Interview with Aleksandra Kaminska

Maria Eriksson, Guillaume Heuguet, Aleksandra Kaminska

Interview with Aleksandra Kaminska

By Guillaume Heuguet and Maria Eriksson
Guest editors, Internet Histories

Interview with Aleksandra Kaminska

Aleksandra Kaminska is an Assistant Professor in the Department of Communication at the Université de Montréal, Canada, where she also co-directs the Artefact Lab and the Bricolab. Her research is based in media studies and aesthetics, and the history of technology. She is currently preparing *High-Tech Paper: Security Printing and the Aesthetics of Trust*, a monograph that examines the making of authentic paper for circulation in secure systems and infrastructures. She situates security printing within media and printing histories, but also as it intersects with art, craft, and design. Her work on authentication devices includes the production of *Nano-verses* (nano-verses.com), an art-sci collaboration that explored how the technology of nano-optical authentication can be rethought as artistic media. The articles discussed in the following interview are: "Storing Authenticity at the Surface and into the Depths: Securing Paper with Human- and Machine-Readable Devices" (*Intermédialités*, 2018); "'*Don't* Copy That': Security Printing and the Making of High-Tech Paper" (*Convergence*, 2019); and "The Intrinsic Value of Valuable Paper: On the Infrastructural Work of Authentication Devices" (*Theory, Culture & Society*, 2020). She recently co-edited an issue of *PUBLIC: Art/Culture/Ideas* on "Biometrics: Mediating Bodies" (2020), and is currently finalizing a co-edited volume of the *Canadian Journal of Communication* on the theme of "Materials and Media of Infrastructure." In 2020–2021 she is co-organizing the online series Paperology: A Reading and Activity Group on Knowing and Being with Paper.

Your work centers on efforts to secure the authenticity and identity of things and highlights how material standards contribute to the ordering of the world. In much of your writings, you place focus on techniques for identifying analog objects such as money and documents/valuable paper but we have also found your work to be highly stimulating for thinking about efforts to identify digital content like moving images and sounds.

In "Storing Authenticity at the Surface and into the Depths" you introduce the concept of "authentication devices" to discuss the role and function of identification techniques. Could you explain a bit more about what you mean by this concept and how/why you think it is useful for thinking about strategies of identification?

Thank you for the opportunity to talk to you about this work, and especially in this context that brings it in conversation with today's digital and online technologies. Let me start with some background on some of the concepts and questions that animate this research before delving into the details of the question.

"Authentication" is derived from the Greek word *authentikos*, meaning original, real, or genuine. In popular culture and speech, we tend to apply it to the idea of *being* authentic, as a manifestation of someone identity through appearance or performance for example. This is somewhat different or less precise than when we use notions of authenticity to assess or describe knockoff products, fake documents, and other counterfeited and forged material things. In these cases, there are physical qualities that materially define the "real" version, so that what become significant is the processes of authentication, or the way that authenticity is determined. What do we *do* when we authenticate? What is there *to* authenticate? How do evaluate, verify, validate? Authentication in these instances is this process of verifying an object's genuineness and legitimacy based on certain hallmarks and predetermined characteristics. This applies to things, but also to individuals when there is a need to verify an identity using documents and prove that the identifying information a person gives is accurate.

People have been authenticating before even thinking of it as such. The question or problem of how to distinguish fakes, forgeries, counterfeits and counterfeiters, and illicit reproductions of all kinds, has a long history in human culture. Today's digital environment provides new challenges as well as opportunities. The big problem of knowing "what is true" has become a question for those interested in content and information and well as those looking for material evidence, inscriptions, and traces. I'm interested primarily in the latter, and I tend to gravitate towards artefacts and things. Quickly my project developed a more historical perspective than I expected. I began with the sophisticated technologies of nano-optics (for the *Nano-verses* project), but it was clear that to understand what was happening and why—in terms of both the technology and how it was being used—I had to go back in time. And when I considered the variety of goods that circulate as real/fake, whether computer chips or medical supplies, I also ultimately ended up with the technologies that brought us the questions of copies and technological reproduction, printing and paper. So this is how I came to anchor this project around paper, but a paper that evolves and changes and becomes highly complex. The newest technologies to protect paper are used for banknotes and passports, but there is wide assortment of papers that must function with authority: mailing stamps, tax stamps, certificates of all kinds (including certificates of authenticity themselves), branding labels, bonds, identification documents, official documents, etc. We are surrounded by such papers even though we rarely stop to think about the technologies that they put to work. We could say that official structures and systems—whether of bureaucracies, states, institutions, industries—must continuously communicate, affirm, and reproduce their legitimacy, and they do so in part through the material things they produce.

