A primer to the nuances of authorisation, authentication, and identification

Enka Blanchard*[1,2,3], Mehdi Bouhamidi[1], and Jörg Pohle[4]

[1] Laboratory of industrial and human automation, mechanics and computer science, Polytechnic University Hauts-de-France
[2] Chaire d'Intelligence Spatiale, Polytechnic University Hauts-de-France
[3] CNRS Center for Internet and Society, UPR 2000
[4] Alexander von Humboldt Institute for Internet and Society, Berlin

May 5, 2024

1 Introduction

Whether online or offline, questions of identities and identification have been a topic of ongoing discussion and debate in society for many years. In many Western societies, the last decades have seen an ever-growing emphasis placed upon the malleability and flux of identities. This is in contrast to the perceived stability of human identities in the past, often characterised by "stable relationships" in society, family or lifelong employment. The celebration of the relative historical novelty of these aspects of identity often overshadows the importance of social categorisation, i.e. the categorisation of others, in shaping an individual's experiences in society [Gid91, Jen00]. Self or group identification, i.e. how individuals or groups identify themselves, is but one mode of identification. The fundamental process of identifying involves specifying what something or someone is and what it is not, including its or their properties or characteristics. Humans regularly engage in dialectic processes of identification with internal and external moments, involving how they identify themselves, how others identify them, and the ongoing interplay of these processes in social identification. Those others may not only be humans but also institutions.

Since at least the fourteenth century, states have created increasingly intricate administrative systems for tracking individual identities in order to better register and control their populations [Gro07], in the pursuit of, e.g., improving tax collection and conscription [Sco98]. This included the development of a range of categorisation and identification practices and documents, including seals, stamps, signatures, and identity papers. Beyond the impact of specific legislations such as the Real ID Act of 2005 in the USA or Regulation 2019/1157 on strengthening the security of identity cards in the EU, we can observe three qualitative changes in recent years. First, the issuance of authoritative identities is not anymore restricted to state actors but is increasingly performed by private actors such as companies. Second, these are not limited to paper documents but have become complex digital identities. Finally, we can observe an increasing convergence of the different identification systems, state and private, analogue and digital, to the benefits of both states and companies, e.g. when matching state-issued and online IDs for social networks.

Behind this apparent harmony of state and private interests, a privatisation of state prerogatives in the area of authoritative identities is taking place, driven by commercial interests [Zub19]. Characterised by what Evgeny Morozov calls "technological solutionism" [Mor13] — the idea that given the right software and data, technology can solve all of humankind's problems — companies have a strong incentive to oversell digital identity systems they create and operate. The multitude and fuzziness of underlying concepts of identity and

*The authors contributed equally and are listed in alphabetical order.

identification, social, legal and technical, has given rise to misunderstandings about what is built into certain systems, what the characteristics and what the consequences are. For example, a recent decision by the French Cour de Cassation on 2-factor authentication is based on the false understanding that the existence of multiple modalities guaranteed security without consideration of the underlying security of each modality. Thus, these misunderstandings can have in turn severe legal implications.

We understand that there are difficulties with the translation of certain aspects between the disciplines and that the infrastructure — including the legal infrastructure — of identity systems is generally built upon assumptions that are made based on past social, legal, and technical experiences, assumptions which might not really be true in online settings. Thus, our aim with this chapter is to provide more solid grounding for people working on identities, analogue and digital, and identification practices and systems at the interface of law and computing.

This chapter, focused on the nuances between authorisation, authentication, and identification, is structured as follows. We start by going over conceptual aspects and setting some definitions around identification and authentication, from adversarial frameworks to information linking and leaking. We follow with a quick overview of the state of the art on technical solutions for authentication. Finally, we discuss the issues of power and normativity in their relationships to identity.

2 Conceptual aspects and definitions

Historically developed bureaucratic categorisation and identification practices, documents, and systems form the foundation for digital identities, which are currently being implemented to monitor and control behaviour and resource use. Unlike previous state-issued authoritative identities, these new systems are increasingly interrelated and all-encompassing. As a result, these digital identification systems have profound implications for how power and authority are distributed in society. They have the potential to both reinforce existing power structures and create new forms of power and control [Zub19]. This section will shed light on the underlying conceptual aspects to provide ground for the subsequent discussion.

2.1 Identification & authentication as crutches for authorisation

Inspired by a remark made by Lars Fischer in an online workshop[1] in 2021, which he says goes back to Carsten Bormann, we base our analysis on the claim that identification and authentication are merely the crutches for implementing the allocation of resources and the authorisation of access to them.

All of the following assumes that it is necessary or deemed desirable to selectively grant access to certain resources (including information) or rights — a question which would take us further from our subject. Looking at the history of the Internet since the 1990s, one can observe an almost universal move from simple authorisation mechanisms to more complex identification and authentication mechanisms [FFS11]. Economic incentives have pushed towards ever more encompassing user profiles as it allows for much better commodification and rent extraction [Zub19]. Efficient pushback is only recently getting more traction, e.g., with the EU General Data Protection Regulation[2] (GDPR). It is now common to have an account for nearly every website: in 2019, the 50 most visited websites all featured either password or biometric authentication [Bla22]). In addition to non-negligible side effects affecting privacy and data protection, IT security has also been strongly negatively affected by this development.

We start by defining authorisation as the process of verifying that an agent asking for a resource or right is entitled to it, and then granting them access to that resource or allowing them to exercise their right. Following the tradition of computer science, we then distinguish between identification and authentication, as the latter can refer to something other than identities. We understand authentication as the proof or the process of proving a claim. With respect to digital identities, authentication serves to prove claims regarding identities or rights to access. Such right to access is often implemented by establishing partial identity to some group of authorised people.

[1] Berlin cyber security & politics community breakfast.

[2] One of the GDPR's main impact — compared to pre-existing national regulations, including those based on the 1995 Data Protection Directive — is that it seems to be more strictly enforced.

In common speech and most of the academic discussion, at least outside of computer science, identification refers to authenticated identification. That is, the provision of proof that one's identification is correct by giving or showing an authority-issued (state-issued or platform-issued) element of proof. However, we can adopt a more general understanding as introduced earlier, whereby identification is the process of specifying what something is and what it is not, including its properties or characteristics [Jen00]. In formal terms, we can distinguish strong and weak (or group) identification. Strong identification is the process of marking some unique element as being the target of that identification. In group (or weak) identification, there may be more than one element marked as target, such as multiple people or objects. Groups may be defined by characteristics, e.g., people who are 18 years or older, or by enumeration, similar to sets. In the latter case, the group's definition by enumeration requires memory, i.e. an account, a list or a database, and relies on a strong identification process. Thus, the group is composed of everyone who can prove that they're authorised to be in the group, i.e. by accessing the account, being on the list or in the database. In practice, with the checking in the database thus being rather simple, the focus in the implementation shifts to the initial process of authorisation (e.g., at account creation).

