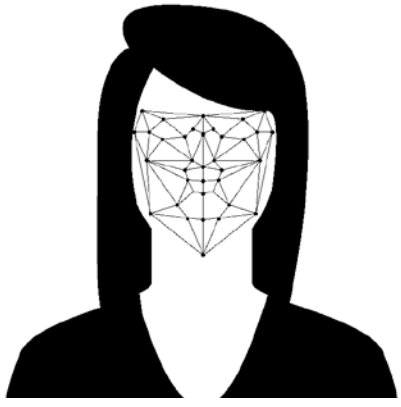
Should (your) identity documents use biometrics?

Responsible biometrics
series
April 2018



Eticas R&C
This document is based on project work conducted by Gemma Galdón Clavell, José María Zavala and Mariano Martín Zamorano.
Editors: Carlos Delclós and Mariano M. Zamorano.
Author: Simone Casiraghi.

Should your ID use biometrics?

Introduction

In recent years, efforts have been made to make the identity documents used to cross international borders more secure and accurate. As a result, today's e-passports contain several physical and digital security features that make them very difficult to counterfeit.

This is not the case for so-called breeder documents. These are documents that can serve as a basis to obtain other legal or legitimate identification documents, such as national identification cards, passports or driver's licenses, which in turn should serve to guarantee the most basic human rights of their holder. The best-known example of a breeder document is a birth certificate.

Despite the crucial role they play, breeder documents are easy targets for fraud and identity theft. They are easy to copy and the requirements for their creation and verification are not always clear or harmonised across international borders. As a result, breeder documents are often referred to as the weakest link in the so-called "identity chain" that starts with the registration of one's birth and ends with the registration of one's death.

To address these problems, in 2016 the European ORIGINS project studied the security of passport breeder documents with the aim of identifying possible solutions to develop more reliable breeder documents. The motivation behind the project was that the securitisation of breeder documents would have positive effects on the level of security throughout the identity chain, including the issuance of e-passports.

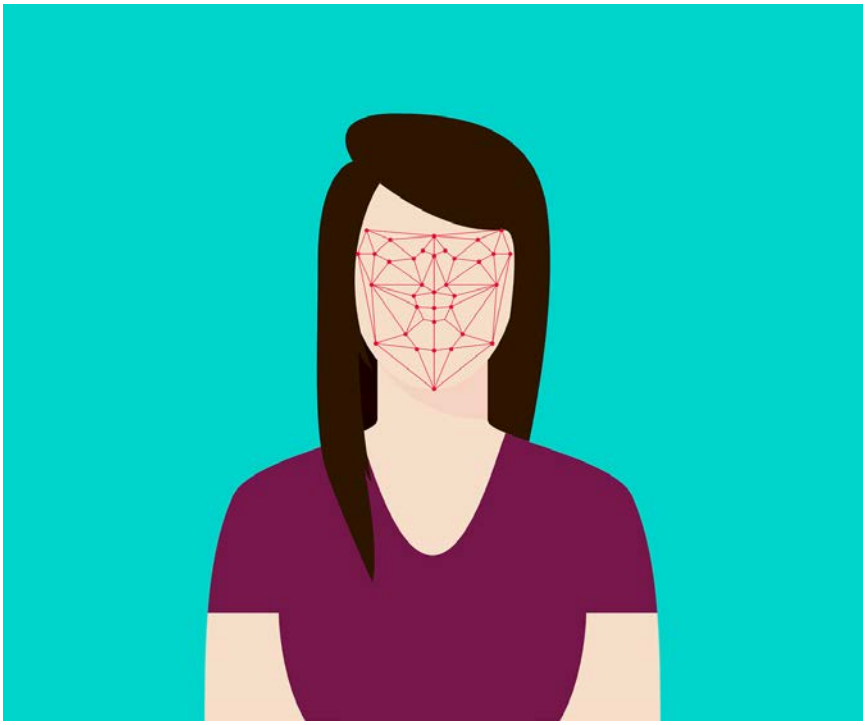
In keeping with this logic, biometric technologies were proposed as a means through which to increase security and prevent cases of identity theft. Biometric identification systems such as fingerprints, iris scans, facial recognition or even DNA are generally believed to improve the accuracy, convenience and reliability of identification documents. But from a social, legal and ethical standpoint, the use of biometrics technologies is very problematic, with important implications for fundamental rights, particularly the right to privacy and the protection of personal information.