There might be an impression that the materials problems of paper are of a different time. On the one hand there is the discourse of the paperless society, which tells us we should no longer have to worry about how authenticity is inscribed through paper (and paper-like things which co-exist alongside cellulose-based paper such as polymer-based paper), because paper itself is becoming obsolete. And there is no denying we have shifted many things outside of the realm of paper. But a paperless world is still largely one of the future. Yes, there are examples to the contrary, including the nearly cashless society in Sweden, the

increase of cashless payments during the COVID-19 pandemic, or workers being implemented with chips so that they no longer have to physically punch in. But it is worth remembering that going cashless is an equity issue: 1.7 billion adults in the world are still unbanked, according the most recent report from the World Bank (Demirgüç-Kunt, A. et al., 2018), which means they operate on cash. We also know that it is still essential to have an identification document like a passport to be recognized as a person—without such papers we are no one belonging nowhere (as is so well denoted in the French expression *les sans papiers*). Meanwhile, according to the Organisation for Economic Co-operation and Development, $509 billion, or about 3.3% of all trade worldwide, was based on counterfeit and pirated goods (OECD, 2019). All of this indicates that, at least for now, we still have to worry about how authenticity is inscribed in the physical world of things.

Coming from media studies, I started to question how we mediate authenticity, and as I mentioned, my interest in how we authenticate rapidly took on a historical scope. I noticed certain technical and aesthetic strategies used across time but, scanning my background, I recalled very few encounters with the topic and techniques of authentication. As I imagine is the case for many with a similar communications and media studies trajectory, the closest I came was trough Walter Benjamin's discussion of technological reproducibility and the aura, which does not really work once the object becomes a banknote rather than a painting, or even once the object becomes the painting's authentication certificate, rather than the painting itself. So I turned elsewhere: art history; theories of the copy; personal accounts of counterfeiters and those who tried to catch them; histories of printing, books, ephemera—and the list goes on. Also very helpful were historical accounts of figures and printers, which give us a wealth of information about how, why, and what it took to go from "mere" printer to *security* printer, or what was also called a printer of fine or luxury paper. Following the story of De La Rue (the world's largest security printer today) is a good example: the company began by printing a newspaper, in 1813, and gradually moved to the printing of playing cards, greeting cards, and eventually stamps, banknotes, and passports. The move came from an interest in printing well, with quality rather than quantity, and in developing new technologies and techniques—motivations which allow us to

understand how making paper valuable, unique, and trustworthy became hallmarks for the production of authentic papers.

Ultimately the security printer develops a variety of devices that makes his paper "secure." As I noted, banknotes and passports are the most sophisticated objects produced by the industry of security printing and they are the ones for which we will develop, integrate, and introduce the newest techniques. Today these include advanced optical imaging using new forms of holography and nanotechnology, magnetic threads, or UV printing, on top of older strategies like microprinting, complex engravings, unique inks, watermarks, and substrates. So even though we don't tend to think of paper as a site of technological development (security printing itself is not an industry the general public knows much about), delving into the world of security printing is a real eye opener. Security printers for instance have their own R&D departments, which develop new features for their clients. I started thinking of these documents as "high-tech paper" to emphasize their perpetual technological newness, one which of course comes from the need to remain one step ahead of everyone else. Why is it that you and I can't reproduce our own passports or banknotes with our photocopier? We all know this to be the case—somehow we learn this early in childhood—and the reason is the material specificity of secure papers. So I started here, trying to understand what constitutes this specificity, and to then "translate" these technologies and the way they have been written about, for media scholarship. Using our histories, theories, and conceptual baggage, how do we, media scholars, address authentication, or what we could describe as the technologies and process of mediating authenticity from an institutional authority to a stored material inscription?