To make the technical concepts more approachable and understandable, we can use the example of a concert in the offline world, which we will further develop below. There are concerts where one pays cash at the entrance and then is let in. If there is no other entrance and the bouncers do not cheat, the fact that one is inside proves that they have paid. Thus, authentication is provided by just being there. At other concerts, one buys a ticket in advance. This ticket is the proof (authentication) that one belongs to the group of authorised guests. Even if one forges the ticket, and depending how good the forgery is, the ticket might be accepted as proof (authentication) by some checking agent. The ticket allows for getting access without the need of identifying and authenticating this identity. If one buys the ticket online, both the individual and the purchase can generally be tracked, i.e. are identifiable. But if the ticket is transferable, there is no proof that the person showing the ticket for authentication is the person who bought it, i.e. no authentication of one's identity. On the other hand, if one buys a non-transferable ticket based on one's identity (e.g., name, age, social security number), the attendance at the concert will be traceable, one is both identifiable and one's identity is authenticated.

2.2 Attack frameworks

Whether they attempt to perform authorisation, authentication, or identification, the systems considered need to ensure that they perform their tasks correctly. This means preventing both unintentional errors and purposeful attacks, which cannot always be differentiated. Crucially, one cannot claim that a system is "secure" in an abstract way [Sch04]. Instead, any security analysis must first start by defining an attack framework. Moreover, the system's specifications should also address whether it should be able to detect attempted attacks (or errors). The fact that no attacks were detected could mean that none happened but most generally means that any that happened bypassed the detection system. The confidence that a system has not been breached should be tempered by the perceived quality of the detection mechanisms.

The two essential elements of an attack framework are the adversaries' — there can be multiple adversaries — goals and their capabilities/constraints. Making a system that is secure for a limited time against unorganised hackers is easier than making one that should resist for a decade or more against state-level adversaries (especially considering that new vulnerabilities are discovered on a daily basis).

We will not attempt to give an overview of the adversaries' potential capabilities and constraints as they vary hugely depending on the exact systems considered, both in theory and practice. For example, the Dolev-Yao model, a standard of network cryptography, assumes that the adversary can overhear, stop, delay or synthesise any message [DY83]. Byzantine analyses in distributed systems address the cases where certain agents (including system administrators) either act inconsistently or are actively trying to create harm. Only by making the threat model explicit can the system be analysed without relying on hidden assumptions — or beliefs that certain attacks are impossible to prevent (and, thus, that the system cannot be improved). Indeed, multiple cryptographic standards can prove that they function as specified when 51% of agents are honest (i.e., follow the rules) and some only require a single honest agent[BMV19]. Those capabilities often come with relevant constraints: an adversary might want to remain undetected at all costs, have limits on their computational power, schedule or budget (indeed, many security systems work by making the attack too expensive for its expected gains).

On the other hand, the adversaries' goals can more easily be typified. When it comes to authorisation, such goals essentially fall into two categories: gaining wrongful access, or preventing someone else's legitimate access.

Although we generally see such systems (and attacks) as belonging to the online world, they have offline parallels. To go back to the concert example, if one pays at the entrance, it is equivalent to a memory-less system with one-time authorisation. The two attacks would then be to fraudulently enter (e.g., by scaling the wall) or to prevent someone else from getting inside (e.g., by stealing their money). The attack detection mechanism would be for the clerk to signal whenever someone tries to go through without paying. Supposing there are no tickets, it should be impossible, once inside, to distinguish a legitimate patron from someone who fraudulently arrived there.

Moving to authentication and identification makes the system more complex and, as such, adds more avenues of attack. The system needs to store data to perform authentication or identification. On top of the previous goals, adversaries can then add other goals linked to the acquisition and modification of this data. A first step would be to steal the existing identification and authentication data, which is concerning in multiple ways. First, a password-based authentication system might leak the set of passwords (which regularly occurs), which could be reused for further attacks (which we'll detail below in subsection 3.2) [JPG$^+$16]. Second, if the accounts are linked to any personal information, obtaining such information would be a worthy goal (semi-targeted attacks have happened, such as the one threatening to reveal the client list of extramarital affairs website Ashley Madison [JPG$^+$16]). Beyond the acquisition of information, an adversary could also want to delete or alter it (such as modifying or even creating an account for someone else and threatening to reveal it). This could also result in denying service to a specific set of users or making the service fail for everyone (both having their advantages in terms of attack complexity and detectability).

Finally, we must make a difference between generic and targeted attacks. The former involves probing for vulnerabilities on a large scale, looking for insecure accounts and servers (the hacker Maia Arson Crimew used such a probing to access, by chance, the US No Fly List and leak it[3] in 2023). Large leaked databases of user credentials are available — some publicly, some for sale on black markets — and these form the basis behind most online attacks. In those, no single user is targeted, the goal being to find the vulnerable ones with a minimal budget per target (and correspondingly limited gain). On the other hand, targeted attacks can be much more involved, with high requirements in terms of material and expertise, and corresponding upfront costs. Guaranteeing security in this context is an entirely different problem — and as made famous by Randall Munroe[4], a strong cryptosystem is useless when one can threaten the password-holder with a wrench.

2.3 Leaking information

Unlike in our concert example, few online services are memory-less. Instead of having a "state" which the different authorised users can modify, they generally keep track of the modifications and user interactions[5]. Although it is rarely the only justification for its existence, keeping a log journal of all events (and especially authorisation requests) is also a standard tool for security audits[6]. An important aspect of the logs is that it should be impossible to erase or alter previously written information, which can for example be realised by making the log append-only.

As above, keeping track of user interactions (and locking them behind an authentication mechanism) also introduces new avenues of attack and new potential goals for adversaries. Beyond the destruction of data and the (sometimes equivalent) denial of service attacks, the main objectives which target the log information

[3] `https://papersplease.org/wp/2023/01/20/the-nofly-list-is-a-muslimban-list/`.

[4] https://xkcd.com/538/

[5] Some services like `notepad.link` offer online documents which can be freely modified, without user logins or user-visible modification-tracking. However, there is no guarantee that the server does not track the user's interactions.

[6] In some ways, this could be interpreted as a crutch where instead of starting with a secure system, the logfile is intended to catch the potential attacks that the developer forgot about. There are, however, two main differences. In the present case, the logfile is an add-on that allows *ex post* detection of forgotten avenues of attack (or unknown vulnerabilities). When authentication is used as a crutch for authorisation, the decision occurs *ex ante*, which can be motivated by the desire to avoid developing a new secure design that ensures privacy-by-default.

fall into the following categories:

- learn the actions performed (or not performed) by users of the service;
- learn, create or remove a link between a user and a set of actions or user properties;
- impersonate a user in their interactions with other users/services — often by acting as a man-in-the-middle[7];
- create a fake user meant to correspond to a real person and link them to a set of actions.

An important cryptographic practice is the study of the amount of information stored and revealed by each action, which should ideally be minimal. Indeed, a transcript of the exchange between user and server should not only avoid revealing sensitive information (such as the user's credentials) but should also ideally avoid revealing whether the user obtained access (information which should only be available to the user and the service). Even a small difference in the time it takes for the server to answer — depending on whether it allows or denies access — can reveal information, timing attacks being one of the standard ways to defeat even cryptographically secure mechanisms.

