Memory in Motion

Published by Amsterdam University Press

Memory in Motion: Archives, Technology, and the Social.
Amsterdam University Press, 2016.
Project MUSE. muse.jhu.edu/book/66527.

For additional information about this book
https://muse.jhu.edu/book/66527
Chapter Ten

The Archival Promise of the Biometric Passport

*Liv Hausken*

Throughout its history, the international passport has been an archival practice. As Mark Salter underscores in *Rights of Passage: The Passport in International Relations* (2003), the passport as well as other ID documents have always been a feature of the activity of matching a person to a number through which the particulars of that person can be traced in other records.¹ As Craig Robertson explains, regarding the USA: ‘In the 1920s the increased administrative reach of the federal government produced a documentary regime of verification in which documents begat documents to produce official identities verified through the archival memory of the state.’² Admittedly, this confidence in the archive contrasts with earlier practices. Even in countries where one had both international passports and checks at the national borders, passport inspectors did not always believe that it was necessary to check the passport and did not always have confidence in this document.³ Robertson illustrates the latter case with an example from the US borders before the First World War. At that time, immigrants were not required to carry identification documents, even if the federal government had taken control of the administration of the US borders in the late 1870s. Until the outbreak of the First World War, such documents were not thought to provide an accurate determination of an individual’s identity. Robertson refers to the documents issued to Chinese immigrants who were exempt from the Chinese Exclusion Act, which the immigration officials apparently ignored. The officials trusted their own ability to verify on the basis of physical appearance the identity of Chinese as merchants and students rather than the distant authority of Chinese government officials and U.S. diplomatic agents distilled in what they considered a questionable document.⁴ According to Robertson,

It was only during and after the World War I that an increased official perception of the value of identification documents led to sufficient enforcement of documentary evidence in the issuance of passports and visas for the U.S. officials then to trust them to provide a useful form of individual verification at the border – that is, to perform the specific role of allowing ‘the state’ to remember people who crossed the border at official points of entry.⁵
The foundation of the League of Nations and the organization of the first Conference on Passports in Paris in 1920 confirm that this history of the US passport is part of a general shift in the direction of more committed international agreements and regulations of human mobility. This entails objectifying the passport as an archival practice.

Passport guidelines and a general booklet design emerged from the 1920 Paris conference. As the booklet design was developed and implemented during the 1920s and 30s, one may in some sense also consider the passport booklet itself a small archive. It is not just a travel document like the safe conduct pass of earlier centuries, which was a letter including the name of the traveller and the purpose of his mission asking that the bearer not be hindered in his journey. Nor is it just a standardized travel document issued by the state and part of a network of archives certifying that the document of the passport is identical to other documents. The booklet is also a place for the storage of documents and records, a means and method of inscribing, storing, and transmitting information. In addition to the information on the cover page and the identity page that is entered when the passport is issued, there are passport pages reserved for visas coming from different embassies or consulates. These pages also include stamps from passport control officers of both the holder’s home country and countries visited, revealing the history of entering and exiting those countries. In some countries, there are also pages for amendments where the issuing country may place travel restrictions, modify conditions for travel abroad, or change the period of validity. The passport not only allows the state to remember people who crossed the border at official points of entry, as Robertson reminds us; the passport booklet is also an archive producing and recording events for the traveller.

Today’s passport booklet is in many ways still a small archive. Yet, since more and more regions of the world are opting for passport-free border crossings, one may experience travelling through many countries without having one’s passport marked with the stamps or visas. This means that the externalized memory of traveling is now full of holes and missing tracks. What is more, in the contemporary ePassport, the inscriptions of data on a microchip are also subject to archival restrictions. Such registration can only be done at the time of the issuing of the passport. To prevent the data on the chip from being overwritten, a public key infrastructure (PKI) scheme has been implemented to assure the reader of the chip that the original data of the authorized issuer have not been altered in any way. As Wolfgang Ernst points out, ‘It is worth remembering that the archive as the condition for our knowledge of history becomes dependent on the media
of its transmission." If we consider the electronic microchip as a medium, it is a medium that enables read-only access. In a certain sense, we may therefore say that the booklet as such (including the chip) is less an archive today than it used to be in its pre-electronic era. However, as an electronic document, today’s passport is inscribed in larger and far more complex and mutable archival networks.

This text will investigate the biometric passport as an archival practice. Drawing on conceptions of the archive as an epistemological project (Foucault 1991, 2010), as technology and medial logic (Ernst 2013), as well as a practice (de Certeau 1984), I will show how the introduction of the biometric passport has transformed the passport not only as a tool and technique for regulating mobility but also as a techno-political model of the world. My argument is informed by recent studies of the history of paperwork technologies, like Cornelia Vismann’s work on the law and its mutual relationship with the technology of files and Lisa Gitelman’s investigation of the document as object of inquiry and epistemic practice. Previous studies of the history of passports and other ID documents have, of course, also been very helpful. Most of these historical accounts focus primarily on the development of the modern state and often end their stories around 1920, which is exactly when the international community recognized the passport as a record for the regulation of identity and mobility. Very little is written about more recent passport history, Mark B. Salter being a notable exception. Even less has been published about the current biometric passport and its technology and materiality, which is the topic of this chapter. By comparing a variety of pre-electronic passports, I will investigate transformations in the archival conditions of today’s biometric passport in order to show the way in which it produces a specific conception of individual identity as well as a special condition of social vulnerability. But first, a brief outline of what a biometric passport actually is.

What is a biometric passport?

