The Sociology of Personal Identification*

Jordan Brensinger
Columbia University

Gil Eyal
Columbia University

* We would like to thank Angèle Christin, John Torpey, participants of the Science, Knowledge, and Technology Workshop at Columbia University, along with the anonymous reviewers at *Sociological Theory* for incisive comments at various stages. Parts of this research were supported by the National Science Foundation (award #1921260). Direct all correspondence to Jordan Brensinger, Department of Sociology, Knox Hall, 606 West 122nd Street, MC 9649, New York, NY 10027; j.brensinger@columbia.edu.

The Sociology of Personal Identification

> Personal identity . . . has to do with the assumption that the individual can be differentiated from all others and that around this means of differentiation a single continuous record of social facts can be attached, entangled, like candy floss, becoming then the sticky substance to which still other biographical facts can be attached. What is difficult to appreciate is that personal identity can and does play a structured, routine, standardized role in social organization just because of its one-of-a-kind quality. – Erving Goffman, *Stigma* (1963:57)

Databases of personal information increasingly shape life experiences and outcomes across a range of settings, including consumer credit, banking, e-commerce, social service provision, policing, immigration, and health. Such processes depend on the ability to link data reliably to unique individuals. The novelty of electronic data collection and digital identities, however, should not prevent sociologists from recognizing the general sociological question these phenomena raise: *how, in a given society, can an individual be identified and reidentified as the same unique person and differentiated from others like her* (Caplan 2001)?

This question pertains to what Goffman (1963:63–64) calls *personal identification*, as distinct from *social identification*, which is about membership in categories such as class, ethnicity, or occupation. The two aspects Goffman associates with personal identification—uniqueness and self-sameness—however, deserve further scrutiny. First, uniqueness is about being able to tell one person from another—the degree of interchangeability of the focal individual with other individuals. This constitutes a continuum. Identifying by means of an address, for example, does not differentiate the individual from other household members (Marx 2016:334, n.14). A modicum of interchangeability remains, but identifying in this way still suffices for many purposes. Second, self-sameness pertains to recognizing an individual as the same individual previously encountered—the degree of biographical mutability permitted to the individual across situations. This too is a continuum. Facial features, for example, routinely serve

as a basis for identification, yet this tactic often requires extrapolation over the many ways appearance can change due to haircuts, makeup, plastic surgery, and aging.

Thinking about personal identification as ranging along these two cross-cutting continua opens it up as a sociological question in a way that terms like uniqueness or self-sameness do not. Uniqueness and self-sameness are better grasped as an organizing fiction, a "taboo" against explicitly treating individuals as interchangeable and mutable. For this reason, however, they do not give sociologists a handle on how personal identification operates in practice. Modern organizations do not expect people to keep the same address, or even the same physical features. They expect *something* to stay the same, but it is hard to pinpoint the exact nature of that something. Individuals can change their physical appearance or their gender. Their bodies may be transformed by accident or illness. The individual may die. Yet organizations may still need to identify the person (e.g., as the author of a will or subject of a territory) and so will continue to use the fiction that something remains "self-same" (see, e.g., Diallo 2021). Uniqueness and self-sameness are simply the expectation of a point at which mutability and interchangeability cease.

Goffman (1963) must be credited with first formulating personal identification as a sociological question, but his approach was limited by his self-admitted "ultimate interest . . . [in] develop[ing] the study of face-to-face interaction" (Goffman 1969:ix). Consequently, empirical studies of how passports, signatures, fingerprints, and DNA get constructed as markers of uniqueness and self-sameness (Alder 2018; Bechky 2021; Breckenridge 2014; Robertson 2010) rarely use Goffman's approach (but see Marx 2016). Despite the process's centrality to governance and social control, we still lack a general sociological approach to personal identification. How is the "assumption" of uniqueness and self-sameness constructed, and what

gives those imputed qualities their "stickiness" so that "a single continuous record of social facts can be attached"?

We propose a general framework for analyzing personal identification as a historically evolving organizational practice. The impetus for this theorization came from research Brensinger (n.d.) conducted on the resolution of identity theft. The main difficulty victims face often has less to do with the theft itself, and more with the recovery process, in the course of which they must reestablish and reauthenticate their links to official records. Why should individuals struggle to identify themselves to organizations? Why should recovery be harder than injury? This alerted us to the need to rethink the process of personal identification and to question the tendency in research on digital technologies to forecast a dystopia of inescapable and precise identification (Gandy 1993; Zuboff 2018). The difficulty of recovering from identity theft demonstrates the limits of such accounts (see also Christin 2020).

Our theory is informed by three types of data: (1) 106 in-depth interviews with victims and organizational personnel, including bank staff, government personnel, attorneys, and victim advocates, (2) participant observation at financial industry events, a nonprofit call center, and the fraud department of a large credit union, and (3) review of training materials, industry guides, and regulatory documents. We also draw on examples from a wide range of social scientific literature related to personal identification to discern generalities. The resulting sociological theory of personal identification offers a shared set of concepts for "sensitizing researchers' attention" (Zerubavel 2020:3) organized into three sections: the *object*, *agency*, and *technique* of identification. Together, our concepts direct scholars to important aspects of personal identification that often get overlooked, while also facilitating comparisons across cultural contexts, historical periods, substantive domains, and technological mediums.

Existing Theoretical Approaches to Personal Identification

The Durkheimian "Category of the Person"

This line of thinking about personal identification is as old as sociology itself. Durkheim ([1893] 1984) foreshadowed it in his speculations about "mechanical solidarity" and developed it further in analyzing the modern "cult of the individual" (Durkheim [1898] 1973) and "the soul" (Durkheim [1912] 2001). The clearest statement of the Durkheimian argument, however, appears in Mauss's ([1938] 1985) lecture on "the category of the person."

Just as the category of time possesses qualities (necessity, universality) that do not derive from the psychological awareness of duration, so there is a social category of the person that cannot be explained simply by reference to the psychological awareness of individuality (Mauss [1938] 1985:3). Both categories are the product of a process of slow, collective elaboration over millennia. They constitute means by which societies organize themselves, and are therefore amenable to sociological analysis. To underline this point, Mauss ([1938] 1985:4) begins with societies that, he argues, possess only "a limited number of forenames in each clan," each of which corresponds to an "exact role . . . expressed by that name." The accuracy of Mauss's analysis of Zuñi ritual does not concern us here. The main point is that he uses this example to relativize the taken-for-granted modern category of the person, this "fundamental form of thought and action" (Mauss [1938] 1985:22). He thus opens up personal identification as a sociological question. People today would struggle to think and act without assuming each individual is always and everywhere a unique and immutable person, but societies exist, Mauss ([1938] 1985:5) says, with only a "certain number of persons." The scarcity of forenames means that not all individuals are persons (women typically are not), some individuals are mutable—

they become several different persons over the life course—and others are interchangeable (through reincarnation) (Mauss [1938] 1985:6).[1]

Mauss's essay did not have much of an impact on sociology, no doubt because of the evolutionary schema Mauss used. Nonetheless, we take from it three points: first, personal identification constitutes a social form distinct from the subjective awareness of individuality; second, personal identification can be organized in different ways along the dimensions of interchangeability and mutability; and third, this organization is partly reflected in and partly determined by the technical means of identification (e.g., forenames).

Goffman's "Identity Pegs"

The beginnings of a true sociology of personal identification lie with Goffman (1963). The term "personal identity," he said, involves two key ideas. First, an "identity peg"—a "positive mark" like "the photographic image of the individual in others' mind," a personal name, or a fingerprint—renders the individual "identifiably different" from others, that is, non-interchangeable (Goffman 1963:56). Second, personal identity also involves the idea of a unique biography: "while most particular facts about an individual will be true of others too, the full set of facts known about an intimate is not found to hold, as a combination, for any other person in the world" (Goffman 1963:56). This unique combination of facts gets "attached to the individual with the help of these pegs," thus becoming the sticky candy floss "to which still other biographical facts can be attached" (Goffman 1963:57). The whole process is guided by the

[1] Where naming conventions dictate that individuals go by only a first name, as in contemporary rural Afghanistan, personal identification is strictly local. This highlights the peculiarity of the modern organizational expectation that an individual can be personally identified anywhere, regardless of local context.

assumption that whatever changes take place, "an individual can really have only one" biography (Goffman 1963:62), that is, her personal identity is non-mutable.

Unlike Mauss, Goffman does not simply describe the ideas contained in the modern category of the person, but analyzes some of the devices that turn it into a prevailing, taken-for-granted social reality. Yet, he takes some dubious shortcuts. The imagery of a "peg" seems to imply that some positive marks—"unchanging biological attributes such as handwriting or photographically attested appearance"—are inherently individuating: "Once an identity peg has been made ready, material, if and when available, can be hung on it" (Goffman 1963:57). This is not convincing. Even putting aside the peculiar characterization of handwriting as an "unchanging biological attribute," the main difficulty in personal identification is not devising an identity peg, but deciding whether particular, situational "material"—a signature, a photo capture at an ATM, a transaction—should be "hung" by means of this "peg." This explains why identity theft victims struggle to resolve their cases, even though their "pegs" have presumably "been made ready." Goffman, that is, glosses over the specific nature of the *techniques* of identification developed by organizations (see also Marx 2016:102). These techniques, and not the identity peg itself, give the candy floss of personal identity its sticky quality.

Accordingly, we will demonstrate that these techniques are best understood as forms of *testing*. This is, in fact, not all that far from Goffman's (1969) later argument about what he calls "expression games." Expression games consist of moves and counter-moves, where one side attempts to glean the true intention and nature of the other's expression, and the other attempts to control what can be learned from it (Goffman 1969:11–23). The "uncovering move" takes the form of a series of tests: "One standard uncovering move is to perform an examination of some

kind. Some examinations focus on the track that the subject leaves. . . . Others involve some form of interviewing and require his presence . . . [others] attempt to monitor the subject when the latter feels he . . . need not cloak his behavior" (Goffman 1969:18). We build on Goffman's analysis, but we also find the framework of a two-party "game," illustrated with examples drawn from the worlds of espionage and policing, quite limiting. Goffman (1969:74) himself notes the need for a "three-party analysis," but he does not follow through. One of the main contingencies in personal identification, as we shall see, is how to coordinate the uncovering moves taken by experts in the backstage with the interests and constraints of lower-level staff interacting with clients at "access points" (Giddens 1990). Accordingly, we will demonstrate that the *agency* of identification is best understood as a far-flung and internally complex *network*, wherein different *coalitions* become possible.