For example, most password authentication systems ask the user to type in their passwords which are then sent to the server to be compared with the password on file[8] [Bla22]. This is not strictly speaking necessary, as the server does not need to know the password. Instead, it only needs to check that the user knows the correct password, which would reveal less information. This is especially true if the user cannot be sure about the trustworthiness of the server and whether it might be a phishing attempt.

Ideally, no user should be compelled to reveal more information than the simple fact that they are authorised. Any proof of such authorisation should be constructed in a way that poses no risk of revealing other information about the user. Thankfully, there are many theoretical and practical solutions, which generally require some complex cryptographic machinery. The central one is called *zero-knowledge proofs*, and the corresponding protocols ensure that two parties can perform a task together without revealing each other's secret information (or the least amount possible). For example, with passwords, each party could give the other a random string of characters and ask to encrypt it with the password and send the result. If it matches what they can each compute independently, they both know that the other has the right password. For the concert example, an imperfect but simple protocol would be to ask what was the first song played (establishing that the other was probably there since the start).

2.4 Linking information

Up to this point, we have focused on different types of attacks and purely online aspects. The complexity increases significantly if we include the online-offline interface, consider temporal aspects, or take into account that users of such identity-based systems also have rights.

However the original identity is created, whether through self-definition, group definition or categorisation, something is already happening that constitutes a linkage. Linkage here means that two or more elements (events, people, other information) are put in connection with each other. An identity is created either 1) through an initial act (e.g., account creation) to which it is intrinsically linked, or 2) through the connection to another event that has been observed and is used as the anchor for the identity (e.g., birth), or 3) through a link to a person taking part in such an act. In the case of state-generated identities, the event might be one's birth that is registered by one's parents with some competent registry office, which then creates a specific civil identity linking a human to their birth (and most probably their parents) and the state's population register via a unique identifier[9]. In contrast, the identity of visitors, immigrants and others, who in most cases already have a state-issued identity but from a different state, might be created — in the

[7] A man-in-the-middle adversary can intercept messages and impersonate both user and service to each other, which can for example allow it to bypass 2-factor authentication.

[8] Despite the first recommendations on not storing unencrypted passwords on the server dating from 1963 [MT79], standard practice in the industry has struggled to evolve beyond this, and rare are the services which implement good practices in terms of password storage [JPG$^+$16].

[9] In France, this is the NIR (corresponding to the social security number), handled by INSEE and registered at birth. The system is based on an earlier system developed by René Carmille in Vichy France.

system — via linking the individual being present at the registry office, their existing identity (or identities) as authenticated by their identity documents and the event of being present in front of some state official.

Linkage is not objective, something that *is*, but something that is *being done* by some actor. Linkability corresponds to this actor's ability to connect different events (or people, or people and events) with respect to some characteristic [PK01], e.g., that one specific human being was present at some event, at some place and/or at some point in time. That ability can refer to a description, i.e. the actor is observing a connection, or a prescription, i.e. the actor is stipulating a linkage.

Against this backdrop, it becomes clear that one is not able to prove who one is. Instead, one can only prove that one is (or is considered by others) the same person who is linked to some event at some point in the past, i.e who did this or that, or who was here or there. In this sense, identification is generally re-identification — and this requires memory, i.e. some form of (individual, institutional or technical) remembering. In turn, this it what drives monitoring and documentation — for future re-identification.

Linkage, or linkability more generally, and its undesired implications for people's fundamental rights and freedoms are the subject of existing legislation: the criteria for the applicability of the GDPR is that personal data is being processed. Pursuant to Article 4 no. 1 GDPR, personal data is any information relating to an identified or identifiable natural person, i.e. information that is linked or can be linked to that person. In that sense, anonymisation, which allows for leaving the GDPR's scope of application, is the act of permanently de-linking data from identifiable people.

De-linking is an ambivalent operation — and unlinkability is an ambivalent state — both with regards to the GDPR and beyond: on the one hand, it is considered a protective measure, e.g., it protects people from linking data or results of data processing to them. On the other hand, it can prevent or render significantly more onerous the exercise of rights, e.g., if their exercise depends upon the very linkage to something, be it an event, an act or an identity. Whether de-linking can be considered a protective measure or a threat also depends upon who the actor is that controls the de-linking, who is affected by it and what the implications are.

This raises multiple questions: how can an identity (including its linkages) be changed, by which actors and in which contexts? The frameworks governing these directly impact multiple central aspects of how identities evolve over time, such as mutability, renewability, or deniability. To start with, mutability corresponds to the possibility (or not) of changing certain aspects of the identity. This varies depending on the aspect and the sociocultural context. For example, the only requirement for a legal name change in most US states is to use the new name[10] publicly (which was the main identifier before the creation of the centralised social security number database in 1936) [Kus09]. At the other extreme, since the 19th century, fully changing one's first name in France can not truly be done: the master records are amended to add the new name while keeping a trace of the entire name history. In this case (and concerning more than just names), the state claims ultimate power as the keeper of identities, which can be partially amended only in the explicit cases the state allows (such as getting married), by following its procedures and with its consent[Lem02]. However, the person's consent is not always necessary, and states have claimed the power to unilaterally change some identity markers (such as enforcing name changes for DACA immigrants in the USA in the last decade) [San23].

Many platforms follow the same framework of unilateral control, and until recently sometimes did so without proposing any way to change identity elements. A common circumvention method was then to delete one's account and create a new one — renewing one's identity — or maintaining both simultaneously. This multiplication of identities requires some effort from the user, but the disadvantages are more often on the side of the platform. Renewability, on the other hand, might lead to individual or social costs, such as the loss of past achievements, credentials or access to one's own historical data. Unlike platforms, which generally do not have that power, states enforce the use of a singular identity — which is rarely renewable (with the partial exception of witness protection programs) — to prevent this kind of problem from occurring in the first place. To balance platforms' interest in enforcing singular identities and users' counter-interests, states may choose a middle option, as the European Parliament's report on the EU Commission's proposal for amending the eIDAS Regulation as regards establishing a framework for a European Digital Identity[11]

[10] Despite the ease of changing one's name there, homonyms have a sometimes humorous prevalence [GGGG15].

[11] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final

suggests: issuing immutable identities, but allowing for the creation of renewable or mutable partial identities (i.e. composed of subsets of attributes), for use towards third parties[12].

Deniability denotes an actor's ability to prevent another actor from provably, plausibly or credibly linking certain observed actions or events to them. It depends both on the relationship between the actors and the requirements for proof, plausibility or credibility, e.g. in a court of law or one of public opinion. If linkage is prescriptive — i.e. some actors have the power to stipulate it — it is hard to speak of deniability as a denial would be trumped by the stipulation of a more powerful actor. Deniability is also not symmetric. It depends greatly on who is denying something to whom — it makes a difference whether it is an actor denying elements attributed to them (such as participation in events or identity) or a second actor denying elements attributed to someone else[13].

Identity theft, or identity fraud, thus denotes the ability of an actor to successfully link their present to someone else's past towards a third party, be it an individual, an institution or a system. Typically, systems are required to prevent such false re-identifications, but what actually matters is which actor is disadvantaged by the identity theft. For example, the original identity-holder, often simplistically called the identity theft's victim, can be complicit, either intentionally or unintentionally[14].