As the ethical and legal partner of the ORIGINS project's consortium, Eticas Research and Consulting pointed out these issues and highlighted strategies and measures to respond to them. This report presents some of the project's main findings and recommendations

with the hope of informing a broader public debate on the social, legal and ethical implications of the use of breeder documents and biometrics in identity management.

Identity, identification and biometrics

The terms “identity” and “identification” are often interpreted as synonyms. Yet these concepts should be distinguished, particularly in the field of biometrics and identity management. Understanding the difference between the two clarifies why using biometrics for identity management can have dramatic ethical and social consequences.



The primary distinction between these concepts is that, while the concept of identity has a changing and dynamic character, official identification is static or “fixed”. Since the 1970s, a diverse range of sociological, psychological and philosophical theories of identity have emerged, abandoning the primordialist tradition that defined it as a fixed and biologically given feature and explaining the ways in which identity is socially constructed (Cote and Levine, 2002). Though theoretical debates about the tension between structure and agency persist, it is broadly accepted across disciplines that, while an individual’s

identity is shaped through individual relationships, it is also shaped by diverse contextual factors that include cultural and societal conditions, and material or symbolic constraints (Gecas et al. 1995; Bourdieu, 1991).

Modern states base their official forms of identification and categorisation on these changing collective or individual identities. In some cases, this more dynamic understanding of identity and the recognition of cultural diversity are gradually being translated into law. For instance, many countries allow transgender people to modify their identity documents to accurately reflect their name, gender identity and gender expression (Johnson, 2015). Another example of how identity and identification are affected by societal change is found in nations such as Estonia, Latvia, or Slovakia, which achieved independence relatively recently, spurring a shift in perceptions of national identity.

Thus, a general distinction must be made between the way an individual identifies him or herself and the way in which this identity is socially categorised and identified by official institutions. This is particularly relevant in the application of biometrics to breeder documents, since the human traits linked to a particular identity at birth can limit the public recognition of identity change in the future.

Proponents of biometrics argue that new technologies avoid the dichotomy between individual and collective identity by identifying the body itself, stabilising identity or providing a more "objective" and "neutral" form of it. In this way, the use of biometrics for identification seeks to shift the question of identity from the domain of narrative (a person's life story) to the domain of templates (digital samples of one's biological data) in order to define who someone is (Ajana, 2013: 96).

But even if the use of biometrics makes official forms of identification more accurate, it cannot truly reflect a person's identity. It can, however, blur the line between the two when combined with information linked to the social processes that shape identity. Consider, for instance, the implications of combining biometric identifiers with practices of profiling and social sorting, which often impute certain behaviours for specific social

categories in order to adapt public services or improve state functioning (Aspinall and Chinouya, 2011: 257).

So while basing the process of identification on biometrics may make an official document more reliable, it does not actually reflect a person's identity, practices and interests. And by eliminating the influence of one's sense of belonging and distinguishing only between "qualified" and disqualified" bodies, biometric identification can be thought of as a form of "dis-identifying" or depoliticising identity (Muller 2004).

> ***"While basing the process of identification on biometrics may make an official document more reliable, it does not actually reflect a person's identity, practices and interests."***

As its contribution to the ORIGINS project, Eticas Research and Consulting developed a theoretical framework through which to analyse the ethical implications of using biometrics in breeder documents. ER&C also examined the potential societal impact of such a measure. To do so, a two-pronged methodological strategy was deployed. On the one hand, a review of existing projects and scientific literature dealing with privacy issues in biometrics was conducted. On the other hand, Eticas carried out 17 in-depth and semi-structured interviews with experts in biometrics, identity issues, ethics, law, fundamental rights, privacy and data protection. The respondents were from 10 different countries, and all were interviewed via online conference.