Goffman (1963:72) takes another shortcut in implying that once a "continuous record of social facts" has been created, it possesses an inherent self-sameness—"some kind of single biographical structure"—that will continuously accommodate additional biographical facts. He describes a man on his "daily round," coming into contact with individuals who know him differently (e.g., as a father, employee, "regular" at the bar), yet he concludes that "the apparently haphazard contacts of everyday life may still constitute some kind of structure holding the individual to one biography, and this in spite of the multiplicity of selves that role and audience segregation allow him." We find this also unconvincing. The characteristic Goffmanian focus on face-to-face interaction overwhelms the analytic question. In other works, Goffman (1955, 1971) described face-to-face interaction as subject to strong ritual rules that require participants to uphold the "face" that others present and "repair" any seeming inconsistencies in their biography.

Self-sameness, the stickiness of the candy floss, would thus be guaranteed by this tacit, yet obligatory, repair work. Indeed, Goffman (1963:62 n34) prefaced the section on biography with a footnote acknowledging his debt to Harold Garfinkel, "who introduced me to the term 'biography' as used in this book." In his classic analysis of "passing," Garfinkel (1984:181–84) says he learned from Agnes's passing practices that self-sameness, or biographical coherence, constituted a contingent, practical accomplishment reliant on "unacknowledged help" of others in interaction. He notes how Agnes used euphemisms and platitudes strategically, counting on her interactants to find their meaning in the "texture of relevances" provided by the interaction. Yet as Goffman's (1969) own examples in "Expression Games" demonstrate, one cannot count on this generous repair work at the passport control desk or during a financial fraud investigation. In these situations, biographical coherence is not assumed but tested, with potentially dire consequences if biographical facts cannot be made to fit within "a single biographical structure."

Face-to-face interaction, therefore, does not offer a good model for thinking about personal identification. For this reason, we make relatively little use of the rich phenomenological literature on identification in face-to-face interaction. When individuals are in the presence of others, they use "recurring typifications . . . [that] form a semantic field of similar practical categorizations" (Tavory 2010:50 n3) to assign the other's social identity. Rarely, however, do they engage in the same interactional process to assign a personal identity ("excuse me, haven't we met before?"), let alone challenge it: "[T]he concealment by one individual of something he should have revealed about himself does not give us the right to ask him the kind of question that will force him to disclose the facts or to tell a knowing lie. When we do ask such

a question a double embarrassment results, ours for being tactless, his for what he has concealed" (Goffman 1963:64). Yet for many organizations, such tactlessness is *de rigueur*.

Goffman (1963:67, 70) did observe that the "recognition of personal identities" represents "a formal function in some organizations," and the "occupation of making personal identifications" constitutes the specialized province of bank tellers, criminal "cornermen," department stores' floorwalkers, police detectives, jail guards, and doormen. The examples he gives demonstrate that he still thinks in terms of face-to-face situations (the floorwalker memorizes what a shop-lifter looks like), but these occupations are much less committed to the ritual rules of everyday interaction. For them, the question of the individual's interchangeability and mutability elicits explicit concern and necessitates testing.

These few examples are presented without attention to the historical development and transformation of these practices. Goffman (1963:57–58) speculates that "personal identification of its citizens by the state will increase, even as devices are refined for making the record of a particular individual more easily available to authorized persons and more inclusive of social facts concerning him." But he offers no explanation as to why one can expect this, under what conditions, and with what variations and limitations.

Foucault, Deleuze, and "Dividuals"

In contrast, the historical emergence and transformation of techniques for personal identification are central to work on surveillance by Foucault, Deleuze, James Scott, Giddens, Gary Marx, and others. This body of literature offers several distinctive advances over Goffman and Mauss.

First, personal identification is analyzed as a historically evolving practice. Foucault, in particular, resists the tendency to reduce identification to the development of certain "ideas," as

Mauss seems to do, or to the needs of the state, as Scott (1998) does. Instead, Foucault's (2000:225) approach focuses on "practices . . . the hypothesis being that these types of practice are not just governed by institutions, prescribed by ideologies, guided by pragmatic circumstances . . . but . . . possess their own specific regularities, logic, strategy, self-evidence and 'reason.'" Unlike Goffman's unsystematic enumeration of examples, Foucault uses a conceptual grid (Foucault 1990:14–24; Veyne 1997) wherein the *object*, *subject*, and *technique* are "specific regularities" constituted by practice itself.

This framework will allow us not only to make structured comparisons but also offer a more balanced approach to the rise of digital technologies of identification. Some current analyses suffer from techno-centric amnesia, declaring the phenomena they study "unprecedented" (Zuboff 2018:12–14). As our discussion of something as mundane as house numbers will demonstrate, one cannot assume that the implications of digital technology obviously differ from those of paper technology. Instead, by focusing on personal identification as a historically evolving practice, our approach enables researchers to investigate how time-honored processes of recordkeeping and paper documentation extend into the present (Bouk 2015; Igo 2018; Lauer 2017), while also specifying the "new affordances" of digital technologies (Kellogg, Valentine, and Christin 2020).

What does it mean to deem the object of identification a "specific regularity" constituted by practice itself? Deleuze (1992) uses the term "dividual"[2] to signify that the object of identification is not the flesh-and-blood individual, but a manufactured object that is "less than"

[2] "Separate, distinct, divisible, divided among or shared by a number" (https://www.merriam-webster.com/dictionary/dividual).

the individual and stands in metonymic relation to her. The concept of "dividual" sensitizes us to the inherent and unavoidable gap between embodied individuals and their surveillance representations—a gap dramatized by recent reports of misidentification of minorities by facial recognition technologies (Hill 2020). Admittedly, Goffman's "identity peg" implies something similar, but the process by which such an object gets *manufactured* is almost completely absent from his analysis. In contrast, the surveillance literature describes a stepwise process involving, to use Giddens's (1990) terms, disembedding potential identifiers—names, faces, handwriting, fingerprints, house numbers—from their embodied or local context; transcribing them into data in a standardized, relational form that permits comparison; and reembedding them back into local contexts through interactions with organizational representatives (humans and non-humans) at "access points." The complexity of this process gives the lie to Goffman's throwaway remark about "unchanging biological attributes." It is this organizational process that endows dividuals with their identifying properties and infuses the candy floss with "stickiness."

Additionally, the complexity of this process offers a counterpoint to Goffman's (1963:57–58) confidence that "personal identification of its citizens by the state will increase," or to the tendency in research on digital technologies to forecast a dystopia of inescapable and precise identification (Gandy 1993; Zuboff 2018). The process of disembedding, standardizing, and reembedding dividuals is laborious, uncertain, and offers multiple opportunities for glitches, errors, resistance, and fraud (see Christin 2020; Liu 2021). This complexity helps explain the fact that increasingly precise identification comes coupled with the proliferation of fake identities (Read 2018), or that the most difficult aspect of identity theft is the cumbersome process of "recovering" from it (Cole and Pontell 2006).

Mauss sketched a historical process during which the "category of the person" acquired greater thickness and interiority. Goffman (1963:58) expressed confidence that organizations would produce identity pegs that are even "more fully inclusive of social facts concerning [the individual]." Yet, the concept of "dividual" suggests an almost inverse historical process. In the transition from a "society of discipline" to a "society of control," says Deleuze (1992:5), "individuals have become *dividuals*," that is, they have shed some of their qualities and become flatter and less comprehensive. The contrast he draws suggests a certain intrinsic limit or tradeoff that all practices of personal identification must negotiate.

Discipline in the Foucauldian sense traces an "enclosure" (Deleuze 1992:4)—the quarantined city, the army camp, the prison—within which a multitude gets transformed into identifiable individuals. Disciplinary practices lay out a spatial grid crisscrossed by lines of visibility meant to render individuals fully non-interchangeable. Additionally, disciplinary practices consist of detailed schedules and exercises that construct institutional biographies for these individuals, such that they remain non-mutable through all their prescribed movements (Foucault 1977:141–62). Yet Deleuze (1992:4) argues that disciplinary practices are fundamentally limited by the enclosure within which they operate. As individuals move from one enclosure to another, they "start from zero," or worse, disappear. Hence, Deleuze describes the emergence of a new practice of identification, which he calls "control." This practice dispenses with enclosures. Individuals move about relatively freely, but are enmeshed in a cybernetic loop, whereby their every movement generates new data, and every bit of new data modulates what they are permitted to do. He gives the example of a city where every movement gets recorded by means of an identity card the individual must carry at all times. As more data about the person is

collected, the control loop revises her terms of access to various parts of the city (Deleuze 1992:7). This control loop, says Deleuze (1992:4), operates "like a self-deforming cast that will continuously change from one moment to the other."

In disciplinary enclosures, individuals are identified by their place in a grid laid out in advance and are molded to fit a prescribed norm. The control feedback loop, in contrast, constantly recalculates the norm on the basis of new data derived from tracking and comparing individuals' behaviors. Consider how the Google algorithm works (Cheney-Lippold 2017:58–62). It infers probabilistic categories of social identity like race, class, and gender from a given pattern of online behaviors—namely, that one has a 51 percent chance of being a 65-year-old White female (but also a 33 percent chance of being a young Latino male)—and then iteratively revises these inferences while directing ads on their basis. As Cheney-Lippold (2017:65) says, this constitutes "allowable wrongness." It allows Google's identifications "to move, to reform the world into new, measured truths."

Although the argument about a historical transition from discipline to control is less convincing—credit ratings and life insurance index files exemplify "self-deforming casts," but date from the nineteenth century (Bouk 2015:62, n.24; Lauer 2017)—the analytic contrast Deleuze draws helpfully hints at an inescapable tradeoff between non-interchangeability and non-mutability. The disciplinary grid is cellular. It renders the link between each individual and the documentary record about them fully non-interchangeable, but at the price of limiting their movements to a prescribed track. Consider how at many hospitals, patients receive wristbands and their every movement, from intake through discharge, gets recorded. At discharge, however, patients cut their wristbands and disappear. The hospital may instruct post-patients not to consume alcohol after discharge, but it would be quite easy to evade any outpatient monitoring

regime. The very precision of a non-interchangeable link between individual and dividual renders it less useful for many other purposes. Many activities will be driven "underground" because none of the parties wish to be so identified.

Many organizations would thus prefer to build some "give" into the link, to accept some interchangeability in return for minimizing mutability. The quintessential example of this is the "cookie" that many websites install on our digital devices (Jones 2020). It moves with us and constantly revises the knowledge about us, but at the price of non-interchangeability, as there could be many different users of the same computer. Similarly, in Deleuze's example of the city, the identity card (and the corresponding set of records in the city's computers) constitutes a "dividual." It creates a continuous and non-mutable record of the movements of whoever happens to carry it. The same is true of the use of pseudonyms (e.g., when testing for AIDS), which "offer a compromise in which literal identity or location is protected while the need for . . . ensuring that the same person is involved when there are repeated interactions . . . is still met" (Marx 2016:103). It makes sense, therefore, to think of practices of personal identification as varying along a continuum where they strike different tradeoffs between interchangeability and mutability.