Thus, mutability, renewability and deniability of identity can be both liberating and constraining, empowering and hindering.

2.5 Security ecosystems

The earliest aspects of modern cybersecurity can be traced back at least to the early 1960s [MT79]. However, some important sociotechnical aspects had received relatively little academic attention until the early 2000s and are still poorly known in the industry. Indeed, no security system can be fully analysed as an isolated technical object. Instead, a thorough analysis must take into account the complex ecosystem around the system — which can include the original developers, users, but also other security systems. Naturally, no security system can guarantee a user's security if their password is "password". Instead of blaming the user, recent work has sought to understand how different design decisions contribute to this kind of behaviour and where the real loci of responsibility and power are [WRBW16]. As stated in section 2.1, the last two decades have normalised the multiplication of accounts, and, as such, of authentication systems. This creates a very high usability cost for users unless they choose between the following:

- authentication re-use (whether it's the same password or the same fingerprint);
- a centralised authentication system (e.g., a password manager).

Whereas the latter can constitute a single point of failure, the former makes all the user's accounts vulnerable. A whole array of attacks — password stuffing, biometric replay, etc. — rely on reusing data from previously-breached authentication systems to breach a second system. These systems can sometimes be breached and the user's information stolen without the user's behaviour having any impact. Even a user who is aware of vulnerabilities might not have any way of resolving them[15]. This creates a complex incentive structure where users do not have a strong motivation to improve their personal security practices as it can be irrelevant in the end. Moreover, one should remember that some actors can be malicious. One could even set up a free service or app that requires a password or biometric information and whose main purpose is to harvest such information for replay attacks — where someone's information from a previous authentication attempt is reused to illicitly gain access elsewhere.

[12] According to the European Parliament, European Digital Identity wallets are supposed to include a functionality to generate freely chosen and user managed pseudonyms, which can be specific for individual sites, platforms or services, to access them through the use of these pseudonyms. See `https://www.europarl.europa.eu/doceo/document/A-9-2023-0038_EN.html`.

[13] Hannah Arendt's concept of an unalienable "right to have rights" [Are51] is what crucially links this second direction of deniability to political power.

[14] There can be reasons for intentionally allowing someone else to do this, including political reasons, e.g. sharing an unlimited bus pass, or some credential with undocumented immigrants.

[15] An interesting case can be found in the 200M$ lawsuit between Michael Terpin and AT&T over the company's failure to secure his account with 2-factor authentication despite his requests after he noticed hacking attempts, and the subsequent theft of 24M$ in cryptocurrencies (see Terpin v. AT&T Mobility, LLC, Case No. 2:18-cv-06975-ODW (KSx)).

Thus, any analysis of a security system should include its dependencies — are there other systems whose breaching could induce a cascading failure — and whether it can itself be the source of further problems if breached. It should also take into account the fact that both the development of practical systems and the elaboration of security norms and standards generally involve a compromise between public and private economic interests, national security considerations and the defence of individual rights[16].

3 Technical solutions for authentication

Despite the impressive advances concerning the development of authentication mechanisms over the last three decades, similar progress has been made in attacking such mechanisms and spectacular vulnerabilities frequently make the news. We have also seen a complex struggle on their appropriate uses. On the one hand, authentication requests have seen an increasing use, originally linked to the multiplication of online accounts but which could continue with the Internet of Things (IoT). On the other hand, there have been multiple attempts to reduce user friction by centralising such mechanisms, often around trusted devices and services (password managers, single sign-on, and more recently the efforts of the FIDO alliance as detailed below). It is impossible to predict how this situation will evolve in the long-term, yet we must still grapple with this technological evolution and its legacies to address their legal ramifications. As such, this section will not focus on giving a state of the art of existing technical solutions but rather an understanding of the underlying principles and the constraints that apply to deployed authentication systems.

3.1 Many factors of authentication

Although passwords are the oldest and most common online authentication mechanism, many alternatives exist, which can be broadly categorised. Each focuses on a different type of underlying *secret element*: something you know, something you have, something you are, or something you do — with the last two sometimes being considered a common category[17].

These are often referred to as "authentication factors". The first and most common correspond to "something you know": information that only the user is supposed to have such as PINs, passwords, or answers to challenge questions. These modalities have one central feature from which stem its different advantages: it is composed of raw information. This makes it flexible: easy to modify, renew (if it gets stolen) or share with trusted parties. However, its resistance depends on the user's ability to keep it secret and unique, making it potentially easy to copy and limiting its usability. Conversely, "something you have" is not information but very material: physical keys, smart cards, USB drives, and nowadays most frequently smartphones. They are harder and costlier to steal, but easier to lose. The last factor, "something you are/do", depends on a specific biological attribute that is ideally unique to the person: fingerprints, facial shape, voice or gait. This is more material than the first while being harder to "lose" than a physical object. Their central concern is that if a high-quality copy is made, this modality is irreparably compromised.

As such, no factor or modality is strictly superior to others as it fundamentally depends on the attack model. Each has advantages and weaknesses, which can sometimes be addressed by combining them.

Combining modalities means adding a second layer of security, which can be done in two ways: *two-step verification* or *two-factor (or multi-factor) authentication.* The two concepts are often used interchangeably but have real differences. Whereas the first type allows the repeated use of a single factor (e.g., password plus PIN), the second requires a combination of different factors, such as password and fingerprint. Combining the latter two, for example, can give stronger resistance to both generic online attacks and to getting one's device stolen (although each factor is vulnerable to one of these). This improved security generally comes with usability costs, with passwords being a central friction point, hence the push to get rid of this modality.

However, for two-factor authentication to truly be more secure, two critical elements must be respected. First, as said before, they must be not just different modalities but of fundamentally different type (hence,

[16] Sometimes, the interplays are complex: a state might want to help the development of a given strategic industry — such as voting technology — to avoid being dependent on other states, even if its security is not on par with international standards.

[17] This consideration stems from the fact that it is not exactly "something you do" but rather "something only you can do" and mixes intrinsic elements of the body with conscious actions, constituting a linkage between your body and a record of your past performance.

different factors). This eliminates combinations such as password + PIN or retinal scan + voice recognition. Second, each factor must, independently, guarantee some security and thus not just be a *different factor* but also a secure one. This goes against the interpretation of the French Cour de Cassation (supreme non-administrative court) in Decision n°20-17.073 from November 24, 2021, in which the Court stated that the existence of multiple modalities was in itself a sufficient security guarantee. The modalities — which governed access to an online service for professional elections — were the employee's full name, date of birth and their city of birth. Neither of these are secure as they are all obtainable with minimal effort, especially to anyone working for human resources[18].

Finally, multi-factor authentication cannot be, by itself, a full solution, due to the complex interplay of security ecosystems. As with state-issued identification documents, nearly every authentication system has a way to reset account access if some elements are lost — otherwise the risk that clients would lose their property or data would be too high[19]. As such, the bypass/override mechanisms can be a more tempting target, which is what happened in the Terpin case mentioned in footnote 15, in which hackers impersonating Michael Terpin made AT&T employees bypass the security code, giving them access to the victim's phone. The court also found AT&T not liable as their privacy policy stated that they did not guarantee that personal information would not be disclosed in a manner inconsistent with AT&T's policy. Multi-factor frameworks then make up just one element in the security toolbox, which relies heavily on both the security of the underlying cryptographic building blocks — such as the system used for each different factor — and that of the potential override protocols. The next subsections will then address the current state of the art in terms of passwords, material solutions and biometrics.