In 2005 the International Civil Aviation Organization (ICAO) approved a new standard for international passports, now commonly known as biometric passports or ePassports. A biometric passport is a machine-readable passport (MRP) containing biometric information on a contactless integrated circuit chip. The United Nations agency ICAO presents their specifications for machine-readable passports in a document called Doc 9303 Part 1. In its sixth edition in 2006, this document is divided into two
volumes, the first dealing with passports with machine-readable data stored in optical character recognition format (MRPs), the other volume giving specifications for electronically enabled passports with biometric identification capability (ePassports). The machine-readable passport was launched in 1980 and its specifications published as the first edition of Doc 9303, titled *A Passport with Machine Readable Capability*. The sixth edition of Doc 9303, Part 1, is the first that also indicates regulations of biometric information to be stored on an electronic chip. The machine-readable data refers to two strings of alphanumeric characters printed at the bottom of the identity page. It is formatted in such a way as to be readable by machines worldwide. It is considered a different representation of the data found in the visual inspection zone (VIZ) of the identity page, as it provides verification of the information in the VIZ—data not specifically intended to be read by a machine but by human beings. The two strings of machine-readable data, however, do not duplicate the information offered by the photograph also present on the identity page of the passport. The photographic information was singular and displayed in one format only until the introduction of the biometric passport.

The chip contains all the data from the MRP identity page, a biometric measure of the passport holder, and a security object to protect the data with Public Key Infrastructure (PKI) cryptographic technology and which conforms to the specifications of Doc 9303. The ICAO recommends facial recognition as the primary biometric, mandatory for global interoperability in passport inspection systems, while the finger and iris are recommended as secondary biometrics to be used at the discretion of the passport-issuing state. The biometric measure of the passport holder is, in other words, a measure of the face and sometimes also contains fingerprints or iris scans. The biometric capture of the face is an integral part of passport photography, which explains why one can no longer use one's own photographs when applying for a new passport. The specifications require that biometric data be stored in the form of high-resolution images on a high-capacity contactless integrated circuit (IC), the IC also being encoded with a duplicate of the MRZ data. Since the data in the machine-readable zone (MRZ) already duplicates the information in the visual inspection zone, the biometric passport provides yet another place and format for the registration of information; notably the microchip.

The machine-readable passport represents a shift from human to machine in the verification of the traveler's identity. The biometric passport presents the chip as its primary source of information. The passport inspectors do
not even have to open the booklet to verify its identity. The microchip is coupled to an aerial (antenna), which allows data to be communicated between the chip and an encoding/reading device without the need for a direct electrical connection.21

Why biometrics?

What is the reasoning behind the introduction of biometric passports? According to the ICAO’s Doc 9303, the biometric passport is a crucial measure for allowing authorities to connect identification papers to the physical singularities of actual human bodies:

11.1. It has long been recognized that names and honour are not sufficient to guarantee that the holder of an identity document (MRP) assigned to that person by the issuing State is guaranteed to be the person purporting at a receiving State to be the same person to whom the document was issued.

11.2 The only method of relating the person irrevocably to his travel document is to have a physiological characteristic of that person associated with the travel document in a tamper-proof manner. This physiological characteristic is a biometric.22

Between these two paragraphs, we find the history of the international passport as we know it. The first paragraph is an understatement, since the guaranteed identity between person and document has been internationally recognized as a challenge for more than hundred years. The latter, however, appears as a deliberate misrepresentation, presenting the latest solution to the challenge identified in paragraph 11.1 as if it was simply not the last in the line of attempts at solutions but the first and only. Biometrics is here considered a ‘physiological characteristic’ relating the person ‘irrevocably’ to his travel document; the ‘only method’ of doing this is to have a physiological characteristic of that person associated with the travel document in ‘a tamper-proof manner’. The entire paragraph comes across as peculiarly insistent, almost like an incantation. After a century of effort to produce the foolproof passport, one is now determined to finally make it.

In 1920, the League of Nations organized the Paris Conference on Passports & Customs Formalities and Through Tickets. The League of Nations was a predecessor of the United Nations,23 an intergovernmental organization
founded the very same year as a result of the Paris Peace Conference that ended the First World War. The Passport Conference of 1920 was the first League Council Session, and it was at this conference that, for the first time, a set of standards for all passports issued by members of the League was agreed upon.

For many years there had been great variations both in terms of the physiological characteristics to be included in the passport and whether or not the passport should also contain a photograph of its holder. In 1914, the US Secretary of State introduced the requirement that all new passports issued should include a photographic portrait.24 The British passport required a physiological description of the passport holder in 1915.25 Although there have been a wide variety of requirements and practices also after 1920, it is from this point onward that we can speak of a transnational history of the international passport. In many ways, this history revolves around the question of how one can relate ‘the person irrevocably to his travel document’.

Biometrics essentially refers to metrics related to human characteristics and traits, as seen, for instance, in fetal biometry, where antenatal ultrasound measurements are used to assess the growth and well-being of a foetus. Yet, the concept tends to be used more specifically to refer to technologies that measure and analyze human body characteristics for identification purposes (authentication, verification).26 Within this operating range, some consider biometrics an appropriate term for ‘automated biometrics’ only, which is often dated back to the 1960s and related to the computer-assisted registration, storage, and distribution of biometric data.27

The physiological information of the passport holder in the 1920s is a biometric as well in the sense that it measures human body characteristics for identification purposes (authentication, verification). This is in keeping with the definition of biometrics in Doc 9303, although the term is not used in this general meaning in this document. In a list of definitions and terms, biometrics is explained as a ‘measurable, physical characteristic or personal behavioural trait used to recognize the identity, or verify the claimed identity, of an enrollee’.28 With this definition in mind, one could say that biometrics has been part of the international passport for about one hundred years.