As we will suggest in the section dealing with the *agency* of identification, this continuum intersects with another tradeoff between *how much* is known about a particular individual and *who* is entitled to such knowledge. The more comprehensive the knowledge, the greater the pressure to limit the circle of those with access to such knowledge, and thereby to rebuild a certain degree of anonymity (Marx 2001:311–13). The combination of these two cross-cutting tradeoffs means the telos of practices of personal identification is not one-way toward a

future of precise identifiability. Forces also work in the other direction toward a certain degree of imprecision and anonymity.

A Framework for the Sociology of Personal Identification

The rest of this article offers a general framework for analyzing personal identification as a historically evolving organizational practice. It is organized around three key analytic categories—object, agency, and technique—each being a "specific regularity" constituted by practice itself. In the tradition of general theorizing (Zerubavel 2020), we flesh out the theory with a wide range of examples that transcend disciplines, cultural contexts, historical periods, and technological mediums. These examples derive from primary research on identity theft as well as existing literature.

Object

The object of identification practices is not the flesh-and-blood individual, but the "dividual," a manufactured object that is "less than" the individual. This proposition chiefly sensitizes sociologists to the inherent and unavoidable gap between embodied individuals and their surveillance representations. Take the case of identity theft. As Cole and Pontell (2006:128) suggest, "it is the repairing of identities and credit that constitutes the true horror of identity theft." It would be difficult to explain this fact without attending to the gap between individuals and dividuals. Why should individuals struggle to identify themselves to organizations? Organizations possess robust and ever more precise dividuals, but the links connecting these dividuals to physical individuals are fragile. Identity theft severs these ties and leaves individuals with the daunting task of translating—through dispute letters, affidavits, police reports—their lives back into the disembedded form of information legible to the organization.

Attention to the gap between individuals and dividuals is important because organizations typically seek to collapse the distinction between the two—to construct personal data as a direct representation of the fundamental qualities of embodied individuals. Yet, even with *biometrics*—data like fingerprints, DNA samples, and facial recognition ostensibly taken directly from the body—a gap persists between the dividual and the individual. Matching blurred and smudged "latent prints" to fingerprints on file, for example, requires substantial interpretation and fallible expert judgment (Cole 2001:175–76, 187–88). The fact that fingerprint experts often refer to some conventional standard (e.g., 16-point matching ridge characteristics; Cole 2001:201–205) underscores that a "match" is simply something that would be defensible in court (Bechky 2021).

Thus, even for biometrics it remains necessary to ask: how does the dividual become equated with the embodied individual? People and their lives do not come in the form of "data." Obtaining fingerprints, for example, involves an intricate technical process designed to produce a standardized transcription that can be compared with others (Nair 2021). Prior to this process, fingerprints possess neither uniqueness nor self-sameness. Looking at our friends' or kids' hands, for example, we would be hard pressed to tell them apart. Fingerprints acquire these qualities—or more precisely, acquire the ability to minimize interchangeability and mutability—through the work of a sociotechnical expert system. The work involves detaching potential identifiers from local entanglements (*disembedding*), building a robust set of "horizontal" associations to other disentangled identifiers in a way that minimizes interchangeability and mutability (*standardization*), and finally constructing a set of "vertical" associations between the resulting "dividual" and individuals in their local contexts (*reembedding*).

Disembedding. The first step in producing dividuals involves extricating potential identifiers from their substantive local meanings and reworking them so they can render local settings legible to a distant gaze (Scott 1998). Consider the case of house numbers. Not only do they furnish an instructive example of the process of disentangling required to transform the messiness of everyday life into organizational data useful for identification, they also serve as bedrock for further layers of identification. As Marx (2001:312–15) notes, locatability is a crucial dimension of identifiability. It does not help an organization much to know who the individual is if it does not know *where* she is.

Addresses do not inherently possess the quality of rendering individuals locatable to an organizational gaze. Prior to being numbered, houses bore the name of the family that resided therein. This practice posed no problem for locals, but it hindered the ability of central state officials to locate their subjects for conscription and taxation (Tantner 2009:9–10). Yet, merely assigning numbers to houses does not solve the problem, if the numbers remain entangled with substantive local concerns. Numbers had to be disentangled so as to be turned into data. One had to devise a numbering system that emptied numbers of their substantive meanings of *cardinality* (identifying the number of elements in a set, i.e., the number of houses in a village) and *ordinality* (identifying rank in a set, as when the Imperial Palace is house no.1), so they could play the role of stable and unique *nominal* indicators of location (Tantner 2009:23–24). Assigning numbers on the basis of cardinality or ordinality—as municipalities and states once attempted—does a poor job of dealing with change over time. As new houses are added, the numbers quickly lose their ability to identify a non-interchangeable location or to render a house non-mutable (the same house is given a new number every few years), or they create chaos in terms of local identifiability (½ or even ¼ numbers are used). Numbers must be disentangled and

transcribed in nominal format so they can be linked in a flexible manner to the stock of existing and future physical houses. The same holds for personal names, birth records, and passports (McKeown 2008; Nair 2021; Scott 1998).

Standardization. The second step in manufacturing dividuals involves standardizing the disembedded transcriptions into a relational database that permits internal comparisons and can be superimposed wholesale over other databases. Without adequate resources for standardizing and classifying fingerprints, for example, the millions of files White South African officials amassed over decades produced little more than administrative backlog (Breckenridge 2014). Nowadays, fingerprints taken by the police on a traditional ink-on-card image need to be digitized. An expert, or an automated process supervised by an expert, needs to detect the ridge characteristics and other distinguishing features and store them with the digital image. The combined record is then indexed to enable easy search and retrieval.[3] Links to other databases—names, addresses, ID numbers, standardized facial photos ("please remove your glasses")—need to be stored with the record as well, but in a way that permits revisions without upsetting their superimpose-ability. Returning to the case of house numbers, the system that ultimately prevailed—odd numbers assigned to one side of the street; even numbers to the other side—did so because it was capable of determining the unique locatability not only of all existing houses, but also of the *empty places*, the houses not yet in existence (e.g., by assigning numbers to empty plots, or by leaving unused numbers "between" assigned house numbers; Tantner 2009:24–25).

This example has an interesting implication, generalizable beyond house numbers. With the new system, house numbers acquired the ability to minimize mutability. No house would

[3] https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/afis-history#:~:text=Maintained%20by%20the%20FBI%20Criminal,does%20include%20military%2Drelated%20fingerprints.

need to change its number over time. But this also means the "true" house number resides not on a plate affixed to the house, but on the map kept in the town clerk's office, since this map also holds the numbers for houses not yet in existence. If there is disagreement between the number affixed to the house and the number on the municipality's map, the municipality's number will likely win. The point is subtle but fundamental. Dis-embedding and standardization minimize the interchangeability and mutability of the *dividual* (the number in the municipality's map, the digitized fingerprint stored in the FBI's database, the identity card carried by Deleuze's city resident), not necessarily of the individual (the physical house, fingerprint, or city resident). They do so by means of "horizontal" links to other dividuals and then layering sets of links one upon the other. (The next section discusses an additional step—reembedding—required for linking these dividuals to individuals.)

A bank can know whether a certain account holder, John Smith, is the same John Smith reported living at a particular address only if the map of house numbers can be linked and aligned with other databases containing a registry of official names; birth, death, and marriage registers; Social Security Numbers (SSNs); real estate property titles; and perhaps also credit card numbers, computer IP addresses, and so on. These databases must contain disentangled, standardized records, arranged in a way that—like opposite street-side house numbers—has enough "give" to accommodate change over time. Moreover, this "layering" has a directionality. Some databases are "below" others and understood to be more rigidly fixed; others are above and have more "give." Hence, the status of the birth certificate as a "breeder document" (Rule et al 1983:232). Immense historical work has gone into constructing, maintaining, and aligning these databases to minimize the interchangeability and mutability of dividuals. A good image for this

process is the way the characterization of unique locations in Google Maps depends on the superimposition of multiple relational databases in the graphic form of being mapped onto one another. Yet, even in Google Maps, a gap persists between the physical location and its digital representation.

Haggerty and Ericson (2000) diagnose a tendency of contemporary surveillance systems to become integrated into an ever more comprehensive "surveillant assemblage" aimed at universal, precise identifiability. The integration of multiple dataflows in "centres of calculation . . . [including] forensic laboratories, statistical institutions, police stations, financial institutions, and corporate and military headquarters," Haggerty and Ericson (2000:613) argue, produces increasingly comprehensive "data doubles" of individuals that make anonymity nearly impossible. They depict a dystopian present in which all the different dividuals are quickly and seamlessly linked with one another, so as to render the resulting candy floss swirl a "double" of the individual. Even setting aside the inevitable errors that happen when the physical gets transcribed into digital format, as well as the distortions introduced by the interests of the agents of identification (see the *Agency* section), we think this imagery of the data double overlooks the final necessary step of reembedding.

Reembedding. The utility of all the intricate work of disentangling identifying marks and constructing superimposable databases ultimately hinges on the capacity to relink the resulting dividuals back to people in their local contexts. Organizations may succeed in compiling ever more precise files, but those files may have very little connection to how individuals are identified in their local contexts. Consider this (admittedly ironic and fictional) depiction of how addresses figured into personal identification practices among the French rural bourgeoisie in the early twentieth century:

> "I come as an ambassador," Hardelot-Demestre explained, "I have been sent by the people of the Rue Blanche." (In Saint-Elme, people were never called by their names; they were described by allusions: "The ones from the Place du Marché; our friends who live near the bridge . . . beside the château . . ." The Rue Blanche was where the Renaudins used to live, before Simone had become Madame Burgères. She had moved away, but she and the street would be as one until the last of the Renaudins had disappeared from this earth.) (Irène Némirovsky, *All Our Worldly Goods*, 1947, p.223).

For some purposes, Simone Burgères, née Renaudin, was associated with a certain address where she received mail and reputedly lived; but for other purposes, she was—forever and "as one"—associated with another address altogether. If Simone had put down her address on an official form as "Rue Blanche," the whole intricate process that disentangled house numbers, standardized them, and linked them with other identifying data to construct a precise dividual would have been for naught. The more general issue can be formulated as follows: any set of dividuals, however precisely assembled and aligned, is worthless if people's local forms of identification are not made to resemble their dividuals. The dividuals must be reembedded in the local context via "access points" (Giddens 1990) where organizational representatives—human or non-human—reestablish contact with individuals. Moreover, reembedding must deal with the problem of change over time: people move, change their names, change their gender, discard their phones, separate from their spouses, remarry, go back to their maiden name, buy a second home and now have two addresses, and so on. The reembedded dividuals must be agile enough to follow individuals throughout their movements.