3.2 Informational and material solutions

One of the most popular ways to restrict access historically is through the use of a password (or similar knowledge-based solutions like PIN codes, passphrases and challenge questions). Due to their increased use, they have been the object of numerous studies and many conflicting and often counterproductive guidelines. A central explanation can be found through the analysis that passwords are affected by multiple conflicting interests. Most users generally try to minimise their efforts, whereas companies try to offload some of the security cost onto users through password policies. Finally, economic incentives push companies to skimp on security, as it is perceived as a cost with no immediate gain, and developers are pressured to focus on other elements [AFM16, ABF$^+$17].

Because of this, passwords suffer from two main security issues. The first is that they are rarely stored securely: even Facebook was found to have stored them unencrypted in 2019 [Kre19]). Ideally, passwords should never be stored as they are but should be *hashed* first: that is, transformed by a mathematical function until it becomes impossible to retrieve the original. Moreover, even when they are hashed, specific hash functions (such as Argon2 with salting) should be used to prevent bruteforce attacks, which is almost never the case in practice [JPG$^+$16], and the non-hashed password should never reach the server in the first place [Bla22]. Disregarding these best practices allows anyone with access to the database to spend computing power to find the correct credentials, which they can then reuse elsewhere.

This is related to the second security issue, which is that users seldom choose secure passwords, and tend to reuse them in many places — as the multiplication of accounts makes memorisation of distinct passwords nearly impossible. Moreover, attempts to prevent this — such as password policies mandating frequent changes or the use of special characters — often become counterproductive. Indeed, they push users to develop an adversarial relationship with the system and seek to avoid the extra costs involved, for example by adding '&1' at the end of their passwords, which does not improve the security [SKD$^+$16].

Password managers were created to address this by locking a set of secure passwords that the user need not memorise behind a master password that generally stays on the user's device. To address different frameworks but in a similar vein, some companies have proposed Single Sign-On (or SSO), whereby a user

[18] The Court stated that the fact that an employee shared their main secret information (the "city of birth") on purpose meant that it was akin to identity fraud as the employee could just as well have shared a password and that the latter would not have been more secure. This ignores the fact that it is easier to guess or ask someone their city of birth discreetly than to obtain their password.

[19] A major exception to this comes from cryptocurrencies, and as such it is estimated that close to 20% of all bitcoins have been lost (because their owners lost their keys), representing more than 100 billion dollars at the time this article is written.[Pop21]

follows a single account's authentication, and the service provider for that account confirms their identity to other online services. In consumer use, SSO frequently depends on major tech actors (such as Facebook or Google). This reduces the multiplicity of accounts (and passwords), and can improve security if the main service provider's competence is higher than average. Both SSO and password managers' strengths come with drawbacks, mainly the presence of a single point of failure : if an attacker manages to get a user's SSO credentials (e.g., by phishing), they gain full access to all the dependant accounts. Depending on how the secondary services are set up, the attacker could keep access to some secondary accounts even if the main access is revoked. Moreover, this single point of failure could also mean that the user loses access to all their accounts if they lose their SSO (or the device with their password manager if they only have one). A secondary concern is that, by locking every service behind the same security system, a user can be pushed to use their SSO for basic tasks, potentially on an unsecure device or network, increasing their exposure to hacking by requiring more privilege than necessary [Kna17].

As long as one depends on a given device — such as the one with the password manager when it is not hosted in the cloud — this device can just as well be used as an authentication mechanism itself. Smart cards, security tokens, or even specific chips (or software) in smartphones can play that role. They often integrate secondary security and are used for multi-factor authentication, such that stealing the device is not enough to gain access to secure accounts. This is useful when securing high-value systems, where preventing unauthorised access is more important than guaranteeing access to all legitimate users. Because of that same single point of failure, these methods make it very easy to lose one's accounts in case the device is lost, stolen or broken. Passkeys — digital cryptographic credentials developed by the FIDO alliance and the W3C to be compatible with a variety of systems — are one of the more recent developments, and in their latest incarnations mix some of the techniques mentioned above to improve availability [Cam23].

All the solutions mentioned above propose compromises between usability, dependency and security. At great cost, a user could manage all their passwords themselves in their memory and thus avoid being dependent on either a device or a service provider. They could also have everything in their phone and risk permanently losing access to their accounts if their device breaks down. Or they could delegate some trust to an online service which could guarantee access even with lost credentials (by providing a state-issued proof of identity) but be dependent on that service and give them access to their data (even if they should legally not access it), become partially locked into that service's ecosystem, and depend on that service not suddenly disappearing. The next subsection will cover the last main option that has been proposed trying to bridge the gap between the user's limited memory and the refusal of external dependencies: biometrics.

3.3 Biometrics

Biometrics' early history starts with fingerprints, employed by Babylonians to sign transactions more than two millennia ago.[Ash99] It acquired the status of modern science with Alphonse Bertillon's work at the turn of the 20th century, through the introduction of a groundbreaking biometric system based on precise body measurements with the aim of transforming criminal identification. It then became automatised with Mitchell Trauring's electronic fingerprint recognition system. [Tra63] Initially confined to military applications and high-security sectors such as banking, it finally expanded to various sectors over the last three decades: hand geometry to access the 1996 Olympic Village [BGF12], Malaysian passports in 1998 [JMW05], and most recently mobile devices. The first smartphones to feature biometric authentication was the Fujitsu F505i in 2003 [GHCL14], but the technology only became mainstream in 2013 with the iPhone 5S, to the point that it is now used by close to half of all worldwide smartphone users [RLG18].

All biometric authentication systems are based on the recognition of a given physical feature. However, not all features can work, as three main aspects come into consideration. First, the feature should be highly unique, allowing reliable differentiation between individuals: even identical twins have varied traits (such as fingerprints) due to developmental differences. Second, the feature should be stable over time and in different contexts: it should exhibit "permanence". While certain characteristics may change slightly with age, they should still have enough distinguishing characteristics to allow for authentication. Finally, the feature should be universal: observable and measurable in every person. This is not truly the case for existing biometrics: some of the features used such as fingerprints or irises are only present in an overwhelming majority, but not the totality, of humanity[20].

Taken broadly, the goal of the authentication system is to capture the feature and compare it to a reference in the database which was captured at enrolment. Although a biometric feature should ideally be stable and permanent, it is never truly the case. Facial patterns, voices, fingerprints and even DNA accumulate minute changes over time. Moreover, the sensors used to measure the individual have an inherent imprecision, which is compounded by variations in context: luminosity and camera angle for facial recognition, temperature and humidity for fingerprints, but also how well-rested the individual is (which slightly affects many features). The capture and the reference are never identical, and the system must calculate whether the two datapoints are close enough that they probably correspond to the same individual (depending on the error threshold set initially). Thus, the handling of errors is a central aspect of biometric authentication.