In the industry and labs that produce these technologies today, authenticating elements are commonly referred to as devices or features. A "feature" is a rather generic term, but a "device" describes a function and I thought could open up some more doors in terms of an analysis. I started working with this notion of the device primarily, even if I use it more broadly than a scientist might. One challenge however is that, interestingly, "device" (at least in English), has not been given the same pronounced analysis as other terms that refer to technologies—machine, tool, instrument, *dispositif*, apparatus, system, etc. What

quickly became clear however is that the device is understood in relationship to its function, to what it *does*, and this made sense in the case I was interested in: the features are securing by assuring and mediating authenticity, trust, and value.

The concept of the device allows us to think about the many ways that authenticity is mediated. There are some techniques that are designed explicitly for this—microprinting for example. But if we think more broadly, an authentication device is also the *feel* of the paper that is used, the *quality* of the specimen. These are constituted through technologies of papermaking and printing. Historically the content has also been shown to play this role: for instance, in his recent *Banknotes and Shinplasters* (2020), Joshua Greenberg examines the thousands of specimen that circulated in the United States in the 19th C. He argues that one way that individuals could distinguish real notes from fake ones was through the images that were used: did an image make sense in the area that it was being used? For example, an image of Niagara Falls on a note produced in California makes little sense, and would trigger some suspicion. In such an instance, the choice of the image itself could work as an authenticating device. These days reproducing the content is not a reliable way of assessing veracity; what is however, is reproducing it *well*, with exactly the same techniques, tools, and skill. This is one way to explain the usually ornamental (i.e., complicated, finicky, fine) aesthetic produced by security printers, as is the layering or multiplicity of devices used on a singular document. It's worth noting here also that people today rarely bother *reading* the text in papers like banknotes, a point that was meant brilliantly by a recent case in Australia, where a note was released with a typo in the microprint that wasn't noticed for six months (BBC, 2019)!

In *Storing Authenticity at the Surface and into the Depths*, my aim was to present large categories of authentication devices based on how they can be read, or what we could call different layers of legibility. Devices that can be verified by a human reader are "at the surface," meaning that they can be fully assessed by the human senses. Devices with their authenticating information stored in such a way that it can only be read by a machine are "into the depths," which keeps authenticating information inaccessible or hidden to human senses. An example of

this could be a biometric chip, like those found in some passports, which can be felt and maybe seen, but this sensory detection is not key to its function: rather, it works only when it is scanned and matched to a database entry, making convincing link. A third type of device works as a hybrid: information can be made sensible on the document itself to the human verifier, but only with the aid of a special reader. This is the case with UV printing, for example. Ultimately what this means is that authenticity is inscribed at many levels and layers, and unevenly accessible to different readers.

As well as becoming unevenly distributed, this process is also increasingly automated: when going to passport control, we are often now told to use a machine that will scan both our document and do a biometric reading. There are two things happening: the ID document is authenticated by the machine reader, and there is confirmation, through a biometric like the iris, that this passport belongs to this passport holder. This means that the passport could be authentic insofar as it is a genuine document produced by a state, but the person presenting the passport still has to prove, or identify, themself, as the rightful owner. The chip as authentication device thus works to both confirm the legitimacy of the passport and the passport holder, and is largely considered now as a decisive authentication device in passports. Devices like the chip also complicate the status of security papers as analog technologies: rather, we see that paper can be connected, inscribed with invisible and coded information, and digitally augmented.

The web is in part exciting because of the freedom people have there to be whoever they want to be, or choose to hide who they are, or change their persona from one day or site to the next. In many instances moments of identification are not tied up to any authenticating mechanism: at the surface at least, we can use a collection of avatars, usernames, and passwords for our pseudo-selves; fake names, birthdays, locations; and we know that is only the tip of the anonymous web's iceberg. Unfortunately, abuses to the system have often emphasized the dark side of anonymity with problems like trolling, catfishing, or deep fakes. Yes, these can be forensically discredited, but this kind of work is not accessible to the average web user. This is not to say that there are no authenticating mechanisms

online: they are there, but not consistent: we could think of the verified accounts on Twitter or the requirement by Facebook to use our real name, secret questions, double-verification processes with an email or phone number, a connection to biometric information such as voice or fingerprint, or in official instances such as government sites, codes and confirmations sent to a physical address. Identity is so loose online, identification can only be meaningful if it is also authentication.

Your work highlights the transition from manual (humanly-readable/ visual/tactile) to automated (computer-readable/covert/non-visual) identification techniques. How would you describe the cultural, political, and economical changes that this shift has brought about? What continuities and ruptures exist between analog and digital techniques for identifying content?

