e. re-use the data it receives from a controller for its own purposes. The CNIL recently published a statement saying "no" unless specific conditions are met.[8]

---

[7] https://www.bbc.co.uk/news/business-59504943

[8] https://www.cnil.fr/fr/sous-traitants-la-reutilisation-de-donnees-confiees-par-un-responsable-de-traitement

These conditions, such as the processor obtaining the prior written authorization of the controller, and the data controller conducting a "compatibility test", and informing the data subjects about the uses of their data for subsequent purposes, will invariably cause a tension between controller and processor.

This presents challenges for processors such as Onfido when we seek to improve our service using the data, in particular reducing bias in our algorithms. This activity, geared as it is to increasing the protection and welfare of users, should be encouraged rather than curtailed.

Use of data for research

In relation to the use of data for research purposes, there is currently a lack of clarity and clear mandate for data processing for research purposes. This is a particular challenge for companies that are (i) dependent on another controller to collect and provide personal data; and/or (ii) reusing personal data collected for one purpose for research. For example the controller who collected the data may have relied on explicit consent for the original processing. This can limit the data available for research where the consent was too narrow and/or the transparency obligations not sufficient to enable the reuse of data.

For innovative companies such as Onfido, who provide AI driven services to corporate clients, these challenges present barriers that do not exist for bigger technology companies that can afford and have the data to build AI services in house. Such companies often have direct relationships with end users and/or control more of the user journey/technology ecosystem and therefore can avoid some of these difficulties.

The lack of appropriate provisions for research can create unease for customers and can add friction and delays to the sales process as they seek to get comfortable with the use of data for research purposes.

A clear statutory definition of research, which includes research undertaken by a commercial organisation, would help increase certainty, and we would strongly encourage this to include a specific reference to commercial research including for the purpose of identifying and/or developing new technologies, or new uses of existing technologies. Simplifying and consolidating the research-specific provisions would remove barriers to growth and innovation in the UK, and help incentivise companies like Onfido to drive product improvements that contribute to better outcomes for society.

Sector-specific barriers

While not a data protection issue, the patchwork of sector-specific rules that govern use of biometric technology for identity verification can chill deployment plans. For example at EU level the implementation of the eIDAS Regulation and AML Directive are fragmented across Member States and providers of identity verification services are effectively blocked from servicing customers on a cross-border basis unless they are recognised in each Member State they operate in. The requirements for a service provider to be recognised in each Member State differ, reducing the ability of such providers to scale. In turn, this also reduces the scalability of such technology as there are barriers to cross-border expansion. Table A provides an overview of the differing requirements in some

Member States.

Table A

Country	Video call requirements for eKYC service providers
Germany	Video call requirement with a list of security requirements[9].
Luxembourg	Video conference call required with limits on outsourcing outside of the country, and requirements including a trained employee for the calls[10].
Netherlands	No specific requirements yet

What can we do to support the delivery and implementation of these technologies in the future?

We set out below a set of specific recommendations which we consider will help stimulate the delivery of these technologies, while realising their benefits more broadly.

1. **Improve legal clarity and certainty on definitions and legal bases for data processing activities related to research**. Onfido supports the Government's proposals in Data: A New Direction for a statutory definition of scientific research, provided this explicitly includes research undertaken by commercial organisations in a commercial context and seeking to clarify the research specific provisions within the UK GDPR.
2. **Remove limitations on the re-use of data for research purposes**. By clarifying the legal bases for the (re)processing of personal data beyond consent, when thresholds are met and with suitable safeguards. In particular, any such changes should take into account the role of service providers in a B-B-C context and not just focus on controllers or B2C businesses wishing to repurpose personal data. This will better accommodate the serendipitous nature of research.
3. **Provide access to more data sets for the responsible, ethical development and training of AI systems**. We support the research provisions outlined above which will provide organisations developing AI technologies more legal clarity and flexibility when processing personal data.
4. **Consider the use case**. We believe that in determining how data can be appropriately used and shared, the use case needs to be at the heart of the consideration. The ability to use data to combat fraud, whether that be reusing the data and/or sharing data between financial service

[9] Circular 3/2017 (GW) - video identification procedures - BaFin

[10] FAQ AML/CTF and customer on-boarding/KYC methods - CSSF

providers, or between those providers and data processors supporting them, should have a clear mandate in the legislative framework. This mandate needs to apply to all legislation which impacts the use of data, such as the Privacy and Electronic Communications Regulations.