These errors come in two different types: false acceptance errors and false rejection errors. The first one occurs when a someone is mistakenly authenticated as a different user, which stem from factors such as system malfunctions, poor quality data capture, or inadequate matching algorithms. For instance, McCulley and Roussev found that they could spoof some *typing biometric* systems and authenticate as any user in at most a few tries, indicating an extremely high false acceptance rate (FAR) [MR18]. Conversely, false rejections can be caused by changes in the user's biometrics, fluctuations in the environment, or restrictions in the enrolling procedure. A system which repeatedly locks out legitimate users would then have a high false rejection rate (FRR). No biometric has a single intrinsic error rate (and even the very notion of error rate can be debated [Dro20]). Rather, the rates naturally depend on the threshold at which the matching algorithm considers the two datapoints sufficiently close. By lowering the threshold, one improves FRR at the expense of FAR, and vice versa. To allow for easier comparison between biometrics, it is then common to use cross error rate (CER, or EER for equivalent error rate), which corresponds to the value at which FRR equals FAR. Hence better biometric authentication systems generally have lower CER (although the entire error curves matter). To compare this with passwords and PIN codes, the FRR cannot be easily estimated (as it depends on the user's memory) although it has been studied [PJGS12]. However, the FAR is easy to compute: the probability of getting a random 4-digit PIN code right is 0.01% per try (and about one in 10 billion for real world passwords [BSB18]). This is low compared to standard biometrics, but it is easier to repeatedly try PIN codes than presenting new faces, thus a common solution in both cases is to implement *rate limiting*, where one cannot repeatedly try to authenticate with no delay between tries.

As the system has to compare the new capture with a reference from the database, new issues arise. First, there is a risk that the stored data could be stolen, as with Biostar 2's stolen database[21] of more than 1 million fingerprints and face recognition data (including that of people with security clearances). This kind of breach enables attacks based on reusing stolen credentials. However, unlike with smart cards or passwords, it is generally not possible to lock out an account until a new password is set up. The very permanence of the biometric feature makes it persistently unsecure if it is ever leaked — for both the original authentication system and any that uses the same feature — and as such is affected by multiple articles of the European General Data Protection Regulation. To make data theft harder, a common technique is not just to encrypt the feature but to transform it in such a way that it should be impossible to retrieve the original data, while leaving open the possibility of comparing the reference to new captures. However, unlike password hashes, the fact that we seek to compare noisy data makes it harder to establish the irreversibility of the data transformation (and some methods that were considered secure turned out to be vulnerable) [DJJ19].

Even if all companies encrypted the biometric data during transit and stored it securely, this would not prevent some actors from creating apps with the explicit goal of harvesting this data from users. However, this would not even be necessary, as biometric data can sometimes be stolen or reconstructed from public sources. Ursula von der Leyen famously got her fingerprints reconstructed from a picture while she was Germany's Defense Minister [GKL$^+$22]. Similarly, videos uploaded to social media could be a good source for hackers to target their victims' biometric data [GKL$^+$22]. This stolen data can be used to gain illegitimate access in a variety of ways, such as presenting a photograph, video or a silicone mask to the camera — known as spoofing biometrics or presentation attacks [MNL14]. The main existing method to prevent these attacks

[20] This creates two different issues: first, some disabled individuals could be prevented from using the system — which can be catastrophic if it aims to become universal and mandatory, as for national identification documents. Second, an individual who suddenly becomes impaired in such a way would be cut off from their access to many services, compounding their issues.

[21] `https://www.vpnmentor.com/blog/report-biostar2-leak/`

is called liveness detection. It relies on multiple techniques (both hardware and software) and often on other biometric modalities, to ensure that the data presented is not a recording but comes from a live user [KWR20]. However, this method is not foolproof, and there is an ongoing arms race between better liveness detectors and better presentation attacks.

In practice, nearly all biometrics[22] belong to one of two groups: physiological or behavioural (roughly corresponding to "what you are" and "what you do"). The first one makes a (generally static) capture of a biological feature. These characteristics, such as fingerprints, iris patterns, hand geometry, face features, are the most unique to each individual and challenging to imitate. Thus, within biometrics, these options generally offer the highest security and lowest error rates. Fingerprints, probably the most commonly used biometrics, typically have CER ranging from 1% to 2%, but are also most easily stolen [CTI+18]. Iris recognition — based on the unique arrangement of fibres and pigmentation — requires more specialised equipment (and is less usable) but generally has lower error rates, ranging from 0.01% to 1% [CTI+18]. Facial recognition is more complex, as it occurs both in authentication biometrics and in person identification (e.g., for criminal reasons through security cameras). It is also one of the biometrics whose performance is highly context-dependent (e.g., because of lighting, camera angle, but also makeup). Although many systems have error rates varying from 1% to 5%, FAR as low as 1 per million have been claimed (notably for Apple FaceID) when it comes to authentication [fac17, TKD+20]. It is also highly contentious due to dataset disparities and accusations of high error rates on subgroups targeted by the police [Per21].

Behavioural biometrics offer a more diverse range of options, as they leverage unique patterns in how individuals interact with systems and devices. This opens up possibilities for using various modalities such as gait recognition, handwriting recognition, mouse dynamics, touch dynamics, and more. One significant advantage of behavioural biometrics is their renewability. Unlike physiological biometrics, which remain relatively fixed throughout a person's life, they can be updated or retrained as users evolve their interaction patterns or as devices change. This adaptability allows for greater user flexibility. However, it's important to note that behavioural biometrics typically have higher intrinsic CER due to factors like variations in conditions or inherent behavioural fluctuations, as well as fatigue. This means that their error rates often go from 5% to 20% — for example, keystroke dynamics have a typical CER close to 5%, whereas electroencephalography often reaches 20% [CHDZ21, DMC16, WWH22]

3.4 Replacements

The increasing acknowledgement of passwords' vulnerabilities has spurred many attempts to eliminate them, with their incoming disappearance claimed as early as 1997 [Poo97] and at most every few years since, with biometrics always considered a strong contender [Kim95]. The most recent efforts — and the first ones to have a real measure of success — come from the FIDO Alliance, a consortium made up of nearly all tech giants as well as VISA, Samsung, CVS Health and many others. Their primary goal is to replace traditional passwords with more secure and user-friendly alternatives — in the goal of reducing ecosystemic vulnerability (and potentially their own liabilities). They seek to standardise many elements, from smart cards to biometric factors. Although laudable, one must warn that some of their proposals have inherent limits. For example, their highest biometric certification is represented by an FAR of 0.01% for an FRR below 5%. They allow further testing (but not certification) down to 0.001%, and the lowest claimed FAR the authors are aware of is 0.0001% (Apple's FaceID) [SS23]. This is low but not enough to provide foolproof security, even in the absence of presentation attacks. As such, it might not be on par with other authentication methods also included as alternatives by the FIDO Alliance.

Biometrics could then more reasonably serve as a first line of defence, not sufficient by itself but providing some basic security and reducing the need for passwords and other security measures to where they are needed (e.g., for banking but not to access a newspaper's website). As such, it seems a fool's hope to expect a system entirely based on them, but they probably have a role to play. Overall, it is likely that the future of security will rely on a mix of different methods, including biometrics, combined with other solutions to offer an optimum level of security while maintaining the security/usability balance.