The automation of authentication—and by extension of identification—is part of the longer history of automation rooted in the technological shifts of modernity and Industrialization. It illustrates a desire for efficiency and expediency that underpins the logic and need for standardization and classification. It also illustrates our collective "decision" to trust machines, and not only that, to trust them more than we trust human judgment and the human senses, and thus each other. How do we assess the consequences of such a change? Does it matter that the things that used to mean something, like someone's word, have little value (or currency, to put it differently) today? Then again, as we usually tend to do, it is easy to make idealistic assumptions about the past, but there are more continuities than we might think.

One of the first texts I read that dealt with the history of banknotes and the problem of authenticating paper is "The Aesthetics of Authenticity: Printed Banknotes as Industrial Currency" by Frances Robertson, to which I have since returned many times. In it she writes about the moment of passage, in England, from metal coins to paper currency. The material and "public relations" challenge of paper was that, unlike coins, it was not perceived to have any intrinsic value (coins were in principle equivalent to their worth). Robertson goes on to analyze how value was created, and how, with the right techniques, paper currency would come to circulate legitimately and be recognized as such by the public. To make a long story short, one of the important techniques that was

used, a hallmark of old currencies, was the geometric lathe pattern produced by the rose engine (these are the circular patterns that look like spirographs). Using a rose engine meant that patterns were made with "machine-like" precision, each one identical to the next. The ornate circles, which are still present on most currencies, had to be made by specific machines, and could not be produced otherwise. The result, Robertson argues, is that from this moment the public learns to shift their trust to the machine aesthetic (mechanically drawn and industrially reproduced)—the regularity of the machine-made form—replacing the trust once reserved for marks of individuals hands and craftsmanship. The expectation of precise repetition of forms allowed for comparison and evaluation, since noticing anomalies became an easier way to assess difference; with the handmade, anomalies made it impossible to evaluate whether the difference was within the accepted range of variation, or if it was evidence of an illicit reproduction. Identical copies beget standardized forms, which opens the door to automation.

Automated identification (through automated authentication of documents) has its consequences. For one, it leaves little room for abnormalities, circumstances that require a human sensibility, care, or empathy, and the possibility of making exceptions, or turning a blind eye. We have all been frustrated by bureaucratic systems, or bureaucrats themselves, that refuse to bend the rule, to open up a category, or to, we might think, use common sense or judgment. Automation doesn't care. Second, automation must be programmed, and programs like programmers, as we know, have biases. There are possibilities of discriminating "results" that, because they are produced by the "objective" machine, are hard to contest. This is being well documented these days in all the fantastic work on algorithmic bias. But to bring it back to the previous point, this is possible because of an ongoing "mechanical objectivity," as Peter Galison and Lorraine Daston memorably put it, a belief that machines are more trustworthy than human perception.

Secure papers use analog, digital, and hybrid authentication devices, and the distinctions are not always clear-cut. Even if they are experienced as analog (e.g. images that use nano-optical technologies have effects seen by the naked human eye), they are built using many digital machines and tools, their colour is produced very differently than printed images or holographs, and this is revealed, notably, when they are magnified. As

this example shows, when dealing with paper thinking the differences between analog and digital devices in terms of categorical ruptures is tricky. I'm less interested in sorting devices as either analog or digital, than in discerning the continuities of the aesthetic logics of authentication devices across devices and through time: what are the overarching features of secure papers? What formal and aesthetic ideas have we been consistently working on and perfecting? Are these mutating or disappearing in digital environments? What are the material traits we invariably if unconsciously associate with "officialdom" and particularly official documents"? What insights can we glean from security printing that might apply to the challenges of digital security?

One such overarching principle I briefly noted already is ornamentation, or the ornamental quality that has long characterized official papers. While there are exceptions (such as the notable minimalism of Norway's 2017 banknote series), security printing has for the most part retained a 19th century aesthetic, what Finn Brunton describes as a "deliberate archaism of banknotes" (2019, p. 22). There are various ways to explain this, whether as a call back to the authority of history or an appeal to what is familiar—in any case, it is not worth undoing. Indeed, since individuals must know what a true document looks and feels like, it is useful to be able to draw on some longstanding characteristics. This is why, for example, American bills have always been printed on the same paper produced by the same papermaker. This paper is no longer the most sophisticated, but it is so recognizable, and so much associated with the "greenback" that no one dare change it… It just wouldn't feel right. The same goes for the particular green ink.