Interview findings

Like the previous projects on the topics of biometrics and privacy (see annex) , ER&C's contribution to ORIGINS focused primarily on policy, governance and the protection of privacy and other human rights. What it added to recent debates, however, was a narrower focus on a weak link in the identity chain, namely the lack of security in the issuance of breeder documents. As the research shows, the use of technology to 'fix' this problem can bring about important privacy and data protection problems.

Experts warned about the general lack of distinction between identity and identification, which in turn creates confusion among stakeholders and the general public. As one respondent pointed out:

> ***"You have an identity whether or not you have an ID document. This is often misunderstood by the bureaucrats. Identity is something internal. Telling someone that they don't not have one is an insult, on a psychological level. It is not an 'identity' card, it is an "identification" card. A reference to your identity, not your identity itself".***

There is also a legal dimension to identification which must reflect the changing character of identity. Being a legally identifiable person provides individuals with the capacity to exercise their rights and obligations. This means that, in addition to being a requirement for accessing other fundamental rights through citizenship, identification is also a fundamental right in itself.

However, experts also highlighted that being identifiable can have many negative implications. Once one is identifiable, they can suffer discrimination and persecution. For instance, centralised systems of identification can be misused, and the loss of anonymity and traceability can lead to privacy risks. Moreover, identification can exclude certain people who cannot demonstrate certain credentials from exercising universal rights.

As many respondents noted, this is particularly egregious when it comes biometric identification systems for breeder documents. All of the experts interviewed expressed doubts and concerns about the necessity of introducing biometrics in order to secure breeder documents. These concerns dealt with four aspects:

- Governance
- Individual rights and freedoms
- Breeder document models
- Societal impact

Governance

Respondents highlighted several political and administrative areas in which the application of biometrics to breeder documents would entail a number of problems and risks. First, the consensus view among all the experts interviewed was that the proportionality of and need for such a measure were highly dubious and very concerning. More specifically, respondents pointed out that the creation of new biometric databases, coupled with their centralisation by governments, would greatly threaten the privacy and individual rights of citizens. One expert pointed to the example of South Korea, where an entire database of government-issued identity documents was hacked in 2014[1].

[1] https://www.theregister.co.uk/2014/10/14/south_korea_national_identity_system_hacked/

Moreover, centralised databases could also lead to potential misuses of personal data by governmental and private actors, including commercial exploitation. This risk, taken with the measures that could be taken to store and collect data in the most secure manner, evoked a dystopian scenario involving the proliferation of authoritarian police states. Avoiding such an outcome would require highly complex forms of governance and tremendous efforts to develop intergovernmental coordination. In the Europe Union, harmonisation between all of the information systems used by Member States for the purposes of identification would be required, while still guaranteeing their autonomy and an acceptable degree of flexibility.

Individual rights and freedoms

The highly sensitive character of biometric information and the invasiveness involved in collecting data from newborn babies were repeatedly pointed out by respondents. Particular concern was expressed regarding the lack of choice or consent from newborns in processing their data. This is also the case for minors, for instance, when

they are asked to provide fingerprints in schools. This happened in the UK, where thousands of pupils were fingerprinted without the consent of their parents[2].

Respondents also claimed that using biometrics could also entail dynamics of systematic exclusion or inclusion among people who cannot provide certain biometrics. Examples include people with specific forms of blindness, who would be ineligible for iris scans, or elderly people, newborns and manual workers, whose fingerprints may be difficult to read or collect. Similarly, while ears are generally believed to provide reliable biometrics parameters, they do not work equally well for all groups, as is the case among some athletes (e.g. boxers, rugby players) or people who have suffered serious injuries.