[22] All deployed biometric authentication systems fall into these categories. However, some theoretical options have been proposed that mix biometrics with challenge questions to measure the user's physiological responses — such as pupil dilation. This would come at a higher usability cost, but give be more resistant to data theft and credential reuse.

4 Discussion

As Western understandings of identity have allowed for more fluidity, the very notion of identity has been a focal point of cultural tension, one that shapes and reflects power relationships among state actors, populations, and private companies. Identity documents do not simply reflect their bearers' identity, but are the materialisations of these power relationships. The categorisation underlying these documents, and the practices that shape them, reflect the world views, fantasies, stereotypes, and prejudices of the institutions and people who create them [Gro07]. As a result, these identification documents also have a significant impact on the formation of their bearer's identity as well, i.e. how they identify themselves — as individuals, as members of groups and in relation to others and society. Thus, identity documents create, ascribe, impose and transform identity as much as they document it.

When it comes to digital identification systems, different groups hold distinct expectations regarding their functionalities and deliverables. The anticipated outcomes of such systems span a variety of dimensions. Some groups may expect access to be shareable — as is widespread with travel cards or entertainment accounts. Similarly, opinions vary on whether individuals should be traceable or remain non-traceable. While operators usually opt for the former, users tend to prefer the latter. The issue of privacy also divides stakeholders, including the question of what privacy actually means on the ground [MKD16]. But most importantly, the very necessity of authentication itself is a subject of debate. The design of these systems is guided not by the expectations of stakeholders alone, but by the power differentials that exist within society and especially between the stakeholders of the very systems that are to be developed. Identity itself can emerge from the links made in these systems, giving vast power to those who can decide how such links are made, maintained or made public. Consequently, the question of power becomes intertwined with system design, shaping the intricate relationships between system designers, users, regulators, and various other entities involved.

Although computational and legal systems have similarities, they also have some major differences. One of these is that, if a contradiction or an error is found in a legal system, it can be fixed by the courts or the legislators, with its impacts generally limited to those directly affected by the error. Despite this, the complexity of updating these legal systems to address non-normative identities is already used by some courts to deny rights to certain minorities, independently of the merit of the underlying claim[23]. However, translating this to the digital realm carries multiple risks. A system suddenly expected to handle non-normative identities — or forced to by a legal evolution — could have cascading failures and potentially break access not just for the non-normative individuals but the whole population. It is thus essential to acknowledge the implicit elements and side-effects that arise from digital identification systems, including from the underlying conceptual and technical framework, regardless of whether they are intentional or not.

This question is both technical and highly political due to its normative aspects: each system of authorisation inherently acts as a system of exclusion, imposing implicit and explicit assumptions about what constitutes the normative bodymind. These assumptions can have far-reaching consequences, affecting individuals who may deviate from the established norms, and perpetuating societal biases. Additionally, biometric assumptions related to the presence or availability of limbs, such as fingers, or specific characteristics, such as friction ridges on fingers, and behaviours further complicate the ethical and political landscape surrounding these systems.

Consequently, there is an ethical imperative, and to some extent (e.g. via the GDPR) a legal duty to thoroughly consider these aspects when implementing digital identification systems. It might certainly be called a duty of care. It first of all applies to scientists, as they should always embrace critique as an integral part of the scientific process, allowing for continuous improvement and avoidance of unintended consequences. But it also applied to practitioners and decision-makers, those who design and implement both legal and technical systems, who write laws and code, and thus shape how we may experience the world [Hil08]. They must take into account the implications of their underlying assumptions, their specific design decisions and implementation details as well as how these digital identification systems will be embedded in social contexts. They must also carefully manage the many conflicting interests and imperfect information, without falling for

[23] For example, the French Cour de cassation rejected an intersex individual's request to indicate "neutral" or "intersex" on their birth certificate — despite agreeing that the individual did not fit as either male or female — motivating it partially by the impact such a decision could have on French legal frameworks as they are based on a sex binary (Cour de cassation, civile, Chambre civile 1, 4 mai 2017, 16-17.189).

techno-solutionism or the easy comparison between existing imperfect systems and idealised solutions (whose drawbacks often appear only when implemented). No perfect protocols exist that guarantee the respect of all stakeholders, individual and collective rights (especially not if efficiency is the goal). Indeed, all such systems risk leaving some minorities aside, all the more so if they are mandatory and not opt-in — although the latter can have similar consequences due to a degradation of service. The first step is then probably to ask of any new system: if implemented with the same competence as existing systems, would it actually answer an unfulfilled need?

Acknowledgements

We wish to thank Malik Chapuis, Jessica Eynard, and Nils Heinemann for their useful comments.

References

Y. Acar, M. Backes, S. Fahl, D. Kim, M. L. Mazurek, and C. Stransky. How internet resources might be helping you develop faster but less securely. *IEEE Security Privacy*, 15(2):50–60, 3 2017.

Y. Acar, S. Fahl, and M. L. Mazurek. You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In *IEEE Cybersecurity Development – SecDev*, pages 3–8, 11 2016.

Hannah Arendt. *The Origins of Totalitarianism.* Schocken Books, 1951.

David R Ashbaugh. *Quantitative-qualitative friction ridge analysis: an introduction to basic and advanced ridgeology.* CRC press, 1999.

Miroslav Bača, Petra Grd, and Tomislav Fotak. Basic principles and trends in hand geometry and hand shape biometrics. *New Trends and Developments in Biometrics*, pages 77–99, 2012.

Enka Blanchard. Client-side hashing for efficient typo-tolerant password checkers. *International Journal of Systems and Software Security and Protection (IJSSSP)*, 13(1):1–24, 2022.

Luís T. A. N. Brandão, Nicky Mouha, and Apostol Vassilev. Threshold schemes for cryptographic primitives. Technical report, National Institute of Standards and Technology, 2019.

L Bošnjak, J Sreš, and Bosnjak Brumen. Brute-force and dictionary attack on hashed real-world passwords. In *2018 41st international convention on information and communication technology, electronics and microelectronics (mipro)*, pages 1161–1166. IEEE, 2018.

Mark Campbell. The road to decentralized identity: The techniques, promises, and challenges of tomorrow's digital identity. *Computer*, 56(6):96–100, 2023.

Ikkyu Choi, Jiangang Hao, Paul Deane, and Mo Zhang. Benchmark keystroke biometrics accuracy from high-stakes writing tasks. *ETS Research Report Series*, 2021(1):1–13, 2021.

Bismita Choudhury, Patrick Then, Biju Issac, Valliappan Raman, and Manas Haldar. A survey on biometrics and cancelable biometrics systems. *International Journal of Image and Graphics*, 18, 2018.

Xingbo Dong, Zhe Jin, and Andrew Teoh Beng Jin. A genetic algorithm enabled similarity-based attack on cancellable biometrics. In *2019 IEEE 10th International Conference on Biometrics Theory, Applications and Systems (BTAS)*, pages 1–8. IEEE, 2019.

Rig Das, Emanuele Maiorana, and Patrizio Campisi. Eeg biometrics using visual stimuli: A longitudinal study. *IEEE Signal Processing Letters*, 23(3):341–345, 2016.