Organizations use multiple mechanisms for reembedding, often working in tandem. They can simply coach individuals to resemble their dividuals. Passé Goffman, handwriting does not "naturally" identify. In the renaissance, for example, people used different scripts for different occasions. Handwriting only became a medium of authenticating identities in the Classical Age: experts in detecting forged documents imposed the requirement of self-sameness on handwriting,

and people were trained to achieve it (Alder 2018). Similarly, filling a form at the local post office, Simone would be instructed by the postmaster to put down her "correct" address, thus reembedding her dividual. Akin to coaching is what Latour (1988:301) calls "prescription": "the behavior imposed back onto the human by non-human delegates." Smartphone fingerprint scanners, for example, prescribe the need to use the same finger and remove bandages. An enormous amount of effort, money, and ingenuity is invested in devising surreptitious forms of reembedding by technological prescription.

Coaching or prescription could come, of course, mixed with coercion and surveillance (Marx 2016:66–69). White officials in early twentieth-century South Africa required all Africans who applied to work in the Rand to carry an endorsed pass. Anyone caught without one—or with one "in any way doubtful"—was immediately imprisoned while officials sought to identify them. Well into the 1960s, about 10 percent of the adult Black male population was imprisoned in this way (Breckenridge 2014:77). Such pervasive coercion, however, proves extremely costly in money, time, personnel, and by virtue of multiplying occasions for resistance (Rule 1973). Moreover, as we noted earlier, it tends to drive certain activities underground. Because identification systems depend on individual cooperation—a point we develop in the following section—their designers routinely take into account public sensitivities. White middle-class Europeans and Americans, for example, have long resisted fingerprinting due to its association with illiteracy and criminality. Coercive reembedding has therefore been used more often to control marginalized populations, like the poor and minorities in the West or subjects of colonial and post-colonial regimes in the Global South (Breckenridge 2014; Cole 2001).

Hence, the far more prevalent mechanism of reembedding (combinable with all the others) involves attaching the dividual to some other desirable good. Having failed to create a

universal registration system during WWI, British civil servants achieved greater success in 1939 by linking food rations to carrying an ID card: "[T]he public had to eat; therefore, the public could be made to carry official identity cards. . . . [This ensured] the card was there for other bureaucratic purposes" (Agar 2001:108). More recently, many of the world's poor in places like Africa, India, and Latin America gain access to in-kind and direct cash assistance only by agreeing to fingerprint identification (Breckenridge 2014; Rao 2019). The dividual thus derives "parasitic vitality" (Agar 2001:102) from being re-entangled with local usage. Smartphones exemplify this "parasitic vitality." It is as if we agreed to constantly report our movements and activities in standardized format, so our dividuals remain up-to-date, in exchange for a multi-stranded tangle of utilities (getting directions, hailing a ride-share, sending real-time selfies). SSNs, for their part, have become entangled with so many other high-value purposes (employment, credit, insurance) that individuals now have a strong interest in monitoring their disclosure and reporting misuse.

The parasitic vitality mechanism, however, has a major drawback: it increases the motivation for alternative uses and fraud, creating new sources of imprecision and error. Immediately upon linking ID cards with food rationing, British officials warned "there will be an enormously enlarged field of 'crime' opened" (Agar 2001:112). Agar (2001:112) cautions that it is unclear "what the fraud meant to the perpetrators," and suggests calling the phenomenon "creative appropriation of official identities." The practice of "identity sharing"—where U.S. citizens or legal residents "loan" their SSNs to others to enable them to access certain resources and services (Harper, Bardelli, and Barrenger 2020)—is a similar form of "creative appropriation." Similarly, Chinese citizens—currently required to present a digital health

passport to gain access to spaces like supermarkets, office buildings, and residential communities—"bypass the system" by uploading screenshots of fake information (Liu 2021). The quest for universal, unique, precise identification backfires and produces its opposite. The more thorough the deconstruction of individuals into dividuals, the more opportunities arise for glitches, creative appropriation, and fraud at their reembedding.

The limiting case, finally, is when organizations proceed as if reembedding is unnecessary. This is exemplified by the statement of the former Director of the NSA that "we kill people based on metadata" (quoted in Cheney-Lippold 2017:189). By this he meant the practice, beginning in 2008, of directing drone strikes by targeting a digital "signature," a pattern of cell phone data that "matches" a pattern calculated to correlate with the presence of terrorists. Consequently, bombs have rained upon suspected terrorists, but also upon Afghani wedding parties and Yemenite villagers. To say "we kill people based on metadata" is to say we pretend to kill precise dividuals, while in fact we are killing imprecise individuals, having made no effort to reembed these dividuals.

To conclude this section, we briefly address the question of whether our framework applies to the identification of non-humans (animals and things). After all, we discussed how numbers render *houses* minimally interchangeable and mutable. Even when discussing people, their smartphones and ID cards loomed larger than their human presence. Deleuze no doubt intended the term "dividual" to minimize the distinction between humans and non-humans. It seems that the same set of practices aimed at personal identification serve to minimize the interchangeability and mutability of cars, shipping containers, phones, "personal" computers, pets, and so on. Animal identification, for instance, not only relies on traditional tagging

methods, but increasingly turns to biometrics and facial recognition.[4] Animals, too, might have their data doubles.

This is no doubt true to some extent. A major characteristic of the "new surveillance" (Marx 2016:40–59) is the degree to which both humans and non-humans get rendered into data. Data analysts are professionally trained to be "post-humanists." From their point of view, it matters little whether location data identifies individuals or shipping containers—we can bomb them both based on their "metadata."

But as the preceding discussion of reembedding should have made clear, the analytic framework we offer here is not limited to the image data analysts, fraud investigators, and NSA intelligence officers might have of their own work—wherein things, animals, and humans are just data. Analyzing practices necessitates attentiveness to their unstated premises and unanticipated consequences. Reembedding requires, as we saw, the active participation of the individuals-to-be-identified, as when they furnish identification documents or dispute seemingly "suspicious" transactions. As the next section will develop, individuals are active participants in the network of actors that manufactures, standardizes, and reembeds their dividuals. This is true for non-humans as well, but their capacity to participate in the network is limited in comparison to humans. Moreover, as the previous discussion of "parasitic utility" made clear, reembedding provokes individuals' unanticipated reactions in ways that loop back to confirm, defy, or modify practices of personal identification (a theme we develop in the *Techniques* section). Non-humans can also act in ways that disrupt the best-laid plans of experts, yet their capacity to do so appears more limited (Jerolmack and Tavory 2014:74).

[4] https://norecopa.no/media/7291/biometric-methods.pdf.

Agency

Who performs the work of identification? We begin with a concrete example. One of us recently flew back home from another state. This involved identifying oneself to the officer at the Transportation Security Administration (TSA) desk. The officer looked at the author's drivers' license, the flight records on the screen in front of her, and at his face, comparing the information gleaned from all three before waving him ahead. Yet, each source of information she consulted linked her to a wider network. The officer's glance at the computer screen linked her to experts who design, maintain, revise, and analyze TSA databases and to other government agencies, like the FBI, with which TSA shares data (United States, Transportation Security Administration 2008). The ID presented linked her to a civil servant in a state Department of Motor Vehicles, who issued the driver's license after considering other sources of information, such as an application and birth certificate. The author himself also performed work to make himself "suitable" for identification: he approached the officer's desk unaccompanied, placed his ticket on the scanner, lowered his mask, and turned to directly face the officer to enable visual comparison.

Thus, the agency of identification is not a unitary actor—the "surveillance agent" (Marx 2016:33; although Marx's analysis is considerably more complex and we will draw on it below), or "the state" (Scott 1998)—but a complex actor-network. In what follows, we will stress three aspects of this complex agency. First, we draw attention to the competing pressures concentrated at the position of frontstage staff like the TSA officer, who mediate between the backstage experts conducting identification "from a distance" and the individual-to-be-identified. This should sensitize sociologists to the fact that the different agents involved in identification may

have divergent interests. The second point follows from the first. Personal identification depends on coordination, and sometimes compromise, between coalitions of actors—including the frontstage and backstage staff, but also the potential audience for identification (like the FBI in the above case). This changing configuration of relations shapes how personal identification operates in practice and often constitutes a distinct obstacle to the project of precise identifiability. Finally, the individual herself participates as a member of the actor-network that creates and maintains her own dividual.

Access points. The TSA desk constitutes what Giddens (1990) calls an "access point" for the complex network performing personal identification. Access points are where the expert systems that run our lives generate trust, but also where they are most vulnerable when things go wrong. Attending to access points means thinking in terms of relations between, at a minimum, three parties: the local, front-facing staff at the access point, the backstage staff performing calculations and issuing instructions from a central office (this is similar to Marx's [2016:33] distinction between the "sponsoring agent" and the "collecting agent" of surveillance), and the individual-to-be-identified whose cooperation (however minimal) must be ensured for identification to proceed smoothly, but whose status as either an ordinary user or fraudster remains uncertain.

The essential point is that personal identification constitutes a collaborative situational achievement by a set of actors whose interests and perspectives may not coincide, and who may strike shifting alliances with one another. Unless in situations of extreme coercion, frontstage staff profit from securing the cooperation and trust of individuals-to-be-identified. Work at the TSA desk runs smoother when individuals present themselves appropriately and participate in their own identification. The trust involved has two interdependent components (Giddens 1990):

trust in the overall accuracy and rationality of the system of identification, and trust in the competence and good intentions of the agents at access points. Organizations are aware of this and coach their front-facing staff in how to inspire trust. Yet, the two forms of trust may also work against one another. One key way front-facing staff signal their trustworthiness to users is by performing role distance and signaling a modicum of independence from the overall system. We typically do not trust staff who appear as mere puppets and parrots. Consequently, the well-coached commiseration with an individual's complaint may turn into a knowing confidence or even outright collusion. Faced by a lender's demand for a second form of ID, one of us was recently told by a real estate closing agent to "just tell them that you showed me your Social Security Card, and I'll tell them the same." Users may come to expect this flexibility and reward it. Yet backstage staff, aware of these dynamics, may also seek to constrain the independence of staff at access points by requiring them to follow strict procedures, monitor their adherence, or even replace them with machines, recruiting individuals-to-be-identified to their side by emphasizing the "mechanical objectivity" (Porter 1996) of procedures and machines.

This complex triangular interplay animated the implementation of India's *Aadhaar*, the world's largest system of biometric identification (Rao 2019:538). *Aadhaar* reformers framed it as a way of minimizing corruption and fraud. The mechanical objectivity of biometric information—fingerprints, iris scans, and facial photographs—was supposed to generate trust and recruit ordinary Indian citizens to the side of the reformers. Yet to achieve this goal—to transform individuals into dividuals—reformers had to rely on the improvised work of frontstage staff at "access points." To obtain an *Aadhaar* number, individuals must first submit prior official documentation, often requiring confirmation by officials in the paper-based system. People who

lack paper documentation must present an official witness—either someone registered as an "introducer" (Baxi 2019), or in the case of spouses and children, a head-of-household whose own official documentation is in order (Rao 2019:544). Staff at enrollment centers transcribe information from these sources into a computer database. Even the collection of biometric information requires active intervention by staff. As Nair (2021:33) recounts, "Operators would routinely leave their seats and cross over to the resident's side, pressing fingers onto the fingerprint scanner with just the right amount of pressure, often with help from family members." In short, the road to "trust in biometrics" was paved with improvisation by the staff at access points.