Another principle would be the camouflaging of information. This can happen in many ways, by making small or invisible. At the surface examples include microprinting (e.g., microtext or micro dots) or watermarks. A more recent hybrid device would include UV inks or some nano-optical features. Digital devices and encoded information are in a way all about hiding, so much so in fact that our human senses cannot reach the information. We can also note the strategies of matching halves and the cut, which are sometimes used together, but not always. This includes artefacts like indentured contracts and carbon copies, but also unofficial paper currencies that cut a designated paper. This was done with playing cards in the 17th century as a way to prove a transaction, and it continues to be a method communities draw on today. For instance,

in the Gaspé region of Quebec, an unofficial currency called “la demi” (“the half”) cuts in half official Canadian banknotes (halving their value by the sake token). These halves have no value outside of the communities that recognized “a half” as currency, those assuring that money circulated within, rather than out of, the local economy.

The signature is a good example of a device that teeters ambiguously across the analog-digital divide, and one that we still use widely to mark documents. It is a device that is or looks like the handwritten, and it generally accepted as an individual’s marker and sign, even though a signature can be quite irregular in practice. The resilience of the signature as a trustworthy inscription is actually very impressive if we consider how unsecure it is: a forgery might not pass a forensic text, but probably neither would the signature we quickly squiggle on touchscreens, to name just one flagrant instance of common signature-distortion. There is much to be said on the signature, but let me just leave it here by noting that we still use unverified signatures in the digital realm even though we could use much more secure methods.

What we do know is that the human body, rather than, for instance, someone’s word, has come to speak for us, and continues to do so, at times despite our own will. We can see this today in all the uses of biometric identification systems: whether it is using the fingerprint, iris, face, voice, gait, heartbeat—it is the body that identifies. This then can be used by states and institutions as a tight link, a guaranteed authentication mechanism between a body and the document it carries, but even more broadly, between a body and the data stored about that body. This is probably one of the main differences with machine-read information and assessment: that we do not necessarily know what information is stored about us and by whom. My bank, for example, now uses my voice to identify/authenticate me, yet I don’t have a recollection of clearly consenting to this: one day I called and no longer had to go through the interminable identification process based on a series of questions. Rather, I was “benefitting” from the expediency of the voice recognition programme. But there are many ethical and legal questions raised by these tools, and we are only beginning to scratch the surface: what happens if my voice is deep-faked? Or if it used to determine I have a medical condition, which is then communicated to my insurance and my employer, among others? Or if it is manipulated in such a way to fake a condition? These aren’t farfetched scenarios. A recent story on a biometric shoe insole that could be used to “record an individual’s unique way of

standing, walking, running, or gait" and then link this to their identity was described as potentially useful for "Health Insurance and Health Care providers, Corporate Security providers, Banking Service providers, Government and Military, as well as individuals and athletes" (Pivcevic, 2020; style in original). But why exactly would my bank want information about my gait? My body speaks for itself, but it might say more about me than I would like, and that, often, I am legally allowed to keep private. So if the body can't be trusted, and its data is used in illegitimate ways, how to maintain control over our identity and ourselves?

What would you say are the biggest political consequences of the shift from manual to automated ways of securing authenticity? What is at stake in the increased reliance on algorithmic and machine-assisted strategies of identification?

It is true that some automated forms of authentication are becoming increasingly important. The biometric chip in a passport is one such example. But it would not be entirely accurate to speak of a complete shift from manual to automated because the two continue to co-exist. In everyday life, most ID cards are not biometrically-augmented, but rather rely on human judgment. A store clerk might ask himself whether the photograph looks like the person standing in front of them, if they look to be the age indicated, if the card itself is a legitimate card, and all of this in a matter of seconds. There is a person making the decision, and this person could bend the rules or make mistakes, make things easier or more difficult. What machine-reading offers—for better or worse—is consistency, and this is in part why machines are "trustworthy". We can trust they will give us the same result each time since they are simply executing a protocol (more would have to be said for machine intelligences, but we will leave that for another discussion). Since there is still a public perception that information provided by machine-reading is neutral, impartial, and free of the machinations of human politics, we could say then that at stake in machine-automated identification is that the impression of consistency masks the humanness of a system that is written by people, using information they obtained, classified, deemed important, *etc*., with all of their biases and subjective motivations, and within specific historical contexts and ideological frameworks. One dangerous outcome is that we lose the capacity to argue,