Itiel E Dror. The error in "error rate": Why error rates are so needed, yet so elusive. *Journal of forensic sciences*, 65(4):1034–1039, 2020.

Danny Dolev and Andrew Yao. On the security of public key protocols. *IEEE Transactions on Information Theory*, 29(2):198–208, 1983.

Face ID Security. Technical report, Apple, 2017. `https://www.apple.com/business-docs/FaceID_Security_Guide.pdf`.

Martin Feuz, Matthew Fuller, and Felix Stalder. Personal web searching in the age of semantic capitalism: Diagnosing the mechanisms of personalisation. *First Monday*, 2011.

Allen C Goodman, Joshua Goodman, Lucas Goodman, and Sarena Goodman. A few goodmen: Surname-sharing economist coauthors. *Economic Inquiry*, 53(2):1392–1395, 2015.

Ming Gao, Xihong Hu, Bo Cao, and Dianxin Li. Fingerprint sensors in mobile devices. In *2014 9th IEEE conference on industrial electronics and applications*, pages 1437–1440. IEEE, 2014.

Anthony Giddens. *Modernity and Self-Identity: Self and Society in the Late Modern Age.* Polity Press, 1991.

Craig Gibson, Vladimir Kropotov, Philippe Z Lin, Robert McArdle, and Fyodor Yarochkin. Leaked today, exploited for life. Technical report, Trend Micro, 2022.

Valentin Groebner. *Who are You? Identification, Deception, and Surveillance in Early Modern Europe.* Zone Books, 2007.

Mireille Hildebrandt. Legal and Technological Normativity: more (and less) than twin sisters. *Techné*, 12(3):169–183, 2008.

Richard Jenkins. Categorization: Identity, social process and epistemology. *Current Sociology*, 48(3):7–25, 2000.

Ari Juels, David Molnar, and David Wagner. Security and privacy issues in e-passports. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks (SECURECOMM'05)*, pages 74–88. IEEE, 2005.

David Jaeger, Chris Pelchen, Hendrik Graupner, Feng Cheng, and Christoph Meinel. Analysis of publicly leaked credentials and the long story of password (re-) use. In *Proc. Int. Conf. Passwords*, 2016.

Hyun-Jung Kim. Biometrics, is it a viable proposition for identity authentication and access control? *Computers & Security*, 14(3):205–214, 1995.

Kenneth Knapp. Applying comprehensive least privilege: A framework for endpoint security. 2017.

Brian Krebs. Facebook stored hundreds of millions of user passwords in plain text for years, 2019.

Julia Shear Kushner. The right to control one's name. *UCLA Law Review*, 57:313, 2009.

Kavita Kavita, Gurjit Singh Walia, and Rajesh Rohilla. A contemporary survey of unimodal liveness detection techniques: Challenges & opportunities. In *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, pages 848–855. IEEE, 2020.

Jean-Jacques Lemouland. *L'identité de la personne humaine. Étude de droit français et de droit comparé*, chapter Le choix du prénom et du nom en droit français. Bruyant, 2002.

Deirdre K. Mulligan, Colin Koopman, and Nick Doty. Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 374(2083), 2016.

Sébastien Marcel, Mark S Nixon, and Stan Z Li. *Handbook of biometric anti-spoofing*, volume 1. Springer, 2014.

Evgeny Morozov. *To Save Everything, Click Here: The Folly of Technological Solutionism.* PublicAffairs, 2013.

Shane McCulley and Vassil Roussev. Latent typing biometrics in online collaboration services. In *Proceedings of the 34th Annual Computer Security Applications Conference*, ACSAC '18, pages 66–76, New York, NY, USA, 2018. ACM.

Robert Morris and Ken Thompson. Password security: A case history. *Communications of the ACM*, 22(11):594–597, November 1979.

Sidney Perkowitz. The bias in the machine: Facial recognition technology and racial disparities. *MIT Case Studies in Social and Ethical Responsibilities of Computing https://doi. org/10.21428/2c646de5*, 62272586(5):15, 2021.

Denise Ranghetti Pilar, Antonio Jaeger, Carlos F. A. Gomes, and Lilian Milnitsky Stein. Passwords usage and human memory limitations: A survey across age and educational background. *PLoS One*, 7(12), 12 2012. PONE-D-12-21406[PII].

Andreas Pfitzmann and Marit Köhntopp. Anonymity, Unobservability, and Pseudonymity – A Proposal for Terminology. In Hannes Federrath, editor, *Designing Privacy Enhancing Technologie*, volume 2009 of *Lecture Notes in Computer Science*, pages 1–9. Springer, 2001.

Ralph Spencer Poore. Passwords: Obsolete authenticators or cutting edge? *Information Systems Security*, 6(1):10–13, 1997.

Nathaniel Popper. Tens of billions worth of Bitcoin have been locked by people who forgot their key. (Published 2021) — nytimes.com. `https://www.nytimes.com/2021/01/13/business/tens-of-billions-worth-of-bitcoin-have-been-locked-by-people-who-forgot-their-key.html`, 2021. [Accessed 08-Jun-2023].

K. Suzanne Barber Rachel L. German. Consumer Attitudes About Biometric Authentication. Technical report, The University of Texas, 2018. `https://identity.utexas.edu/sites/default/files/2020-09/Consumer\%20Attitudes\%20About\%20Biometrics.pdf`.

Linda E Sanchez. Exclusion by design: The undocumented 1.5 generation in the us. *Frontiers in Sociology*, 8, 2023.

Bruce Schneier. *Secrets and lies: digital security in a networked world.* Wiley Publishing, Indianapolis, 2004. Paperback Edition.

James C. Scott. *Seeing like a state: How certain schemes to improve the human condition have failed.* Yale University Press, 1998.

Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip (Seyoung) Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Transactions on Information and System Security – TISSEC*, 18(4):1–34, May 2016.

Nils Tekampe Stephanie Schuckers, Greg Cannon. FIDO Biometrics Requirements. Technical report, FIDO Alliance, 2023. `https://fidoalliance.org/specs/biometric/requirements/Biometrics-Requirements-v3.0-fd-20230111.pdf`.

Philipp Terhörst, Jan Niklas Kolf, Naser Damer, Florian Kirchbuchner, and Arjan Kuijper. Face quality estimation and its correlation to demographic and non-demographic bias in face recognition. In *2020 IEEE International Joint Conference on Biometrics (IJCB)*, pages 1–11. IEEE, 2020.

Mitchell Trauring. Automatic comparison of finger-ridge patterns. *Nature*, 197:938–940, 1963.

Rick Wash, Emilee Rader, Ruthie Berman, and Zac Wellmer. Understanding password choices: How frequently entered passwords are re-used across websites. In *12th Symposium on Usable Privacy and Security – SOUPS*, pages 175–188, Denver, CO, 2016. USENIX Association.

Min Wang, Song Wang, and Jiankun Hu. Cancellable template design for privacy-preserving eeg biometric authentication systems. *IEEE Transactions on Information Forensics and Security*, 17:3350–3364, 2022.

Shoshana Zuboff. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books, 2019.