Breeder document models

In addition to the social, legal and ethical concerns described above, the effectiveness of using biometrics to secure breeder documents was also discussed in technical and logistical terms[3]. Several respondents noted how the aging of a data subject negatively affects the reliability of biometrics such as fingerprints or facial recognition. Collecting biometrics from children at a very young stage simply increases the possibility of false positives or negatives for the next several years.

Moreover, the types of biometrics which could be used were considered alongside their levels of invasiveness. Here, there was a consensus among the experts that DNA is the only form of biometric data that could be considered reliable, since it remains static and does not change over time. However, using DNA simply introduced more serious problems of invasiveness as well as tremendous societal impacts, further described in the following section.

Additionally, respondents expressed serious concerns regarding the controversial points of a future research agenda on biometrics and breeder documents. First, they

[2] https://www.independent.co.uk/news/education/education-news/privacy-concerns-raised-as-more-than-one-million-pupils-are-fingerprinted-in-schools-9034897.html

[3] For further information please check Deliverable XXX

mentioned the issue of collecting biometrics from newborns. Of the seventeen experts interviewed, fourteen were against this initiative on the grounds that it was intrusive, unnecessary and risky. They also considered it unreliable for reasons described above. Second, the idea of collecting biometrics and adding it to a centralized government database was opposed by 12 of the respondents, who considered this an inappropriate use of biometric data with a high risk of "function creep", i.e. expanding the use of this sensitive data to purposes beyond the original motivation behind its collection.

Societal impact

Serious concerns were expressed by a number of respondents regarding the social acceptability of using biometric technology for breeder documents. One expert pointed to the example of the Netherlands, where the inclusion of biometric passports was rejected by a number of civil rights groups, who depicted them as a violation of Human Rights[4].

Another social risk described by respondents was that of social sorting, a concept popularised by the sociologist David Lyon which describes the application of surveillance technology to the categorisation of individuals based on observable, distinguishable features, facilitating practices of discrimination (Lyon 2003). Today, social sorting is overwhelmingly carried out through the use of data, relying on technologies of identification and authentication to extract and compare personal information and biometric data.

To better illustrate the societal risks associated with using biometric data to secure breeder documents, let us return to the example of DNA (which, as mentioned earlier, is ultimately the only reliable biometric parameter applicable to newborns). Even if DNA could be collected in a non-invasive way, it includes far more information than is required for the purposes of 'identification'. As a result, this information could be used against someone for a broad range of purposes other than the ones for which the data was collected, including as a health predictor. This information could be exploited by a wide

[4] https://www.rnw.org/archive/dutch-biometric-passports-cause-controversy

range of actors, including pharmaceutical companies and insurance providers, in ways that dramatically affect one's most basic human rights.

Conclusions

As shown throughout this report, the vast majority of the experts interviewed questioned the need, proportionality, feasibility and desirability of using biometrics to secure breeder documents. The efficiency of such a measure was questioned and several warnings were made regarding its potential impact on human rights.

In keeping with the relevant scientific literature, serious reservations were expressed regarding the ability of current biometric technologies to correctly identify individuals by using babies' fingerprints, facial or iris images. Both the quality of the data and the capacity of algorithms to "predict" changes in these identifiers were identified as sources of problems.

Moreover, the negative societal impacts of using biometrics to secure breeder documents were emphasised. Much of this problematic was centred on the relationship between identity and identification. The progressive intervention of the State and private companies in identity management, together with the introduction of biometric technology, was viewed as a new way of assessing and identifying both valid and non-valid individuals "through mechanisms of digital profiling" (Ajana, 2013:12).