evaluate, or assess outside of machine-based results, ultimately rendering us powerless in the face of the "judgment" provided by the machine. What if a machine hasn't been updated? What if there's a bug? What if it can't read me for whatever reason? What if it's mistaking me for someone else but I can't prove it? Rendering a decision is one thing but proving it is still another. Being able to prove or disprove who we are, to argue, explain, point out discrepancies, argue (in the sense of applying a logical argument) or appeal to human sensibility or empathy, these are perhaps some or the things at stake when we leave things up to automation.

In *Don't Copy That: Security Printing and the Making of High-Tech Paper* you argue for the need to study media technologies that "work to maintain and secure (social, political, economic) order." Elsewhere, you have also located authentication and identification techniques within the history of governance, management, and administrative logics. Could you expand on how you conceive the relation between identification technologies and administrative/bureaucratic rationalities? How do authentication devices tie in with broader historical efforts to organize, supervise, and index things/information?

The arguments I make around this build on the invaluable existing research that has mapped the co-evolution of identification practices and techniques with those of governance, management, and administrative logics. While identification documents are just one type of document I'm looking at, they function in a particular way, and one that, as we just mentioned, eventually leads to today's deployment of biometric devices. The important thing for me is not to rewrite or retell this story, but to understand it within the changing practices of authentication, and specifically in relation to the development of devices that are used to inscribe and communicate trust, value, and authenticity.

The story of Alphonse Bertillon is probably familiar to many of readers, but it is still worth mentioning here since it is an important contribution. Briefly, working as a clerk in a Paris police station at the turn of the 20th C, Bertillon developed a systematic way of identifying persons based on the anthropometrics, or the measurements, of their body. As Simon Cole recounts in his book on fingerprinting *Suspect Identities* (2002), Bertillon was trying to solve an administrative problem: in a world that has yet to issue

identification documents to all of its citizens, how do we keep track of prisoners, and especially recidivists? The system in place at the time was to organise prisoners' files by name, but names are changed on a whim if there is no document to prove otherwise. The result was the same individuals kept coming back, creating a new name, and thus requiring a new file, each time. Bertillon's idea to link the identity to the body would characterize an individual based on a set of data that could be compared against the data of all those on record. This is a very managerial way of understanding and classifying individuals, around a certain set of measurable facts, and it is the same logic that is used today. Bureaucracies need efficient, standardized, and preferably automated modes of verification: things like narratives, family connections, or someone's word require time and a case-by-case approach, all in a technological environment that precisely seeks to eliminate human judgement and assessment. With time, we have become used to being identified by numbers, and to being treated accordingly. Having chips embedded in our bodies by our employer is becoming an increasingly small leap to make. And this is just one example of how we have completely bought into a desire for efficiency, especially when tied to productivity.

We know, however, that the administrative world can also be frustratingly inefficient, and this often correlates with paper-based systems. It would seem few professions have clung to paper and the human signature as much as law and real estate (Graham, 2020). Sign here, initialize there, and please do so in triple sets, each original copies, etc. So we live very much in a hybrid world, one where we can pay our taxes online, and have our faces scanned at airports, but also where, as we saw recently in the US, we must sign a mail-in voting ballot, or physically go to a notary to sign paper documents.

There are also many, many, other kinds of organizational systems that rely on identification and authentication technologies. Infrastructures of global circulation monitor the movement of goods from point A to point B, from seller to buyer, so that the right things arrive at the right place. Goods particularly affected by counterfeiting such as medical supplies, brand name luxury products, cigarettes, or electronics, need to maintain the value of their products. As they pass through verification points such as ports, which are part of the logistical systems of global shipping, containers with goods are scanned to check their contents, or a tag might

be scanned to check the history of all previous verification/scan points, thus being able to verify that this container has indeed followed the rightful trajectory. Ultimately the goal is to make sure that the container is not full of dupes.

In *Storing Authenticity at the Surface and into the Depths,* you talk about the importance of "biographical pedigree" that are included in devices such as RFID tags. Do you see pedigree as being a more current, maybe more and more dominant, criterion for authenticity? How would you locate emergent technologies such as blockchain projects within the longer genealogy of authentication devices?