In his entertaining and idiosyncratic book *The Passport. The history of man’s most travelled document* (2003), Martin Lloyd refers to a variety of different practices of relating physiological characteristics of a person to his travel document, one of them being the passport of the Kingdom of Belgium,
which in 1920 required a list detailing hair, eyebrows, eyes, forehead, nose, mouth, chin, face, beard, and height – in addition to a photograph. Many of us remember our passports from earlier decades or that of our parents or grandparents. The Swedish filmmaker Ingmar Bergman opens the short film *Karins Ansikte* (Karin’s Face, 1986) with an image of the photograph in his mother’s last passport before letting the camera slowly slide down the passport identity page and showing the data that the Swedish authorities at that time (1964) deemed relevant in order to identify Karin Bergman as a person with permission to leave and enter the country: profession (in her case, her marital status), date of birth, place of birth, residence, height (without shoes), colour of hair, colour of eyes. Compared with the biometrics Lloyd refers to in the Belgium passport of 1920, the amount of information is markedly limited. Compared with a more contemporary Belgium passport, we see the same tendency; Jean Chevremont’s Belgian passport from 1968 lists profession, place and date of birth, face (shape), eyes (colour), height, and ‘special peculiarities’ in addition to name, nationality, signature, and a photograph of the passport holder. The biometric passport that the ICAO launched in 2006 further reduces the amount of information. At this point, the only mandatory biometrics is the face.

To be more precise, the face is the only mandatory biometric requirement described as just this in Doc 9303. It states quite explicitly that ‘Doc 9303 considers only three types of biometric identification systems’: facial recognition (which is mandatory), fingerprint recognition, and iris recognition (the latter two are optional). These are the biometrics to be stored on the microchip. However, if we apply the more general definition of biometrics from Doc 9303, there is more biometric information in today’s passport than the biometric measures stored on the chip. More importantly, with the biometric passport, biometrics has been given a new status and also some radically new archival premises.

### From eye-readable to machine-readable biometric inscriptions

If we first compare the current requirements for mandatory categories on the identity page of the machine-readable passport (MRP) with those of the pre-electronic passports, three or four additional biometric features are significant: date of birth, sex, signature, and, in a sense, also photographic portrait. These are all mandatory for MRPs as well as for ePassports, and they are in line with the abovementioned generic definition of biometrics in Doc 9303.
Date of birth is usually not considered biometric information. However, as an indicator of age, it provides some information about the individual even though it is not distinct enough to enable differentiation between two individuals. The same goes for biological sex. Just like date of birth, the sex of the holder may be considered permanent. Doc 9303 provides three categories for the sex of passport holders, ‘F for female, M for male, or X for unspecified’. These may, as all categorizations, be discussed and criticized. The point here is to show that biological sex, just like date of birth, satisfies one of the two fundamental premises about biometrically relevant body traits: relative permanence. However, as biometric traits, both date of birth and biological sex suffer from a lack of discriminative power. It is therefore sometimes referred to as ‘soft biometrics’.

The signature is the third additional biometric feature that is mandatory on MRPs. Like date of birth and sex, it should be displayed on the data page. For ePassports also, it must be stored on the chip. The signature has been considered a behavioural (rather than physical) biometric modality, and signature verification is still regarded as a poorly developed biometric modality. It is nevertheless considered vital in international passports because of its long pedigree, its considerable legal recognition, and its continued usage in document authentication and authorization related to, for instance, checks and credit card receipts. Comparative approaches to the international requirements specified in Doc 9303 may thus include date of birth, sex, and signature. A possible fourth candidate is the displayed photograph. Different countries or states may also supplement identification features to be displayed on the passport’s data page. The Swedish passport, for example, also contains information about the passport holder’s height.

If we compare the visible (eye-readable) information about physiological characteristics in contemporary Belgian or Swedish passports with the list of data in Karin Bergman’s 1964 passport, we see a significant reduction in biometric information. At first glance, it may seem that all the physical features that a fraudster might easily change and that today’s law-abiding citizens are in fact changing on a regular basis—such as hair colour (and to some extent also eye colour, thanks to coloured contact lenses)—have been removed from the list. Only physical traits that cannot easily be altered remain, such as age, gender, and (for the Swedish passport) height.

Yet, as mentioned above, these features are all typical examples of soft biometrics—physical, behavioural, or adhered human characteristics that have been derived from the way in which human beings normally recognize their peers. The substantial reduction in biometric information on the
passport identity page is, then, also a reduction of the types of information that people rely on in order to identify other human beings.

Instead, biometric information has been displaced to the chip, to be verified by machines. Certainly, and somewhat surprisingly perhaps, the choice fell on computerized face perception, which is proving to be an incredibly difficult technology to engineer.40 This stands in sharp contrast to the human ability for face perception, often described as the most developed visual perception skill in humans.41 Despite this difficulty, the ICAO chose to concentrate on only one body part (the face) and one primary method (facial recognition technology, or FRT), with the option of including two additional features (fingerprint and iris scan).42 Comparing biometrics in pre-electronic and electronic passports, we now see fewer biometric inscriptions on the human-readable identity page. The current passport is primarily aimed at just one area, which is investigated more thoroughly through digital technologies.

Body, network, state

In addition to the changes in biometric information described above, a comparison between the pre-electronic passport and the current biometric passport (as specified in Doc 9303) shows three major changes.

First, compared with Karin Bergman’s 1964 passport, the current ID page in international passports indicates a striking reduction of the social dimension of individual identity: profession, social status, children, and residence are no longer mandatory information.43 There is, in other words, a substantial decrease in all the types of information that people rely on in order to recognize and identify other human beings, both biometric and social information.

Second, the list of inscriptions on the ID page inscribes the passport as well as its holder into a network of registries. This applies not just to the passport number (passport registry) and the personal number (national registry) but also to the date and place of birth. Place of birth is often used in legal documents, together with one’s full name and date of birth, to uniquely identify a person.44 Place of birth then indicates entries in databases like church records and population registries and refers to individual identifiers like ‘personal number’, ‘social security number’, ‘Unique Population Registry Code’, or else ‘Personal ID Code Number’. The date of birth – an indicator of age that may be considered biometric information – equally refers to a number of public registries, databases, and archives. As stated
by Doc 9303, the holder’s date of birth shall be specified ‘as recorded by the issuing State or organization’. So even as date of birth may be a physical biometric and place of birth could be said to have a social dimension, both connect first and foremost the holder of the passport, as well as the passport document itself, to public bureaucracy and to the state to which the document belongs.