With the goal of helping policymakers and tech developers tackle the problems identified in the abovementioned analysis, ER&C compiled some recommendations drawn from its own analysis and suggestions made by the experts interviewed during the course of the ORIGINS project. The first set of recommendations was based on a model of the data life cycle of breeder documents. The idea at the time was that each stage should be compliant with the data protection principles proposed by the OECD (though this must now be extended to the European Union's General Data Protection Regulation):

1) Data collection or mining. Data collection must be minimised in this stage. From the perspective of the collector, it is important to know who is going to collect the data, how much and what type of information is collected (data relevance), and what the data collection procedure entails. From the perspective of the data subject, informed

consent must be provided and the invasiveness of data collection must be properly understood.

2) Data storage. This phase covers the time frame between data collection and deletion. To prevent ethical and social concerns, during storage, data must be analysed and/or shared in a specific location, such as a centralised server or a local authority or database. As in the previous stage, principles of transparency and data minimisation (i.e., avoiding collecting data in the first place instead of struggling to make it more secure) must be observed.

3) Data analysis. When their data are analysed, data subjects must know precisely what their data are being used for. To comply with data protection regulations and avoid threatening privacy, any and all analyses must be performed using anonymised datasets.

4) Data sharing. There are four different scenarios of data sharing. These include: (a) sharing within the same Member State or within the EU, which is fairly low-risk given the existing similarities between legal frameworks and the implementation of GDPR; b) sharing with states outside the EU, which is a fairly risky practice due to differences between states in terms of their legal frameworks; c) sharing with private entities, which is also considered high-risk because they may involve interaction with new or unexpected infrastructures (i.e., not entitled or qualified to handle a given type of data), making it strongly advisable to pose strict limitations on their access to centralized data; and d) sharing under emergency protocols, which must be well defined and categorised in order to prevent the misuse of data.

5) Data deletion. This is the closing stage of the data lifecycle, when personal or sensitive data should be destroyed once the goal has been achieved or discarded. To accomplish this, secure deletion mechanisms are required to guarantee that biometrics samples are effectively destroyed.

Besides the data life cycle, several other recommendations were made for how to secure breeder without introducing biometric data. First, a clear need to harmonise the issuance of breeder documents and identity management systems beyond each state's specific forms was identified. Moreover, greater attention must be paid to the security concerns and storage policy affecting existing data from breeder documents.

As with any decision to include biometric data, the need and proportionality of such a measure must be thoroughly considered, as well as its social desirability. The social acceptance of such a policy should be measured from the perspective of the data subjects themselves, with particular emphasis on transparency, awareness, knowledge and informed choice issues. The potential impact of including biometrics in breeder documents should particularly be evaluated for vulnerable populations such as refugees, displaced people and the poor.

Finally, in addition to complying with existing legal frameworks for data protection, the role of ethics in the implementation of data-intensive technologies must be considered. Technology makers and engineers in particularly must understand the relevant ethical and social frameworks and be aware of their own biases with respect to these.

References

Ajana, B. (2013). *Governing Through Biometrics: the Biopolitics of Identity.* Palgrave Macmillan, UK.

Aspinall, P. J., Chinouya, M. (2011). Determining the Identity of Black Africans in UK Population and Health Policy Contexts: Ethical Issues and Challenges. *Journal for the Study of Race, Nation and Culture, 17*(2), 255-270.

Bourdieu, P. (1991). *Language and symbolic power*. Harvard University Press, Cambridge.

Cote, J. E.; Levine, C. (2002). *Identity Formation, Agency, and Culture*. Lawrence Erlbaum Associates, New Jersey.

Gecas, V.; Burke, P. J.: Self and identity, in Cook, K. S. (1995). Fine, G. A.; House, J. S. (Eds): *Sociological perspectives on social psychology*. Allyn & Bacon, Boston, 41-67.

Johnson, J. (2015) Minnesota (Trans)Gender Markers: State Statutes and Policies on Amending Identity Documents. *William Mitchell Law Review*, Vol. 41.

Muller, B. J. (2004). (Dis)qualified bodies: securitization, citizenship and 'identity management'. *Citizenship Studies, 8*(3), 279-294.