It's interesting that you phrase your question around an idea of pedigree being potentially more current. In the sense that I used the term I had in mind rather the modern European towns and villages Valentin Groebner writes about this in his fantastic book *Who Are You?: Identification, Deception, and Surveillance in Early Modern Europe* (2007), which would have us think the pedigree as a return to something past. As he points out, in such settings a person's identity could be vouched by someone already known to the community, or they could be identified as someone's family member. This was proof enough. But as one travelled and needed to be granted passage through each village, they had to show documents which would identify them and justify their trip. Only once this was approved would they be granted passage (this could take the form of a letter that itself communicated authenticity—the precursor of the passport).

In the context of a village, then, people could know who everyone is, or at least know who was in which family. Someone's profession could also play such an identifying role—Groebner for instance notes that people's clothes could be more pertinent than their face since this is what identified them as merchants or tradespersons of specific goods, and this is what was considered the most significant identifying information. So by biographical pedigree I have in mind this information about someone's life that becomes used to make sense of who they are—their relations, where they are from, what they did or do—in a way that, in a given moment in time, was considered identification enough.

If we were to place blockchains as part of an overarching strategy of authentication, perhaps they could be thought, in a broad sense, as also constituted and vetted through their past or "life story," in the sense of being built and affirmed with each recorded transaction. This is not unlike a notion of pedigree, where the record of ancestry provides credibility. These constitutive records that depend on each other are perhaps analogous to our families, neighbours, or communities vetting for us. In other words, in such systems we are entangled with others and become less trustworthy when we are free agents.

You show that authentication devices have to be secretive and partly situated outside of public scrutiny to be efficient, yet at the same time there needs to be a global trust without which they can't fulfil their mission. How do you think the production of trust has evolved with the materiality of authentication devices? And is there a space for an ethnographic study of the production of trust through technology?

That's a very interesting question. Trust is, as we've been mentioning, essential in the enterprise of identifying and authenticating. If we return to the beginning, surface devices allow each person to evaluate what is passing through their hands. This is what is called the "first level assessment"—the public's ability to assess whether the authenticating device is legitimate. With time, as counterfeiters catch up with techniques, issuers of secure papers have had to introduce new devices and educate the public accordingly. If we consider trust as an outcome of the material qualities of secure paper, then the public needs to understand the authentication devices used in these papers and how to assess them.

For banknotes and passports, it is the government's job to teach us about new devices and how to evaluate them. They produce brochures and websites that teach us what to look for. Importantly though, only a small subset of devices is revealed to the public, while the rest is meant for specific readers. Some devices are made known only to particular evaluators—bank tellers, or passport control officers, for example. There are also devices that are just for the issuers themselves. This is the layer that is difficult to research in real time. If we return to the discussion on machine reading however, we are already aware that certain elements are no longer

fully known to us, and this in itself perhaps fuels mistrust: not mistrust in the authenticity of the document, but mistrust in the institution itself.

How do we study, and can we even study, the production of trust through technology? Turning back to documents provides some historical clues about how trust was built to begin with. Security printing indeed emerged from a need to create paper that would be trusted by the public, that would be considered valuable. As we shifted from coins to paper in the 19th century, people had to be convinced a material they considered to be flimsy, quotidian, banal—paper—could be worth something. Out of this need offshoots a whole branch of the printing industry, one interested in creating perfect, genuine, and innovative paper things. These were the qualities that came to stand in for trustworthy, official paper. This was "fine" paper that was materially and sensorially *different* than the newspaper or the paper used to wrap groceries. A historical approach brings out the ongoing principles or logics that are used by security printers to produce trust. I mentioned a few examples here with principles like quality and material specificity, and strategies like ornamentation, concealment, cuts, and halves. To what extent to these continue to function as authenticating mechanisms, in and outside of the paper realm?