Third, this emphasis on the state or nation is repeatedly stressed on the passport identity page: the issuing state and the nationality of the holder are stressed twice, both in full (e.g. SVENSK SWEDISH) and by a three-letter code (e.g. SWE for Sweden). In countries where the place of birth automatically determines the nationality of the baby, the holder’s place of birth also indicates the nationality (or citizenship) of that person or his or her parents (such as NEW YORK, USA, which would also indicate US citizenship). In these cases, there are three entries explicitly stating nationality only in the visual inspection zone (VIZ) of the identity page. In cases where the issuing state is the same as the nationality of the holder, the nation is almost more pronounced than the person.

The political dimension of this emphasis is particularly evident in cases where national affiliation is disputable or unclear. This is strikingly obfuscated in Doc 9303. A well-hidden example may be found in a footnote to
the list of three-letter codes for nationalities specified in the first volume of Doc 9303. Remarkably, this is the only footnote to the list. It refers to the dispute between the governments of Argentina and the United Kingdom of Great Britain and Northern Ireland ‘concerning sovereignty over Falkland Islands (Malvinas)’, as it says. The code that has been provided with this footnote is FLK. It may, in other words, seem as if Doc 9303 has taken sides with Great Britain in this dispute, as the British name ‘Falkland Islands’ is chosen over the Spanish ‘Islas Malvinas’. More important in this context, the example shows how strongly the contemporary passport nationalizes its subject. This nationalization of individual identity is also clearly demonstrated in cases where people are without nationality (e.g. stateless persons, refugees), as this must be marked in the passport as XXA, XXB, XXC, or XXX, codes that define people according to the requirement of nationality. Both these examples underscore the significant connection of nationality to machine-readable passports as well as the political dimensions of such nationalization.

To sum up, the biometric passport specifies a person’s identity in terms of a name and signature, gender and age, a biometric measurement of the face, as well as a body of data connecting individual identity to societal regulations of work, taxation, government benefits, health care, and other governmental functions. This information is given maximum-security protection in accordance with current ideologies, systems, and technologies of document security. In the current passport regime, individual identity is thus defined as: (1) machine-readable body measurements and (2) a set of personal data recorded in governmental and other public archives that are (3) mediated by a document owned and managed by the state.

**The archival practices of enrolment and inspection**

As we have seen, few –if any –human observations of physical (or social for that matter) traits are inscribed in the ePassport. Admittedly, some countries do note both physical details (such as height and eye colour) and place of residence in a local or national passport registry. For the passport booklet, however, the passport issuer will verify the identification papers of the applicant against available records and databases before capturing one or several biometric samples from the applicant by use of a high-resolution image capture technology for facial image enrolment (mandatory globally) as well fingerprints or iris scans in countries where this is required.
Sometimes biometrics is also used in the identification process in order to improve the quality of the background checking that is part of the passport application process. Identification is then understood as performing ‘a one-to-many search between proffered biometric data and a collection of templates representing all of the subjects who are enrolled in the system.’ This assumes, of course, that one has biometric records such as a passport registry or a police record that can be searched in order to find a biometric template of the enrollee. Doc 9303 defines ‘biometric template’ as ‘a machine-encoded representation of the trait created by a computer software algorithm’ which ‘enables comparisons (matches) to be performed to score the degree of confidence with which separately recorded traits identify (or do not identify) the same person.’ Such a template is, as they also say in Doc 9303, of relatively small data size. This is due to the amount of information being sharply reduced compared with the high-resolution image as captured during enrolment. It is, therefore, a highly simplified representation created by a computer software algorithm.

Biometric templates are used for matching the high-resolution image on the microchip against archives during enrolment (as mentioned above) as well as in passport inspections. The templates and their readers are not internationally standardized. Each manufacturer of a biometric system uses a unique template format, and templates are not interchangeable between systems. According to Doc 9303:

Facial recognition vendors all use proprietary algorithms to generate their biometric templates. These algorithms are kept secret by the vendors as their intellectual property and cannot be reverse-engineered to create a recognizable facial image. Therefore facial recognition templates are not interoperable between vendors – the only way to achieve interoperability with facial images is for the ‘original’ captured photograph to be passed to the receiving State. The receiving State then uses its own vendor algorithm (which may or may not be the same vendor/version as the issuing State used) to compare a facial image captured in real time of the MRP holder with the facial image read from the data storage technology in their MRP.

Doc 9303 does not specify a globally interoperable machine-assisted verification method. However, it warns against relying on a single feature to verify authenticity because this increases the risk that the method will be compromised. Overall, we can still say that the high-resolution image of the face is stored on the chip to be used as input in facial recognition
systems. The verification system uses a camera to capture a facial image of the traveller in real time and uses an algorithm to compare this image with the one stored on the chip. Mark Salter (2003) underscores the fact that ‘[…] the modern passport does not guarantee the ‘security’ or even the ‘identity’ of the bearer’. He also claims, somewhat inaccurately, that ‘the passport certifies only that the document of the passport is identical to other documents.’ When looking into the verification process from an archival perspective, we can see that the information inscribed in the pre-electronic passport implies a human verification not only of documents but also of people’s appearance. The same applies to the electronic passport, except that now a machine checks the papers as well as the traveler’s appearance. But Salter is right that the passport cannot prove the identity of the traveller. This also holds true for the biometric passport, no matter how hard the ICAO insists that the ‘only method of relating the person irrevocably to his travel document is to have a physiological characteristic of that person associated with the travel document in a tamper-proof manner.’ As Julian Ashbourn and others have underscored, we should never consider a biometric as positive proof of identity.

In the early days of automated identity verification, a common claim was that a biometric check proves that you are who you say you are. Of course, this is simply not the case; a biometric check proves no such thing. […] All we are doing is comparing two sets of data and, according to predefined criteria, reaching a conclusion as to whether they are alike enough to be considered a match.