This triangular dance continued after enrollment when individuals wished to avail themselves of the benefits linked to one's *Aadhaar* number. Ration shop owners, for instance, were expected to distribute rations to beneficiaries following identification by a mechanically objective fingerprint scan. The scales for weighing rations were linked to the scanner with the intention of turning the shop owner into a mere cog in an impersonal transmission belt. Yet internet connectivity issues and fingerprint authentication failures frequently impeded the system. In response, shop owners devised creative "fixes." They authenticated beneficiaries at a separate location with good connectivity, printed a weight slip beneficiaries could bring to the shop later, and then used a system of informal paper booklets to track who got what and how much (Chaudhuri 2019). In short, *Aadhaar* identification was shaped by the interests and pragmatic concerns of staff at access points, who struck an alliance with beneficiaries. Without the shop owners' creative fixes, trust in the system would have collapsed. Yet, the fixes compromised the accuracy of the information conveyed to the backstage staff.

Coalitions. Beyond the "vertical" triangle we just described, identification unfolds within complex "horizontal" actor-networks composed of various parties whose interests must be translated and coordinated. A key dimension of variation is the scope of the "audience" privy to identifying information. This is often described as "function creep," that is, the tendency for information collected for one purpose to be used for other purposes by other surveillance actors. Research often portrays function creep as an almost inescapable consequence of the age of "big data" (Brayne 2017; Fourcade and Healy 2017:16). In contrast, our framework sensitizes sociologists to the complex coordination that underpins function creep. Function creep is not automatic; it requires reconciling the potentially divergent interests of various horizontal members of the network.

A prime example of "function creep" is the Social Security Number. In the context of consumer credit, Lauer (2017:189) writes that when credit bureaus adopted the SSN as a unique identifier, "financial identity . . . acquired its magic key, and American consumers were literally reduced to numbers." We think this is somewhat hyperbolic. The SSN's ability to serve as a unique financial identifier for multiple organizations depended on complex interactions between all the different actors—horizontal and vertical—who needed to coordinate their respective interests.

In the 1960s, credit bureaus began consolidating and computerizing their records, eventually culminating in a few mega-bureaus. Faced with the challenge of merging records for customers, many bureaus relied on some combination of names, birth dates, addresses, occupations, and spouses' names (Lauer 2017; Rule 1973:220). In their efforts to prevent duplicates, they even considered using fingerprints or voice spectrographs—visual

representations of the various component frequencies of sound over time (Lauer 2017). Ultimately, however, they settled on SSNs, which by the early 1960s were increasingly used as identifiers by government agencies (Fourcade and Healy 2017; Lauer 2017).

SSNs, however, presented a unique coordination problem between the Social Security Administration (SSA) and financial institutions. Originally, each SSN included a two-digit year of birth and three-digit registration-location indicator, the latter issued sequentially by states. The number thus remained entangled with the substantive meanings of ordinality and localization, enabling fraudsters to predict SSNs based on public information (Acquisti and Gross 2009). This led the SSA in 2011 to begin assigning random, that is, purely nominal, SSNs (Social Security Administration n.d.). Randomization, however, presented financial institutions with difficulties. Like fraudsters, they used the substantive elements of ordinality and locality to verify whether a particular SSN really existed. Fraudsters began to create nonexistent people using fake SSNs—a form of "synthetic identity"—and banks were at a loss how to detect these.

Following industry lobbying, the SSA partially solved this coordination problem in 2020 by creating the electronic Consent Based Social Security Number Verification (eCBSV) service. It allows banks to verify that a name, date of birth, and SSN match SSA records. This is by no means the final word on the matter. As Brensinger learned from interviews and industry events, financial institutions do not rely on the SSN alone, but endeavor to collect as much personal information as possible—official names and addresses of course, but also transaction information, device information, third-party data sources, and so on. They create, or partner with vendors to deploy, tools that superimpose digital traces—browser information, IP addresses, hardware-software type, and other data collected by cookies—over SSNs. The SSN's function

does not "creep" by itself, but only over a tighter web of links woven between the various dividuals and the individual.

At this point, another coordination problem arises. Banks must collect all this additional information without offending or overburdening current or prospective customers. In insider lingo, they must balance identifiability with the need to avoid appearing "creepy" and to minimize "friction," that is, the steps required of consumers, such as entering a password or showing an ID card, that slow down their intended course of action. This leads banks to self-impose limitations on data collection, aggregation, and data sharing with other organizations, as well as to create internal firewalls limiting who has access to identifying information.

We would like to underline the significance of the preceding account. The transformation of the SSN from its original role as a means for tracking Social Security benefits into a unique financial dividual and *de facto* national identification number constitutes a prime example of "function creep." Focusing on interrelations between the different parties in the identification network, however, reveals the complex and uncertain work of coordination that underpins function creep. Most importantly, it indicates that function creep is by no means automatic and irreversible. Precisely because consumer identification generated increasingly comprehensive data doubles, financial institutions find it necessary to limit the *audience*, the circle of those with access to identifying information, thereby creating a distinct limit to function creep and to precise identifiability (Marx 2016:33). A tradeoff exists between *how much* is known about a particular individual and *who* is entitled to such knowledge (Marx 2001:311–13). Organizations are keenly aware of this tradeoff. They may seek to preserve their ability to collect identifying information by building internal firewalls or limiting their data sharing with other parties, or they may opt to preserve the scope of the audience by collecting less information or operating at a

lower degree of specificity (i.e., introducing some form of de-identification). Whatever they opt to do, they effectively grant a certain degree of anonymity to individuals. The most perfect "data double" equals pseudo-anonymity if very few people are allowed access to it (Marx 2016:104).

We would be remiss not to mention that organizations can also try to avoid this tradeoff by keeping their data collection or data sharing efforts secret. Banks have implemented "passive" identification processes that collect information like computer metadata without requiring user input (Magnet 2011:22). They contract with unregulated data brokers, such as Acxiom and LexisNexis, who compile data from various sources and sell the resulting data doubles without consumers' knowledge (Roderick 2014). Such strategies keep people in the dark about how much identifiability is possible in the system (Zuboff 2018), while also avoiding "friction." Function creep may not be automatic, but neither are the limits to it. These limits depend on political struggle, as evidenced by the much stronger privacy protections in the EU compared with the United States and especially the global South (Breckenridge 2014; Lyon 2009). For our purposes, however, the key point is that where and how the tradeoff gets struck depends on the interrelations between all the relevant actors and is not predetermined. In many situations, securing individuals' cooperation, and thus retaining the ability to at least partially identify them, necessitates granting them a certain measure of anonymity.

Responsibilization. Finally, individuals are enlisted in and made partially responsible for their own identification. People do not come in the form of data, so identification depends on individuals to perform work to furnish information and make it intelligible to expert systems. First, despite their claims to impersonality, many organizations rely heavily on individuals' subjective input to build their dividuals. Banks and social welfare programs solicit identifying information directly from individuals via forms or verbal testimony (Rule 1973). Even

"documentary regimes of verification" (Robertson 2009) like birth registration require someone to produce a name and other information to a certifying official (Noiriel 2001). As Brensinger learned from interviewing identity theft victims and the professionals with whom they interact, many financial fraud claims hinge on little more than an individual's word.

Second, even seemingly "objective" bodily identifiers require individuals to furnish them in legible ways. *Aadhaar* enrollment depended on discrete individuals presenting themselves in person for biometric registration—wives too, as Indian men learned to their bewilderment (Nair 2021). Staff had to teach enrollees how to position their fingers on the scanner and orient their faces to the camera. Manual laborers had to clean their hands to make their fingers legible (Chaudhuri 2019).

Third, as noted earlier, organizations will go to great lengths to obtain individuals' cooperation in their own identification. They will limit the audience privy to identifying information; they will keep dividuals apart, avoiding their integration into a "data double"; they will reduce the "friction" involved. All of this constitutes prima facie evidence that such participation is necessary for personal identification.

We emphasize the key role played by individuals in their own identification, but this does not imply they participate on an equal footing. Disembedding local knowledge results in a reversal of power/knowledge and trust relations. Personal, local knowledge is rendered partial, subjective, and suspect. Disentangled and standardized dividuals acquire the attributes of objectivity, precision, and credibility (Scott 1998). Reembedding offers opportunities for individuals to negotiate with staff at access points, but this is viewed with skepticism by the backstage staff (Robertson 2009, 2010).

This becomes evident when observing how cases of identity theft get resolved. The main burden of repairing the link to dividuals *falls on the individual herself,* and yet she stands at a distinct disadvantage throughout the process. Her participation is secured, even required, but on unequal terms. In the United States, regulations like the Fair Credit Reporting Act (FCRA) and Regulation E of the Federal Reserve make individuals responsible for monitoring their accounts and credit reports and disputing apparent fraud or error. This is not to consumers' advantage. As we shall explain in the next section, if you overlook a fraud or error—perhaps because identifying them involves substantial labor, such as regularly reading bank statements—it will be treated by organizations as correct. Your own protestations after the fact will appear subjective, hard to distinguish from fraud itself, and in need of disembedding in order to be trusted. In short, you will be playing a double role—at times, a responsible individual; at times, a potential fraudster—that staff find hard to parse. To reestablish your status as trustworthy, you will be funneled through a set of access points—bank call centers and credit bureau web portals—where front-facing staff record your complaint, gather additional information, and compare it with existing records. At each access point, gatekeepers are predisposed to trust disembedded and standardized information, so they may funnel you to another access point. They may ask you to file a police report to give your claim the veneer of impersonality. In short, identity theft resolution reveals that even as individuals participate in constructing and auditing their dividuals, they also participate in restricting their own agency.

Technique

What does it mean to identify? What does the *technique* of personal identification consist of? Popular and expert discourses often depict identification as a process of matching new data to well-established "originals" (Cole 2001). Because the object of identification is the dividual,

however, *there is no original*. We suggest, therefore, to think of identification not as matching, but as a process of continuous *testing*, "an orchestrated attempt to reveal an entity's potentially unknown properties or capacities" (Marres and Stark 2020:420).