Lyon, D. (2003). *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*,

London: Routledge.

Eticas R&C (2016). *Deliverable 7.1: Report on Privacy and Data Protection Framework for Technology Solutions in Breeder Documents Issuance* (1-65). Origins project.

Eticas R&C (2016). *Deliverable 7.4: International Survey on the Ethical and Fundamental Rights Aspects of Breeder Documents* (1-47). Origins project.

Annex: European projects on biometric identification

1) PRACTIS (Privacy - Appraising Challenges to Technologies and Ethics) is an EU FP7-supported project under the framework of the FP7 Science in Society (SiS) program, lead by the Interdisciplinary Center for Technological Analysis and Forecasting in Israel. This initiative aimed at coping with "the future of privacy in Europe due to emerging technologies that might cause potential threats to privacy and to find ways to cope with these threats (mainly legal and ethical) to reduce their impact". PRACTIS embraces a wide range of technologies and societal developments, identifying both privacy threats and privacy enhancing aspects in the long term, as well as changes in privacy perceptions. These privacy impacts relating to emerging technologies had been conducted in several fields such as Nanotechnology, Biotechnology, Robotics and Information Technology. Among the technologies analysed there was activity-related biometrics. The mission of this project was to "increase readiness and awareness to the impact of emerging technologies on privacy issues among citizens, policy makers and stakeholders". Through its activities, this project contributed to the improvement of privacy protection and data security as an effective policy tool in Europe.
2) ETHICAL ("Promoting International Debate on Ethical Implications of Data collection, use and retention for Biometric and Medical Applications") is a FP7-funded project (2009-2010) that aims at enhancing the debate on the ethical implications of data collection, use and retention in medical and biometric applications. This debate should help to create a consensus and a roadmap towards a secure environment while respecting the human rights.

   The resulting conclusions should help to spread the technological breakthrough concepts to a wider public and to cope with societal challenges in data privacy and protection in collaboration with EC Committees, media, non-governmental organizations and companies.

   The empirical ground for the report was based on real cases of data misuse as well as their legal consequences. To augment the sources needed for analysis structured research literature was added and feedback and opinions on relevant ethical implications from a sample of targeted future beneficiaries of the conducted research were also collected.
3) The FP7 project HIDE (Homeland Security, Biometric Identification & Personal Detection Ethics) states that its aim is to "set up a platform devoted to ethical and privacy issues of

biometrics and personal detection technologies which addresses transnational (European) and international problems".
This project (2008-2011) departed from the premise that personal detection technologies focus specifically on identifiable individuals, and biometrics is the "application of technologies that make use of a measurable, physical characteristic or personal behavioural trait in recognizing the identity, or verifying the claimed identity of a previously registered individual".The HIDE project proposes a "conversation" between technology, security, ethics and policy experts and encourages public discussions and dialogue. In order to achieve these goals, various research and communication mechanisms and tools were deployed, like focus groups, policy forums and problem solving workshops.

4) PRESCIENT ("Privacy and Emerging Sciences and Technologies") is a FP7-programme that took place from 2010 to 2012. It aims at identifying and assessing privacy issues posed by emerging sciences and technologies and contributing to the development of new instruments for the governance of science and technology through EC policy. It also contributed to the quality of research in the field of ethics, by distinguishing between privacy and data protection and analysing the ethical, legal and socio-economic conceptualizations of each. The main field of research is second-generation biometrics (as opposed to traditional ones, like fingerprinting) and their impact on privacy and human dignity.
5) Project PACT (Public perception of security and privacy: Assessing knowledge, Collecting evidence, Translating research into action) is an FP7-supported project developed between February of 2012 and January of 2015. This project performed an assessment of the existing knowledge of the relation between security and privacy and the role played by trust and concern. After collecting evidence through a pan-European survey on this matter regarding fundamental rights, a Privacy Reference Framework for Security Technologies was proposed.