So, when a traveller enters or exits a state or for any other reason has his/her biometric passports checked, the information on the chip is not just compared with the image of the traveller captured on the spot (often referred to as a ‘one-to-one match’). The information on the chip and the newly obtained image data can also be compared against a small number of biometric reference templates on file (locally or accessed from elsewhere), for instance when matching against a ‘watch list’ of persons who warrant detailed identity investigation or are known criminals, terrorists, etc. This is the archival practice of passport verification.

The archival promise

The background for developing electronic passports with biometric capability is the perception of increased security threats in our globalized society.
The first volume of Doc 9303 asserts that: ‘The growth in international crime and illegal immigration has led to increasing concerns over the security of travel documents and calls for recommendations on what may be done to help improve their resistance to attack or misuse.’ Research gives no indication that crime is on the rise, yet we witness (as Doc 9303 also states) a more ‘security-conscious world’. As a result, ‘the need for machine-assisted global interoperability has become pressing’ and has ‘necessitated the standardization of one primary biometric identification method and of one method of data storage.’ The ICAO has therefore developed recommendations ‘specifically in response to the needs of passport issuing and immigration authorities to ensure accurate identification of a passport applicant or holder while minimizing facilitation problems for the traveller.’ The primary purpose of using chip technology in the passport has been to augment the security of authentication of the passport documents as well as their legitimate holders.

Another reason for developing electronic passports is the desire for efficiency, faced with a global population increasingly ‘on the move’ across borders. Doc 9303 tells the story of how the ICAO started this work in 1968 with the development of the first machine-readable travel documents. A panel was charged with developing recommendations for a standardized passport book or card that would be machine-readable ‘in the interest of accelerating the clearance of passengers through passport controls.’ In 1998, the next chapter of this story began – the work ‘to establish the most effective biometric identification system and associated means of data storage’ for use in passports and other machine-readable travel document (MRTD) applications, ‘particularly in relation to document issuance and immigration considerations.’ ‘Throughput’ they call it (e.g. ‘travellers per minute’), whether it refers to ‘the biometric system or the border-crossing system as a whole.’

This call for security and efficiency in the identification and verification of individual identity overlaps in striking ways with historical attempts at registering and storing biometric information about repeat offenders in late nineteenth-century police archives. Allan Sekula is often credited for having brought forth the Paris police official Alphonse Bertillon in this regard. In his influential essay ‘The Body and the Archive’ (1986), Bertillon is described as the inventor of:

the first effective modern system of criminal identification. His was a bipartite system, positioning a ‘microscopic’ individual record within a ‘macroscopic’ aggregate. First, he combined photographic portraiture,
anthropometric description, and highly standardized and abbreviated written notes on a single fiche, or card. Second, he organized these cards within a comprehensive, statistically based filing system.69

Anthropometric description refers to a measurement of the human body (from the Greek words anthropos, meaning ‘man’, and metron, meaning ‘measure’) transformed into a verbal text. This text was pared down ‘to a denotative shorthand, which was then linked to a numerical series’.70 According to Sekula, this was ‘not merely a self-contained archival project. We can understand another, more global, imperative,’ Sekula states, ‘if we remember that one problem for the late-nineteenth-century police was the telegraphic transmission of information regarding suspects.’71 Bertillon’s response to the problem was to make all the data telegraphable. The ambition was, as we can see, global – both in its technical design and with regard to current communication technologies.

Sekula is mostly interested in the photographic archive. He is concerned with the way in which the archive, as he argues, became the dominant institutional basis for photographic meaning somewhere roughly between 1880 and 1910.72 However, for photography, the ‘archival promise was frustrated by the messy contingency of the photograph as well as the sheer quantity of images’.73 As Sekula sees it, the solution to this was ‘to invent a machine, or rather a clerical apparatus, a filing system, which allows the operator/researcher/editor to retrieve the individual instance from the huge quantity of images contained within the archive.’74 This is what Bertillon did and with success. ‘Thus Bertillon arrested the criminal body, determined its identity as a body that had already been defined as criminal, by means that subordinated the image – which remained necessary but insufficient – to verbal text and numerical series.’75 Herein lies the archival promise of the late nineteenth-century police archive: it allowed the operator to retrieve the individual instance from the huge quantity of instances contained within the archive and the exchange of information between police departments and between states.

The Bertillon system should not only be precise but also efficient. Bertillon wanted ‘to accelerate the work of processing criminals and to employ effectively the labours of unskilled clerks’. Sekula positions Bertillon as a ‘prophet of rationalization’ akin to Frederick Taylor, ‘his American contemporary, [...] the inventor of scientific management, the first system of modern factory discipline.’76 In his discussion of the history of the US passport at the beginning of the twentieth century, Craig Robertson refers to Sekula’s perception of Bertillon’s project as the invention of a system
‘for regulating and accelerating the flow of texts, profoundly linked to the logic of Taylorism.’77 Robertson argues that the passport developed into an archival technology that ‘classifies and orders evidence in the service of the production of truth to be used to explain who “we” are and where “we” come from. And it does this, Robertson states, ‘in the anticipation of a future need to know. The archival pact with the future is established through the “rationalization” which Sekula foregrounds to articulate archival practices.’78

The parallels between the late nineteenth-century police archives and current biometric passports are striking both in terms of ambition and mindset, even if the techniques vary and the archival conditions are radically different. One of the most conspicuous keywords in Doc 9303 is the notion of ‘global interoperability’. It shows up already in the foreword to volume one and is introduced with reference to the previous edition of Doc 9303 (from 2003): ‘global interoperability’ is understood as ‘the capability of inspection systems (either manual or automated) in different States throughout the world to exchange data, to process data received from systems in other States, and to utilize that data in inspection operations in their respective States.’79 Yet ‘global interoperability’ is not only understood descriptively but also normatively: it is ‘a major objective of the standardized specifications for placement of both eye readable and machine readable data in all MRTDs’. With reference to ‘the security-conscious world of today’, it is further stressed that ‘the need for machine-assisted global interoperability has become pressing’ and that this has ‘necessitated the standardization of one primary biometric identification method and of one method of data storage’.80 I will maintain the importance of scrutinizing these standardizations of archival entries and functionalities of the biometric passport to understand how this practice shapes identities and societies.