Matching and testing differ in three ways, awareness of which represents a contribution to the sociological analysis of personal identification. First, matching implies the dividual is directly compared to the individual. Testing, on the other hand, constructs comparisons *between dividuals*. Second, matching is binary. It constitutes a single event that yields a match or non-match. Testing, on the other hand, is iterative and aims at minimizing interchangeability and mutability to within an acceptable range. Third, matching deals with an unchanging given, the "original." Testing, on the other hand, has interactive characteristics, noted by Goffman (1969) in his analysis of "expression games" and in accounts of "looping" (Hacking 1995) and "reactivity" (Espeland and Sauder 2007). This last point is hugely important. It means that the historical process of transformation of identification processes *has no directionality*. We are not moving toward a fuller category of the person (Mauss), nor toward increased personal identification by the state (Goffman), because the interactive nature of testing turns identification into an unpredictable "moving target" (Hacking 2007).

We derived these distinctions from observing the practices of identity fraud investigators, for whom the process of identification entails a high degree of uncertainty. Rather than discovering the "true," non-interchangeable and non-mutable individual, identity fraud investigators construct the qualities of minimal interchangeability and mutability from tests designed to reduce uncertainty and anticipate "covering" and "counter-uncovering moves" (Goffman 1969:12–31) undertaken by fraudsters.

Lest the reader think identity theft is an extreme example, we would like to start with a humble, pervasive, and long-standing dividual: the *signature* (Fraenkel 1992). Ostensibly, the signature gets matched against an "original" signature to authenticate one's identity. The procedure of "matching" signatures, however, conceals the long historical process that gave rise to the fiction that self-sameness inheres in one's handwriting (Alder 2018). This fiction became part of the modern *habitus*. One of the authors still remembers the care and pride with which his grandparents—good students that they were—signed their names, each time endeavoring to reconstruct the precise features that made their signatures supposedly non-interchangeable.

Experts did not "discover" self-sameness in handwriting. They *made* it reside there, perfecting over time a particular test that minimized the interchangeability and mutability of signatures, but which did not yield a secure binary result. To this day, given that one's handwriting changes over time, it is never quite clear what constitutes forensic evidence for authenticity. A match that is "too close" can raise the suspicion of forgery, necessitating another test (Alder 2018). Precisely when a single binary result is obtained, iteration and judgment become necessary.

More importantly, the "original" signature itself needs to be constructed as such, transformed from handwriting on a page into bureaucratic "fact," perhaps by a notary public. The notary legitimizes the signature by affixing her seal on the document—a practice deriving from the process by which the "King's house" gradually became "the state" (Bourdieu 2014:296–302). Yet, what authenticates the seal itself? Most likely a certificate hanging in the notary's office, itself authenticated by the signatures of relevant officials at the credentialing institution. And so it continues. What ultimately certifies identification is not some "original" signature, but the

length and strength of this endlessly receding chain of dividuals and the fact that its nodes have been constructed, by the combination of bureaucratic procedures and socio-cultural positions (Robertson 2009), to withstand tests.

Finally, what should we make of electronic signatures? How can an act that plainly could be performed by anybody be legally constructed as an "original"? We think this demonstrates the interactive character of testing. In the series of moves and counter-moves of which testing consists, the signature has lost primacy of place. Our grandparents would have been horrified to see how carelessly we sign our names, but we have been coached by now to expect that however perfunctory our scribble, it will be admitted as "good enough" because it is surrounded by further tests. As fraudsters got better at covering moves (forging signatures), organizations responded with uncovering moves (tests that attend to context, behavioral pattern, and metadata), and the battle has shifted to the terrain of counter-uncovering moves. The signature is by now a "moving target" (Hacking 2007): no longer objective evidence, and not quite mere subjective testimony, it requires further tests to authenticate.

We now outline three concepts to sensitize researchers to different dimensions of the testing process. First, identification systems *construct a baseline* against which to compare subsequent information. Second, such comparisons are informed by *expert judgment.* Finally, testing is *interactive.*

Constructing a baseline. Because no "original" exists, testing requires the construction of a baseline dividual against which to compare others. Organizations use different approaches to achieve this. As noted earlier, some bootstrap from individual subjective attestations. They may undertake registration campaigns to create "official" baseline data (e.g., birth registries or biometric databases) for previously under-identified subpopulations (Breckenridge 2014;

Breckenridge and Szreter 2012) or designate official "witnesses" capable of vouching for self-reported information (Rao 2019; Robertson 2009). These efforts produce a baseline for those included, but they disadvantage those left out—typically members of marginalized groups. Black workers, for example, were excluded from the Social Security Act of 1935 and prevented from obtaining SSNs (Igo 2018). "Undocumented" populations today, including migrants and the homeless, face similar challenges (Baxi 2019; Cheong 2019; Diallo 2021). This is but one way identification processes reinforce existing inequalities.

Investigators dealing with suspected identity theft take a different approach to constructing a baseline. They accumulate "data lakes," as they put it, collecting everything from application information to computer metadata, surveillance footage, and call center recordings. Then they partition all data points into two categories—"suspicious" and "legitimate"—based on whether consumers disputed them or not. Uncontested data points become the baseline for assessing the legitimacy of ostensibly "suspicious" activities. Thus, investigators do not match dividuals against an "original," but against a bootstrapped baseline provisionally constructed out of the very testing activities it makes possible. Note that most of the datapoints included in the "uncontested" pool simply *cannot be contested* because they are not visible to consumers. Consumers dispute transactions, but often the most crucial information consists of metadata associated with these events. Investigators value this data precisely because they believe it is more resistant to conscious manipulation. From the consumer's perspective, this seems unfair, almost a "catch-22." First, the baseline derives from taking one's word (anything disputed gets treated as suspicious), but then the test is constructed precisely by not taking one's word (the legitimate category consisting of behavior "given off" [Goffman 1959]). From investigators'

point of view, this duality reflects the structure of the "expression game" (Goffman 1969:11–12, 17–19) they are playing, in which the consumer appears simultaneously under two guises: first, in the "naïve move" the consumer "can be taken as he appears," and second, in the "uncovering move" the consumer is taken as a "gamesman" whose "manipulation and design" the investigator must "crack, pierce, penetrate and otherwise get behind." Testing involves a constant equivocation between these two alternatives.

Efforts to resolve identity theft within abusive domestic relationships prove especially tricky precisely because testing involves constructing comparisons between dividuals. Fraud investigators commonly rely on location and device data to evaluate disputes, interpreting geographic proximity and recognized devices as evidence supporting the legitimacy of transactions. Yet because spouses and partners typically live together and may use each other's devices, such inferences do not apply to instances of domestic financial abuse. Comparing dividuals cannot resolve these cases because each dividual packages together the two characters—the responsible individual and the fraudster—with little ability to distinguish between them. This is further complicated by long-standing gendered assumptions (Hyman 2013; Krippner 2017) that lead investigators to assume women fall under men's finances. Domestic financial abuse tends to disproportionately harm women, so this points to another way techniques of identification can reinforce social inequalities.

Expert judgment. After constructing a baseline, organizations rely on expert judgment to make comparisons. Such judgments play a role in rudimentary and technologically sophisticated identification processes alike. TSA officers judge whether a passenger's face appears sufficiently similar to a picture ID, and bureaucrats in the Malaysian registration office assess dialect during

interactions (among other things) to determine the legitimacy of documentation for birth registration (Cheong 2019). As this latter example reinforces, expert discretion can trump or at least cast suspicion on official documentation (see Browne 2010). On the more technical side, fingerprint experts decide whether ridge characteristics are sufficiently comparable to render prints identical (Breckenridge 2014; Cole 2001), and DNA analysts interpret graphs outputted from instrumentation to determine the likelihood of identification (Bechky 2021).

Financial fraud investigators also rely heavily on honed, but ultimately subjective, judgments. They assess whether a disputed transaction fits the pattern of a consumer's "uncontested" past behavior, or whether two independently obtained screenshots of surveillance footage capture the same person. During fieldwork, Brensinger observed a fraud investigator visually comparing the photo of a consumer from an uncontested government-issued photo ID with a still frame from surveillance footage on side-by-side monitors. The investigator compared noteworthy physical markers, style of dress, and other visual cues to arrive at a judgment of their similarity. Such judgments, however, commonly reflect racial and other biases (Todorov et al. 2015). In the absence of baseline data—as when a consumer with no prior relationship to an institution disputes a new account—investigators draw on their experience assessing the legitimacy of data. They use metadata to reveal the IP address and location associated with online account openings. They immediately flag as suspicious any use of virtual private networks (VPN) or large gift-card purchases, because in their experience these are often used for money laundering.

Whether working with faces, fingerprints, signatures, or metadata, experts—and many social scientists for that matter—commonly describe the knowledge they draw on as embodied and tacit (Bechky 2021; Dreyfus and Dreyfus 2005). Even as they present themselves as

objective and neutral, they seek to foreclose scrutiny of their expert judgment, claiming it involves experiential knowledge and "gut feelings" that lay individuals cannot easily acquire or evaluate. Such claims aim to legitimize experts and protect their domain (Bechky 2021; Magnet 2011). Yet they also open up expert systems to critiques of arbitrariness (Cole 2001).

Seeking to insulate themselves from such critiques, organizations turn to algorithms, whether human- or machine-executed. These are supposed to endow organizational decision-making processes with mechanical objectivity superior to the subjectivity and bias of expert judgment (Krippner 2017; Porter 1996). Yet, as the examples above document, even when the most sophisticated technology is deployed, experts must still determine whether the cutoff programmed to declare a "match" has been legitimately applied. Technologies can facilitate the testing process, but they cannot eliminate the reliance on expert judgment. Rather, they tend to shift expert discretion into more opaque parts of the organization, thereby protecting it from scrutiny (see Brayne and Christin 2020). Additionally, the developers of algorithms engage in "knowledge acquisition" from the experts and then encode such judgments—inclusive of assumptions regarding race, gender, sexuality, and disability—into how algorithmic identification is executed (Benjamin 2019; Magnet 2011). Facial recognition technology, for instance, often fails at higher rates for Black faces due to the "logic of prototypical whiteness" built into that technology (Browne 2015:113). Far from disappearing, expert judgment about what or who to privilege during identification simply moves to the backstage. Tests for personal identification ultimately rest on a bedrock of expert judgment.

Interactivity. Finally, reconceptualizing the technique of personal identification as testing draws attention to its interactive nature. Tests do not passively describe some entity, but actively intervene and interact with it (Marres and Stark 2020:420). Testing is a process to which

individuals react in unanticipated ways, which then "loop" back to modify practices of identification.