There are limits to what we can access about the present of security printing, but this does not make it impossible to study. The industry is secretive, but it still has a presence. Some security printers have websites that provide a wealth of information, not because they giveaway their technical secrets, but because they present a world of concerns that has been largely under-examined in media scholarship. Through these sites we can enter into the discourse of security printing and we immediately get a sense of the challenges and objectives that have to be met. We see how devices are being positioned and marketed, the rhetoric that is used, where emphasis is given—and the whole purpose of this messaging is to convince the reader that the end-result are technologies of trust and security. This is of course just one kind of work that can be done, and scholars from a number of disciplines are looking at how official documents are made to function authoritatively. I also highly recommend Anna Weichselbraun's work on the production of trust. As an anthropologist she did indeed do a year-long ethnography at the International Atomic Energy Agency as an intern in the Department of

Safeguards. She examines the security seals, the inspector's manual, and other documents that outline protocol to understand how security, trust, knowledge, and expertise are configured across relationships between people and things (2019). These are just a few examples, but they do indicate I hope that there are ways to research the production of trust through technologies, even though this often occurs in ways and places that are opaque. Perhaps this is precisely why we should find ways to examine and think about the things that we trust.

In *The Intrinsic Value of Valuable Paper* you discuss how authentication devices are not just defined by what they can do (monitoring and securing identities etc.) but also by how they are *used* and integrated into circulatory systems (and used to safeguard law, for example). Are uses of authentication devices always related to the state apparatus or do you also observe other groups or institutions utilizing them? There is of course the case being made for markets of "surveillance capitalism," but is there also a space to think about more decentralized or grassroots initiatives trying to harness security and/or identification tools?

The need for authentication goes well beyond the state. Branding, especially for luxury goods and sports apparel, is the biggest source of counterfeiting. Medical supplies, electronic products, and in general consumer goods or production parts are all major targets for counterfeiters. Cities like Shenzhen have become famous for their ability to produce fakes, so it is no surprise that brand protection—and the quality, standards, and reputation that go with it—is a big area for security printers. Authentication devices are also used in official documents not issued by states. Certificates fall into this category, and include everything from education degrees to authentication certificates for sports memorabilia or artworks. In these cases, not entirely differently than the passport, the document that authenticates exists as separate from its object, and it must be able to validate itself, as well as the particular object to which it refers. This is by no mean a failproof method, and there is perhaps a future for authentication devices embedded in objects themselves, just as we do with biometrics. Perhaps we will have authenticating threads within the very canvas of a painting: we wouldn't need to analyze the work forensically or to rely on a certificate, because a quick machine read of the device,

integrated into the material composition of the work, would provide the proof and information needed. This is entirely speculative, but not impossible!

Real security printing, with the most current technology, is an expensive endeavour probably inaccessible to most grassroots initiatives. But this does not mean the same basic strategies of authentication cannot be applied. If we look at communities that develop their own currency, as I mentioned above, we see how they come to produce *something* that can be circulated with trust. At the heart of this is an agreement. And this could be anything. This is true of everything I've discussed: we as a community or a society decide what it is that we trust and what it is we consider authentic—it starts with an agreement.

References

BBC News (2019, May 9). Typo on millions of Australian bank notes. https://www.bbc.com/news/world-australia-48210733

Brunton, F. (2019). *Digital Cash: The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cryptocurrency.* Princeton: Princeton University Press.

Cole, S. A. (2002). *Suspect Identities: A History of Fingerprinting and Criminal Identification*. Cambridge, MA: Harvard University Press.

Demirgüç-Kunt, A. et al. (2018). *The Global Findex Database 2017: Measuring Financial Inclusion and the Fin-tech Revolution.* Washington, DC: World Bank. http://dx.doi.org/10.1596/978-1-4648-1259-0

Graham, D. A. (2020, October 21). Signed, sealed, delivered—then discarded. *The Atlantic*. https://www.theatlantic.com/ideas/archive/2020/10/signature-matching-is-the-phrenology-of-elections/616790/

Groebner, V. (2007) *Who Are You?: Identification, Deception, and Surveillance in Early Modern Europe*. Mark Kyburz and John Peck (Trans.). Brooklyn: Zone Books.

OECD (2019, March 18). *Trade in fake goods is now 3.3% of world trade and rising.* OECD Newsroom. https://www.oecd.org/newsroom/trade-in-fake-goods-is-now-33-of-world-trade-and-rising.htm

Pivcevic, K (2020, December 11). *Biometric shoe insole provides new way to measure health-insights.* Biometric Update. https://www.biometricupdate.com/202012/biometric-shoe-insole-provides-new-way-to-measure-health-insights

Weichselbraun, A. (2019). Of broken seals and broken promises: Attributing intention at the IAEA. *Cultural Anthropology, 34*(4), 503-528. doi: https://doi.org/10.14506/ca34.4.02