The ICAO’s standardized specifications of eye-readable and machine-readable data in MRPs apply not only to the placement of data but also to the question of which information to convey and in what form it should be conveyed. Earlier in this article we saw how the information on the identity page of the ePassport has been significantly reduced. The issuing state is to some extent free to select certain traits (such as Sweden, where information about the passport holder’s height is included), but the choices are limited. Doc 9303 also strictly regulates the location of the various types of information on the identity page, but in addition to these factors, another form of cultural homogenization is also operative. Cultural homogenization may notably be seen as one of the main characteristics of globalization and refers to the reduction in cultural diversity as the result of processes by
which local cultures are transformed or absorbed by a dominant culture. Homogenization of the international passport has been an ambition since the first convention on passports in Paris 1920, if not earlier. In addition to the general booklet design and other passport guidelines (including requirements for physiological descriptions and photographic portrait), the League of Nations decided that all passports were to be written in at least two languages, one of which was French, the diplomatic language of that era.

Today, all passports contain information in at least two languages, of which one is either English, French, or Spanish (an extension of what is considered to be internationally accessible languages, from one to three). Meanwhile, Doc 9303 specifies a strict regulation of acceptable letters, particularly in the machine-readable zone (MRZ) but also in the visual inspection zone (VIZ) of the identity page. National characters may be used in the VIZ, but if they are not Latin-based, then a transliteration into Latin characters must be provided. Dates should be entered in accordance with the Gregorian calendar, and numbers must be presented as ‘Arabic numerals’ (i.e. Indo-Arabic or Hindu-Arabic numerals). States that use numbers other than ‘Arabic numerals’ to represent numerical data in the VIZ shall provide a translation into Arabic numerals. If national characters are accepted in the visual inspection zone (VIZ) of the identity page, they shall not appear in the machine-readable zone (MRZ). The same applies to diacritical marks or accents, apostrophes, etc., which are not allowed in the MRZ. The explanation is simple and technical: national characters and diacritical marks generally appear only in the computer-processing systems of the states in which they apply and are not available globally.

The desire to develop such a globalization of letters, calendars, and numbers is not surprising and also perhaps necessary for better international communication between societies. However, I will argue that it is vital to notice who is creating the world in their image, that is, which local standards act as templates to create global standards: Latin letters, the Gregorian calendar, and what is often called Arabic numerals. These standardized specifications for both eye-readable and machine-readable data in the MRP are part of a practice that produce not just the document but also the specific human identity the passport provides evidence for.

The second major security and efficiency measure in Doc 9303 involves technical standardizations of the MRP as such as well as the development of a standardized biometric identification method and a method of data storage. The two strings of alphanumeric characters at the bottom of the
identity page (referred to above as the machine-readable zone, or MRZ) enables border controllers and other law enforcement agents to process passports more quickly without having to input the information manually into a computer. In other words, MRPs incorporate an MRZ to facilitate the inspection of travel documents. In addition to increasing efficiency at passport checkpoints, the MRZ provides verification of the information in the VIZ and may be used to provide search characters for a database inquiry. In addition, it may be used to capture data for registration of arrival and departure or simply to point to an existing record in a database. These are the archival promises of the MRZ.

According to the ICAO, the primary purpose of using chip technology is to have the ability to capture biometrics in the travel document. Further, the key application of the biometrics solution is to relate an MRP holder to the MRP he or she is carrying.
Each time a traveller (i.e. MRP holder) enters or exits a State, his identity can be verified against the image created at the time his travel document was issued. This will ensure that the holder of a document is the legitimate person to whom it was issued and will enhance the effectiveness of any advance passenger information (API) system.89

Such verification can be done without touching the passport booklet, since the aerial connection allows data to be communicated between the micro-chip and an encoding/reading device at a distance of ten centimetres.90 Hence, the biometric passport presents the chip as its primary source of information. The chip also functions as a backup of all the vital information otherwise available in the booklet (except visas and stamps). The standardization of one primary biometric identification method (facial recognition technology) and one method of data storage (the chip and the security object) are presented as more than promising for the fulfilment of the desire for greater safety and efficiency in the regulation of travelling. These are the archival promises of the microchip.

The contemporary biometric passport is developed in the name of security and efficiency, its biometrics presented as something brand new, unrelated to the international history of the passport and its changing attempts to connect the traveller irrevocably to his travel document. Yet, to see its parallels to the nineteenth-century police archive, we must first note some significant differences. First, Alphonse Bertillon’s police archive was a system designed to register and detect criminals (more specifically, recidivists or repeat offenders). The biometric passport, on the other hand, is a system put in place to register all travelers and to protect society from criminals. Both are, therefore, systems for the protection of society against criminals, but the first is aimed at the criminals and registers these, while the other detects (in principle) all people to protect them from any potential criminal among them. The second difference is connected to the first and concerns scale. As the director of the Identification Bureau of the Paris Prefecture of Police, Bertillon’s archival practice was large and ambitious. It could be used internationally and was also exported and used in other countries, particularly the US. However, the archive was soon outdone by other methods (particularly fingerprinting) and never enjoyed enduring global distribution. In contrast, the ICAO is an international organization, a United Nations specialized agency with nearly 70 years of experience in addition to the 26 years of The League of Nations. It collaborates with 191 member states and global aviation organizations to develop an international
Standards and Recommended Practices (SARPs) that are used as a reference by states when developing national civil aviation regulations, including the current biometric passport.91 In Doc 9303, global interoperability is one of the ICAO’s major keywords.