Early twentieth-century U.S. immigration restrictions generated incentives to claim false identities, produce false documents (McKeown 2008), or claim "paper families" (Lau 2006). Administrative procedures sought to transform migrants from illegible members of dense local networks into legible dividuals and members of nuclear families. At Ellis Island, Naftula, Son of the Merchant, a designation thick with local context, became "Nathan Fabrikant," a legible *dividual* and member of a clearly bounded family unit. Yet, this meant the layers of practical knowledge (Scott 1998:6–7) built into the original naming convention were lost. Without those, how could officials tell whether familial claims—Mr. Fabrikant seeking to bring into the country his wife and child—were legitimate? For early-twentieth-century immigration officials, the solution involved conducting long interviews comprised of a battery of questions. In Goffman's terminology, they used "uncovering moves" to detect inconsistencies in applicants' accounts. Officials grilled individuals claiming derivative citizenship about details of their family context in the home country, including the physical environment (e.g., "layout of the applicant's home village" or "the numbers of windows, doors, and animals in the house") and local events (e.g., "gifts given during visits from other family members") (McKeown 2008:277). Officials then compared the answers against written history and the testimony of supposed family members. This uncovering test, however, provoked a counter-uncovering move. The more officials wanted to know, the more people became aware of how they were represented in official records, and the more they adjusted their accounts accordingly. Because officials interpreted inconsistencies as evidence of fraud, migrants were compelled to practice "correct" responses that would fit into the

appropriate bureaucratic categories. Even when no fraud was involved, migrants' answers should be seen less as reflections of who they were, and more as constructing the kind of stable documentary identities the test required.

Similarly, one of the most paradoxical insights about identity fraud—a pervasive concern in identification discourse worldwide—is how, far from undermining identification processes, it tends to legitimize them. Identity fraud constitutes a transgression that confirms the organizational fiction of non-interchangeability and non-mutability. This happens because organizations generally respond to fraud not by rethinking the underlying logic of identification, but by endeavoring to collect more data and construct better tests (Breckenridge 2014; Noiriel 2001; Rao 2019; Robertson 2009). Covering moves are met by uncovering moves. Counter-uncovering moves elicit orchestrated checks and even traps. The aforementioned U.S. customs officials realized their new techniques inadvertently coached migrants in how to provide "correct" responses. Yet they responded with "more testimony and better filing techniques" (McKeown 2008:281). The same tendency can be seen in official accounts that offer biometric identification as the solution to paper-based fraud (Breckenridge 2014; Rao 2019). Because fraud thrives under impersonal identification, it is highly unlikely biometrics will eliminate it. Rather, fraud serves to justify the need to expand testing. The same is true for the multiple errors that plague identification systems (Eubanks 2018; Magnet 2011), or when algorithms engage in racial discrimination (Benjamin 2019; Noble 2018): we hear calls to reform identification systems, not jettison them. Yet, as experts reconstruct tests and individuals adapt to them, practices of identification keep changing and personal identification remains a moving target.

As we noted earlier, testing is iterative and continuous. This holds for both paper and digital technologies, but the latter clearly offer a new affordance by allowing dividuals to be

more dynamic than with the former (Kellogg et al. 2020). During fieldwork, Brensinger regularly heard financial industry insiders talk about the greater density and instantaneity of the data produced by mobile devices, and about machine learning models promising near real-time decision-making based on various tests embedded into consumer behavior, such as "behavioral biometrics" (analyzing the angle at which users hold their handheld devices or the pressure they apply to touchscreens). Digital technologies and the sensors they incorporate enable ever more continuous testing, along with the accompanying uncertain reactions and outcomes.

Conclusion

In this article, we offered a framework for analyzing personal identification as a historically evolving organizational practice. As summarized in Table 1, this approach offers a number of advantages over existing literature.

[Table 1 about here]

First, we delineated the domain of research with greater precision. Scholars typically understand personal identification to mean finding, locating, and naming a unique and self-same individual. Even a sophisticated observer such as Marx (2016:102–103) has recourse to what he calls a "distinctive core identity" generated by "the laws of physics and biology." This figure, we argued, is better grasped as an organizing fiction: in reality, practices of personal identification vary a great deal in the degree to which they minimize the interchangeability and mutability of dividuals.

Second, we sensitized sociologists to the main difficulty all identification practices must negotiate, namely the inherent and unavoidable gap between embodied individuals and their surveillance representations. We did so by emphasizing that the *object* of identification practices is the *dividual*, and by offering a theory of how dividuals are manufactured through

disembedding, standardization, and reembedding. In the context of triumphalist rhetoric about digital technology, shining the light on this process of manufacturing and its persistent glitches and opportunities for resistance represents a key challenge for sociological research.

Third, we provided preliminary sketches of the different actors and actants that combine to form the *agency* of identification. Although no doubt incomplete, our list should suffice to draw sociologists' attention to the potentially divergent interests and changing configurations of relations between the parties involved, and thus turn analytic focus to mechanisms of coordination.

Fourth, we provided a more realistic account of what it means to identify. We drew on the case of recovery from identity theft to demonstrate that identification does not consist of matching signs to an "original" individual, but of iterative testing that probes the strength of associations *between dividuals*. This is done by constructing a baseline of trustworthy dividuals, to which other dividuals are constantly compared. This should alert sociologists that identification is probabilistic, uncertain, and relies on fallible expert judgment.

A great deal of current research into digital technology invokes the imagery of a dystopian future of continuous, precise, and inescapable identification. A fifth advantage of the framework we developed is that it incorporates into the analysis multiple counter-tendencies that allow a more realistic assessment of the directionality of change. The difficulties involved in reembedding dividuals create a tradeoff between non-mutability and non-interchangeability. The interests of frontstage staff and the dynamics of securing trust at "access points" can impede the flow of precisely identifying information. An organization's own interests in securing trust can lead it to strictly limit the audiences for identifying information, thereby rebuilding a measure of

pseudo-anonymity. Finally, the interactive nature of testing creates multiple points where resistance and creative adaptation may reshape identification practices in unexpected ways.

Finally, in the tradition of general theorizing (Zerubavel 2020), our approach illustrates the benefit of bridging historical and contemporary research, national contexts, and substantive silos in social science literature. It enables scholars to see commonalities in how personal identification operates in national contexts as diverse as China, England, France, India, South Africa, and the United States, and across domains such as credit, policing, immigration, and health. Crucially, it practices initial agnosticism regarding the technology of identification. As much as possible, we sought to treat paper-based and digital technologies symmetrically, focusing on processes, problems, and dilemmas common to both. We thus illustrated how scholars studying dated and contemporary identification processes might productively learn from one another, which would be especially useful for clarifying which aspects of digital technologies represent novel affordances.

Our approach to personal identification is not without its limits. General theorizing intentionally overlooks differences between cases and contexts in order to identify analytic constants. This should not imply the absence or insignificance of differences between identification processes across these settings. Cultural interpretations of identification techniques vary considerably across time and space, as do such things as privacy norms, legal treatments of people and information, and technical infrastructures and capabilities (see, e.g., Breckenridge 2014). We briefly suggested a few such differences in the course of elaborating our theory. Future research should more fully explore how such contextual differences matter for identification processes and their consequences. Nevertheless, as personal identification becomes increasingly ubiquitous and consequential, our concepts should enable scholars with disparate

regional, historical, and thematic interests to learn from each other about the inner workings, migration, and transformation of key modes of governance and social control.

References

Acquisti, Alessandro, and Ralph Gross. 2009. "Predicting Social Security Numbers from Public Data." *Proceedings of the National Academy of Sciences of the United States of America* 106(27):10975–80.

Agar, Jon. 2001. "Modern Horrors: British Identity and Identity Cards." Pp. 101-120 in *Documenting Individual Identity: The Development of State Practices in the Modern World,* edited by J. Caplan and J. Torpey. Princeton: Princeton University Press.

Alder, Ken. 2018. "The Forensic Self: Proving Identity from the Counter-Reformation to the Dreyfus Affair." October 15, Uppsala University.

Baxi, Parul. 2019. "Technologies of Disintermediation in a Mediated State: Civil Society Organisations and India's Aadhaar Project." *South Asia: Journal of South Asian Studies* 42(3):554–71.

Bechky, Beth A. 2021. *Blood, Powder, and Residue: How Crime Labs Translate Evidence into Proof.* Princeton, NJ: Princeton University Press.

Benjamin, Ruha. 2019. *Race after Technology: Abolitionist Tools for the New Jim Code*. Medford, MA: Polity.

Bouk, Daniel B. 2015. *How Our Days Became Numbered: Risk and the Rise of the Statistical Individual*. Chicago: University of Chicago Press.

Bourdieu, Pierre. 2014. *On The State. Lectures at the Collège de France, 1989-1992*. Cambridge: Polity Press.

Brayne, Sarah. 2017. "Big Data Surveillance: The Case of Policing." *American Sociological Review* 82(5):977–1008.

Brayne, Sarah, and Angèle Christin. 2021. "Technologies of Crime Prediction: The Reception of Algorithms in Policing and Criminal Courts." *Social Problems* 68(3):608–24.

Breckenridge, Keith. 2014. *Biometric State: The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present*. Cambridge, UK: Cambridge University Press.

Breckenridge, Keith, and Simon Szreter, eds. 2012. *Registration and Recognition: Documenting the Person in World History*. Oxford, UK: Oxford University Press.

Brensinger, Jordan. N.d. "Identification and Insecurity in the Data Economy." Unpublished PhD dissertation, Department of Sociology, Columbia University.

Browne, Simone. 2010. “Digital Epidermalization: Race, Identity and Biometrics.” *Critical Sociology* 36(1):131–50.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham, NC: Duke University Press.

Caplan, Jane. 2001. “‘This or That Particular Person’: Protocols of Identification in Nineteenth-Century Europe.” Pp. 49–66 in *Documenting Individual Identity: The Development of State Practices in the Modern World*, edited by J. Caplan and J. Torpey. Princeton, NJ: Princeton University Press.

Chaudhuri, Bidisha. 2019. “Paradoxes of Intermediation in Aadhaar: Human Making of a Digital Infrastructure.” *South Asia: Journal of South Asian Studies* 42(3):572–87.

Cheney-Lippold, John. 2017. *We Are Data: Algorithms and the Making of Our Digital Selves*. New York: New York University Press.

Cheong, Amanda R. 2019. “Omitted Lives: Access to Civil Registration and Its Implications for Inequality.” PhD dissertation, Department of Sociology, Princeton University.

Christin, Angèle. 2020. “Powerful Metrics - Steffen Mau, *The Metric Society: On the Quantification of the Social* (Cambridge, UK, Polity, 2019, 200 p.).” *European Journal of Sociology 61*(3):486–89.

Cole, Simon A. 2001. *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge, MA: Harvard University Press.

Cole, Simon A., and Henry N. Pontell. 2006. “‘Don’t Be Low Hanging Fruit’: Identity Theft as Moral Panic.” Pp. 125-147 in *Surveillance and Security: Technological Politics and Power in Everyday Life*, edited by T. Monahan. New York: Routledge.

Deleuze, Gilles. 1992. “Postscript on the Societies of Control.” *October* 59:3–7.

Diallo, Alimou. 2021. “Inanimate Politics: Identifying ‘Lifeless and Undocumented Migrants’ in Guinea and Morocco.” Pp. 324-342 in *Identification and Citizenship in Africa: Biometrics, the Documentary State and Bureaucratic Writings of the Self,* edited by S. A. Dalberto and R Banégas. London: Routledge.