5. **Drive ever-greater coordination across regulators.** Regulatory coordination is very important, especially for smaller companies seeking to navigate the regulatory requirements. The various initiatives that impact the use of biometric technology, data and associated services need to be closely aligned, in sync with each other and not duplicating work or creating inefficiencies for industry. For example, the National Data Strategy does a good job of mapping out the overall regulatory framework and key pillars within that. Looking forward we also hope to see that the outcome of the Data: a New Direction and any associated reforms will closely align with the government's AI strategy and expected White Paper.

6. **Review guidance on AIaaS.** We understand that the ICO intends to expand existing AI-related guidance to consider "AI as a service" (AIaaS). We would hope that this work and any associated outputs are fully aligned with any reforms to avoid any unnecessary complexity and uncertainty. Separately we are also concerned that this work on AIaaS may be targeted towards organisations with outsourced arrangements on AI as opposed to those using it in-house. At first sight this would appear to be an arbitrary distinction which may have the effect of generating competitive distortions in the market. We consider that any work undertaken in relation to data and AI by DCMS and the ICO needs to be closely coordinated as a minimum and we would welcome the opportunity to discuss this further with the ICO, as well as offer any support that might be helpful.

7. **Promote consistent certification and standards.** Certifications and standards may assist with transparency and certainty in the context of AI testing and development of biometric technology services. Information technology experts should be given sufficient scope to develop these frameworks with the aim of improving accountability and transparency, and we consider such standards could act to drive further user trust and confidence in them. We would want to ensure that industry had maximum opportunity to input into any certifications or standards development work.

8. **Reform rules on automated individual decision making.** We recognise the importance of upholding individuals' rights and the strong basis of Article 22 in the 1995 Directive. Further we are conscious that we, and the UK technology sector more broadly, rely heavily on the free flow of data internationally and therefore want the UK to maintain a close alignment to the GDPR. However, given the wide-range of applications that can potentially fit within the definition of 'solely automated processing', it would strongly benefit roll-out of the technology if the scope of Article 22 were clarified and narrowed to exclude AI systems which are subject to appropriate human oversight / other safeguards, even where individual decisions are not necessarily always subject to human review. Further We consider that there is merit in considering reform of Article 22, in particular deleting Article

22 paragraph (4) which prevents automated decisions in relation to special categories of data. We have further evidence to support our reasoning on this point that we are happy to share if it would be helpful.

9. **Remove consent requirement for specific use cases.** Subject to strict safeguards to protect against misuse, removing the requirement for consent when biometric technology is used in specific use cases focused on consumer protection and combating fraud would be extremely helpful to businesses. For example, when the technology is used in authentication and fraud detection, removal of the need for consent would facilitate greater use of the technology, leading to enhanced levels of consumer protection. Other forms of biometric technology such as device fingerprinting are used as a passive authentication method and to detect fraud for a wide range of digital services. Such technologies access information from a device, however to require consent for this collection would introduce friction for the user and defeat one of the purposes of this type of technology. Such activities may be reasonably expected by legitimate users of digital services and should be distinguished from advertising and other use cases involving tracking technologies, which are often seen as invasive, unfair and not sufficiently transparent. Any residual risks mitigated through transparency obligations. Sectoral codes and regulatory guidance could be helpful here in prescribing the safeguards necessary to enable limited use cases of device fingerprinting and similar technologies without users' consent.

About Onfido

Onfido is a UK-headquartered global identity verification provider. We partner with organisations across the world to remotely onboard users securely and swiftly, providing a best-in-class user experience. Our leading biometric and AI technology, coupled with human-in-the-loop oversight, enables clients to prove that their customers are who they claim to be.

Started ten years ago, we have scaled rapidly and now employ over 250 people in the UK and more than 600 in total worldwide, with offices across Europe, the US, Singapore and India. We are continuing to invest and grow our team and global presence to meet increasing customer demand in both the fintech space and other verticals.

We are thought leaders in AI bias, ethics, fraud, security and privacy. We were winners of the 2020 CogX Award for "Best Innovation in Algorithmic Bias Mitigation" and "Outstanding Leader in Accessibility" and were "Highly Commended" in the SC Europe Awards 2020 for "Best Use of Machine Learning". We work with Interpol to develop leading practice in fraud prevention and publish a widely-acclaimed annual Fraud Report considering the state of the market. Onfido is a founding member of the Better Identity Coalition in the US and a board member of the FIDO alliance that is dedicated to best-in-class global authentication standards.

22 April 2022