However, the large-scale collection and archiving of data of entire populations also changes the archive. As underscored by Jonathan Finn in Capturing the Criminal Image. From Mug Shot to Surveillance Society (2009), ‘Once brought into the archive, all bodies can be identified and re-identified according to changing needs of those in control of the data and the specific parameters for searching and using the archive.’92 And with digitally networked, large-scale archives, they will. This is not just a technical condition for the large-scale archive but also its political terms. One clear example is seen in the recurring phenomenon of ‘function creep’ or ‘scope creep’. Scope creep is, simply put, when a service conceived for one purpose is pressed into service for another purpose. According to Julian Ashbourn in Guide to Biometrics for Large-Sale Systems (2011), this is among the most prevalent and destabilizing effects within large-scale systems, particularly in the public sector.93 The source of scope creep is often political, Ashbourn states: one government agency wishes to access data held by another. 94

Scope creep is not a new phenomenon. A very widespread case is the quite blurry histories of the development of identification numbers. Many countries issued identification numbers for a singular purpose, but over time, they became de facto national identification numbers. The most well-known and obvious example is probably the Social Security number system developed in the United States in order to disburse Social Security benefits. Due to scope creep, however, these numbers are used for other purposes to the point where it has become more or less mandatory for one to have a Social Security number if one wants to open a bank account, obtain a credit card, or drive a car. Yet, if the phenomenon is not new, it is reasonable to assume that digital information technologies and networked databases make scope creep easier to resort to and also more tempting politically. This is, however, in conflict with privacy principle number one, the purpose for collection: information is collected for a lawful purpose connected with a function or activity of an agency, and the collection of the information is necessary for that purpose. Scope creep threatens to undermine this basic principle in democratic societies. It also seems to compromise the operational integrity of the archive.95

By way of concluding, I will give an example of how scope creep can make visible the political radicality of the biometric passport and its archival promise in a way that demonstrates the parallels rather than the differences
between the nineteenth-century police archive and the biometric passport. The example also sheds light on the inscription of the passport in the history of the effort to combat crime as part of an emergent global archive of pre-criminals.

On 21 June 2013, the Norwegian Passport Act (1997) was adjusted on an important point: the § 8, which concerns the Passport Registry. The general rule was, and still is, that only the passport authorities – Kripos (the national unit for combating organized and other serious crime) and the Norwegian border authorities – should have access to the passport registry unless otherwise provided for by law or by regulation pursuant to law. On 21 June 2013, a list was added (section 8a) specifying the kind of cases where the police could access and repurpose information from the passport registry. ‘We will make the passport registry an effective tool in combating crime,’ stated then Minister of Justice and Public Security Grete Faremo during a press conference.

This is a classic example of scope creep. The source is political; one government agency wants to access data held by another. There are reportedly several types of cases that form the basis for this bill, including grooming and child abuse. But the main background was the official report from ‘the 22/7 commission’ (2012) following the terror attacks in Norway in 2011. This report does not restrict itself to discussing the actions that took place before, during, and after the terror attacks; it also provides recommendations and advice as to how to prevent similar attacks in the future. As part of these preventive measures, the report states that the PST [Norwegian Police Security Agency] would like to gain access to a number of […] information sources, including the Customs Directorate and the Immigration Administration records, as well as Employer and employee registry and the Passport registry […]’. And so, less than a year later, the access was granted, not just for serious crimes under investigation (as was the case previously) but also for more minor offenses, including ‘the prevention or investigation of an action that according to law may lead to a higher sentence than imprisonment for six months’.

This particular example of scope creep also demonstrates another tendency in today’s society that is vital for assessing the archival situation of the contemporary passport: the increasing emphasis on the precautionary principle in criminal law. To accept that personal information from a passport registry can and should be handed over to the police to prevent a criminal action from happening seems to be not just a challenge to the passport as institution but also in conflict with the presumption of innocence,
the principle that one is considered innocent until proven guilty.101 To risk being charged based on the suspicion that you may think of planning illegal actions is also a threat to the freedom of thought and the freedom of speech and even undermines the possibility of changing one’s mind.

The example illustrates that the history of the passport is no longer simply a parallel to the history of the police archive. The two archives converge. The genealogy of the passport can be traced back to nineteenth-century criminal records as an instrument of discipline and subordination to the state. This confirms and exemplifies Jonathan Finn’s more general point about the body and the archive in current society:

In the nineteenth-century archive, the image captured the criminal, representing his identity within its frame. In the new digital space, the image captures the body independently of any such fixed identity. Criminality is less a function of an actual criminal event or body than it is an attribute that all bodies are prone to. As a result, all bodies, not just those identified as criminal, are sites to be monitored and administrated. The body in the digital archive exists as something that is potentially criminal and, therefore, as something warranting continued surveillance.102

The passpot is not just an archive; it is a pre-active criminal archive anticipating a future need to know: we are all potentially criminals, and the passport is part of a global surveillance system for monitoring all citizens to prevent and solve crime. This is the archival premise of the biometric passport.

To conclude, the biometric passport defines individual identity as machine-readable body measurements and personal data recorded in governmental and other public archives mediated by an electronically enabled document (or micro-archive) owned and managed by the state. This small archive is part of an archival assemblage of national, bilateral, and international hubs. The passport is thus not just ‘Man’s Most Travelled Document’, as Martin Lloyd put it. Its archival condition has radically changed since the paper-based archives of Alphonse Bertillon, which depended on the telegraphic transmission of information to communicate across countries and regions. It is not just less space-based and hence to a lesser extent dominated by spatial order.103 Today, the archive is, in principle, ubiquitous, premised not just on networks but also on transfer speed. Temporal efficiency –achieved through the combination of machine readability, connection between
microchip and aerial, and biometric templates that match high-resolution chip images against various types of archives —underpins the impression that the passport is increasingly interwoven in a system of ubiquitous surveillance. Accessing information in close-to-real-time also stimulates scope creep and other challenges to the rule of law. The biometric passport has thus transformed travelling individuals from being socially defined by peer recognition to bodies of information sorted according to ever-changing political perspectives on who is on the inside and the outside of a ‘we’ defined by its vulnerability to crime, terrorism, or other threats.104