Dreyfus, Hubert and Stuart E. Dreyfus. 2005. “Peripheral Vision: Expertise in Real World Contexts.” *Organization Studies* 26(5):779-792.

Durkheim, Émile. 1973. “Individualism and the Intellectuals.” Pp. 43-57 in *On Morality and Society, The Heritage of Sociology*, edited by R. N. Bellah. Chicago: University of Chicago Press.

Durkheim, Émile. 1984 [1893]. *The Division of Labor in Society*. New York: Free Press.

Durkheim, Émile. 2001 [1912]. *The Elementary Forms of Religious Life*. Oxford, UK: Oxford University Press.

Espeland, Wendy Nelson, and Michael Sauder. 2007. "Rankings and Reactivity: How Public Measures Recreate Social Worlds." *American Journal of Sociology* 113(1):1–40.

Eubanks, Virginia. 2018. *Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor*. New York: St. Martin's Press.

Foucault, Michel. 1977. *Discipline and Punish: The Birth of the Prison*. New York: Vintage Books.

Foucault, Michel. 1990. *The History of Sexuality, Vol. 2: The Use of Pleasure*. New York: Vintage Books.

Foucault, Michel. 2000. "Questions of Method." Pp. 223–38 in *Power, Essential works of Foucault 1954-1984 / Michel Foucault*, edited by J. D. Faubion. New York: New Press.

Fourcade, Marion, and Kieran Healy. 2017. "Seeing like a Market." *Socio-Economic Review* 15(1):9–29.

Fraenkel, Béatrice. 1992. *La signature, genèse d'un signe*. Paris: Gallimard.

Gandy, Oscar H. 1993. *The Panoptic Sort: A Political Economy of Personal Information*. Boulder, CO: Westview.

Garfinkel, Harold. 1984. "Passing and the Managed Achievement of Sex Status in an Intersexed Person: Part I." Pp. 116–85 in *Studies in ethnomethodology*. Cambridge, UK: Polity Press.

Giddens, Anthony. 1990. *The Consequences of Modernity*. Stanford, CA: Stanford University Press.

Goffman, Erving. 1955. "On Face-Work: An Analysis of Ritual Elements in Social Interaction." *Psychiatry: Journal for the Study of Interpersonal Processes* 18(3):213–31.

Goffman, Erving. 1959. *The Presentation of Self in Everyday Life*. New York: Anchor Books.

Goffman, Erving. 1963. *Stigma: Notes on the Management of Spoiled Identity*. New York: Simon and Schuster.

Goffman, Erving. 1969. *Strategic Interaction*. Philadelphia: University of Pennsylvania Press.

Goffman, Erving. 1971. *Relations in Public: Microstudies of the Public Order*. New York: Basic Books.

Hacking, Ian. 1995. "The Looping Effects of Human Kinds." Pp. 351–94 in Causal Cognition: A Multidisciplinary Debate, edited by D. Sperber, D. Premack, and A. J. Premack. Symposia of the Fyssen Foundation. New York: Oxford University Press.

Hacking, Ian. 2007. “Kinds of People: Moving Targets.” Proceedings of the British Academy 51:285–318.

Haggerty, Kevin D., and Richard V. Ericson. 2000. “The Surveillant Assemblage.” *The British Journal of Sociology* 51(4):605–22.

Harper, Annie, Tommaso Bardelli, and Stacey Barrenger. 2020. “‘Let Me Be Bill-Free’: Consumer Debt in the Shadow of Incarceration.” *Sociological Perspectives* 63(6):978–1001.

Hill, Kashmir. 2020. “Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match.” *The New York Times*, December 29.

Hyman, Louis. 2013. *Debtor Nation: The History of America in Red Ink*. Princeton, NJ: Princeton University Press.

Igo, Sarah. 2018. *The Known Citizen: A History of Privacy in Modern America*. Cambridge, MA: Harvard University Press.

Jerolmack, Colin, and Iddo Tavory. 2014. “Molds and Totems: Nonhumans and the Constitution of the Social Self.” *Sociological Theory* 32(1):64–77.

Jones, Meg Leta. 2020. “Cookies: A Legacy of Controversy.” *Internet Histories* 4(1):87–104.

Kellogg, Katherine C., Melissa A. Valentine, and Angèle Christin. 2020. “Algorithms at Work: The New Contested Terrain of Control.” *Academy of Management Annals* 14(1):366–410.

Krippner, Greta R. 2017. “Democracy of Credit: Ownership and the Politics of Credit Access in Late Twentieth-Century America.” *American Journal of Sociology* 123(1):1–47.

Latour, Bruno. 1988. “Mixing Humans and Nonhumans Together: The Sociology of a Door-Closer.” *Social Problems* 35(3):298–310.

Lau, Estelle T. 2006. *Paper Families: Identity, Immigration Administration, and Chinese Exclusion*. Durham, NC: Duke University Press.

Lauer, Josh. 2017. *Creditworthy: A History of Consumer Surveillance and Financial Identity in America*. New York: Columbia University Press.

Liu, Chuncheng. 2021. “Seeing Like a State, Enacting Like an Algorithm: (Re)Assembling Contact Tracing and Risk Assessment during the COVID-19 Pandemic.” *Science, Technology, & Human Values* doi:01622439211021916.

Lyon, David. 2009. *Identifying Citizens: ID Cards as Surveillance*. Malden, MA: Polity.

Magnet, Shoshana Amielle. 2011. *When Biometrics Fail: Gender, Race, and the Technology of Identity*. Durham, NC: Duke University Press.

Marres, Noortje, and David Stark. 2020. “Put to the Test: For a New Sociology of Testing.” *The British Journal of Sociology* 71(3):423–43.

Marx, Gary T. 2001. “Identity and Anonymity: Some Conceptual Distinctions and Issues for Research.” Pp. 311–27 in *Documenting Individual Identity: The Development of State Practices in the Modern World*, edited by J. Caplan and J. Torpey. Princeton, NJ: Princeton University Press.

Marx, Gary T. 2016. *Windows into the Soul: Surveillance and Society in an Age of High Technology*. Chicago: The University of Chicago Press.

Mauss, Marcel. 1985 [1938]. “A Category of the Human Mind: The Notion of Person; the Notion of Self.” Pp. 1–25 in *The Category of the Person: Anthropology, Philosophy, History*, edited by M. Carrithers, S. Collins, and S. Lukes. New York: Cambridge University Press.

McKeown, Adam. 2008. *Melancholy Order: Asian Migration and the Globalization of Borders*. New York: Columbia University Press.

Nair, Vijayanka. 2021. “Becoming Data: Biometric IDs and the Individual in ‘Digital India.’” *Journal of the Royal Anthropological Institute* 27(S1):26–42.

Noble, Safiya Umoja. 2018. *Algorithms of Oppression: How Search Engines Reinforce Racism*. New York: New York University Press.

Noiriel, Gérard. 2001. “The Identification of the Citizen: The Birth of Republican Civil Status in France.” Pp. 28–48 in *Documenting Individual Identity: The Development of State Practices in the Modern World*, edited by J. Caplan and J. Torpey. Princeton, NJ: Princeton University Press.

Porter, Theodore M. 1996. *Trust in Numbers: The Pursuit of Objectivity in Science and Public Life*. Princeton, NJ: Princeton University Press.

Rao, Ursula. 2019. “Population Meets Database: Aligning Personal, Documentary and Digital Identity in Aadhaar-Enabled India.” *South Asia: Journal of South Asian Studies* 42(3):537–53.

Read, Max. 2018. “How Much of the Internet Is Fake? Turns Out A Lot of It Actually.” *Intelligencer*. https://nymag.com/intelligencer/2018/12/how-much-of-the-internet-is-fake.html.

Robertson, Craig. 2009. “A Documentary Regime of Verification.” *Cultural Studies* 23(3):329–54.

Robertson, Craig. 2010. *The Passport in America: The History of a Document*. New York: Oxford University Press.

Roderick, Leanne. 2014. “Discipline and Power in the Digital Age: The Case of the US Consumer Data Broker Industry.” *Critical Sociology* 40(5):729–46.

Rule, James B. 1973. *Private Lives and Public Surveillance*. London: Allen Lane.

Rule, James B., Douglas McAdam, Linda Stearns, and David Uglow. 1983. “Documentary Identification and Mass Surveillance in the United States.” *Social Problems* 31(2):222–34.

Scott, James C. 1998. *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*. New Haven, CT: Yale University Press.

Social Security Administration. n.d. “Social Security Number Randomization.” https://www.ssa.gov/employer/randomization.html.

Tantner, Anton. 2009. “Addressing the Houses: The Introduction of House Numbering in Europe.” *Histoire & Mesure* XXIV(2):7–30.

Tavory, Iddo. 2010. “Of Yarmulkes and Categories: Delegating Boundaries and the Phenomenology of Interactional Expectation.” *Theory and Society* 39(1):49–68.

Todorov, Alexander, Christopher Y. Olivola, Ron Dotsch, and Peter Mende-Siedlecki. 2015. “Social Attributions from Faces: Determinants, Consequences, Accuracy, and Functional Significance.” *Annual Review of Psychology* 66(1):519–45.

United States, Transportation Security Administration. 2008. “Secure Flight Program.” *Federal Register*, October 28, 64,018.

Veyne, Paul. 1997. “Foucault Revolutionizes History.” Pp. 146–82 in *Foucault and his interlocutors*, edited by A. I. Davidson. Chicago: University of Chicago Press.

Zerubavel, Eviatar. 2020. *Generally Speaking: An Invitation to Concept-Driven Sociology*. New York: Oxford University Press.

Zuboff, Shoshana. 2018. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. New York: Public Affairs.

Table 1. Analytic framework for the study of personal identification

Concept	Sensitizing sociologists to…
Interchangeability and mutability	The range of variation in what constitutes identification.
Object – dividual	The inherent gap between embodied individuals and their surveillance representations.
Disembedding	How identification practices disentangle potential identifiers from local context, thereby reversing the relations of power/knowledge.
Standardization	The fact that identification mainly consists of minimizing the interchangeability and mutability of dividuals.
Reembedding	The persistent tradeoffs and limits faced by practices of identification as they seek to make individuals resemble their dividuals.
Agency – actor-network	The potentially divergent interests and changing configurations of relations between the parties involved.
Access points	The tension concentrated in the position of frontstage staff.
Coalitions	The tradeoff between how much is known about the individual and who has access to this knowledge.
Responsibilization	The need to secure the cooperation of individuals in the creation and maintenance of their own dividuals.
Technique – testing	The uncertain and interactive nature of identification.

Baseline	The mechanisms involved in differential allocation of credibility to data.
Expert judgment	The crucial role of potentially fallible expert judgment.
Interactivity	How resistance and creative adaptation reshape identification practices in unexpected ways.