Notes

1. See Salter, p. 93.
3. For a thorough discussion of early modern passport history, see Torpey.
5. Ibid.
6. The safe conduct pass is well known since at least the early thirteenth century. See, for instance, Salter, pp. 12-20.
7. The birth of the modern passport system is a complex topic with wide variations within and across different countries, but if the US can serve as an example, the historic moment in time may be indicated by the political decision giving the Department of Foreign Affairs the responsibility of issuing passports in the name of the state in 1782. See Robertsen, 2010, p. 253.
8. See Featherstone and Manoff.
10. Ernst, p. 42.
14. The notions ePassport and biometric passports are used interchangeably. However, the ePassport does not necessarily contain biometric information. E-passports are, rather, electronically enabled passports with biometric identification capability.
15. Doc 9303 contains current ICAO specifications for machine-readable travel document (MRTD), including machine-readable passports (Part 1), visas (Part 2), and ID cards (‘travel documents’) used in crossing the borders (Part 3). Parts 2 and 3 will not be discussed here. For simplicity reasons, I will henceforth refer to Part 1 in its sixth edition (2006) only as Doc 9303. After the deadline for phasing out non-machine readable passports 24 November
2015, Doc 9303 has been reorganized and divided into 12 parts. The regulation of biometric information is specified in Volume 9 without significant changes since the previous edition.

16. Today, machine-readable passports are required globally. Admittedly, the ICAO has no supranational authority. Therefore, of course, the requirement applies only to contracting states. For these, the deadline for phasing out all non-machine readable passports was 24 November 2015. Contracting states shall ensure that the expiration date falls before 24 November 2015, so that all non-machine-readable passports should be out of circulation by this date. See http://www.icao.int/Security/mrtd/Pages/24-NOV-2015.aspx [accessed 2 May 2015]


23. The League of Nations lasted for 26 years before the United Nations (UN) replaced it after the end of the Second World War in 1946. The UN inherited a number of agencies and organizations founded by the League. The responsibility for setting passport standards was passed to the ICAO (the International Civil Aviation Organization) when that authority was founded in 1947. The ICAO had then 188 contracting states. See Salter, pp. 78-86; Stanton, p. 254.


25. See ibid., p. 7. Lloyd refers to these descriptions as ‘physiognomic’. Without going into the complex history of physiognomy, I will here use the more neutral term physiology.

26. See, for instance, Jain et al., Handbook of Biometrics.

27. See, for instance, Jain and Kumar; Paveši and Ribari.


33. For a critical discussion of biometrics with regard to gender and race, see Magnet.

34. See Nandakumar et al., 2008; Jain, Dass and Nandakumar, 2004.

35. For people who cannot write a signature, ‘a usual mark of the holder’ is required (see vol. 1, IV-8).


39. Idrus et al.

40. See, for instance, Gates, p. 9.

41. See, for instance, Gates, p. 11.

42. Currently, both the Swedish and Belgium biometric passports have included fingerprints on the chip.

43. An exception to the rule of not including titles, professional and academic qualifications, etc. is if the issuing state considers these to be legally part of the name. See Doc 9303 vol.1, IV-18 and IV-19.

44. It does not always refer to the place where the parents of the new baby live but rather the place where the person was born, for instance in a hospital. In many countries, this also means that the government requires that the birth of the new baby be registered at the place of birth. In other countries, such as Sweden, there is a concept of ‘domicile of birth’, which means that the domicile of the baby’s mother is the registered place of birth. See Statens offentliga utredningar, 1994:44, 1994, p. 32. In all these cases, place of birth indicates entries in a range of databases.


46. Under the law of most countries, passports are government property.

47. Place of birth as an unconditional basis for citizenship is the predominant rule in the Americas but is rare elsewhere.

48. Vol. 1, IV-44.

49. See Doc 9303 vol. 2, II-3.

50. ‘Identification’ may be contrasted to ‘verification’, which means ‘to perform a one-to-one match between proffered biometric data obtained from the MRP holder now and a biometric template created when the holder enrolled in the system.’ See Doc 9303 vol. 2, II-3.


53. Ibid.


55. Vol. 2, II-3

56. Vol. 2, II-11

57. See vol. 1, III-20


59. Salter, p. 93.

60. Asbourn, p. 114.

61. See, for instance, Doc 9303 vol. 2, II-3.


64. Doc 9303, vol. 1, foreword, p. iii.
66. Vol. 1, I-1. In 1980, the specifications and guidance material developed by this panel were published as the first edition of Doc 9303, titled *A Passport with Machine Readable Capability*, which became the basis for the initial issuance of machine-readable passports by Australia, Canada, and the United States.
69. Sekula, p. 18.
70. Ibid., p. 33.
71. Ibid.
72. Ibid., p. 56.
73. Ibid., p. 17.
74. Ibid., p. 18.
75. Ibid., p. 33.
76. Ibid., p. 25.
77. Ibid., p. 57, cf. also Robertson, 2006.
78. Robertson, 2006, italics added.
79. Vol. 1, foreword, p. iii.
80. Ibid.
82. Vol. 1, IV-23.
83. Arabic numerals should not be confused with the Eastern Arabic numerals (also called Arabic-Indic numerals and Arabic Eastern numerals), which are the symbols used to represent the Hindu-Arabic numeral system in conjunction with the Arabic alphabet in the countries of the Arab east and its variant in other countries.
89. Ibid.
91. See http://www.icao.int/Pages/default.aspx [accessed 6 April 2015]
92. See Finn, p. 107.
94. Ibid.
95. Cf. Ashbourn.
97. Translated by the author. https://www.regjeringen.no/nb/aktuelt/politiet-far-utvide-bruken-av-passregist/id726715/
101. More officially stated as (Lat.) *Ei incumbit probatio qui dicit, non qui negat*: the burden of proof is on the one who declares, not on the one who denies.
102. Finn, p. 105.
103. See de Certeau 1984.

Works cited


