YEAR 22 JUNE 2019/ **ISSUE 80**

INFOSECURA

Cash: where it is accessed and where it is counterfeited

ACCESS TO CASH REVIEW

Final Report

March 2019

Falschgeldkriminalität

Bundeslagebild 2018

A magazine for the security printing industry worldwide, published four times a year by Intergraf in Brussels and mailed to named members of the security printing community, such as security printers, their suppliers, banknote issuing, government and postal authorities as well as police forces in more than 150 countries.

INTERGRAF

www.securityprinters.org
www.intergraf.eu

Contents

InfoSecura is published four times a year by Intergraf in Brussels. Information is accepted from industry contributors on a bona fide basis. Signed articles imply the personal opinion of the author and do not necessarily reflect the policy of Intergraf.

Information and articles may be submitted to the publisher, who is free to accept or reject any item for publication. The publisher reserves the right to edit all submissions including reader's letters.

Editor-in-chief: Beatrice Klose
Editor: Manfred Goretzki
Editorial office and publisher:
Intergraf, 130 A, Avenue Louise
B-1050 Bruxelles
T. + 32 2 230 86 46
F. +32 2 231 14 64
securityprinters@ intergraf.eu
Advertising inquiries: Manfred Goretzki

Choices to ponder

Unlike many larger magazines, Infosecura has no predetermined editorial plan. Instead, issues arise, be it at conferences, in discussions with colleagues and also in the general as well as in the specialized press. This issue seems to be dominated by surveys and reports and, in the ID document part, by questions surrounding facial recognition.

These reports bring a welcome note of objectivity into the discussion, especially the one by the German equivalent of the FBI, the Bundeskriminalamt, which looks in greater detail at figures for Euro counterfeiting. Criminals seem to be slightly less interested in currency counterfeiting than before, preferring electronic ways of getting money illicitly. But even in banknote counterfeiting, the Internet plays an increasingly important role, mainly through the access the darknet provides to counterfeit holograms and "how-to-do-kits".

There is no direct electronic equivalent to banknote counterfeiting, but it we define it simply as a financial crime, there is. It would be instructive if we could compare the financial losses to the public caused by circulated counterfeits to the losses through the many forms of card fraud, credit as well as debit. However, the card industry keeps these figures close to its chest.

In both areas, cash and ID documents, the debate about retaining physical banknotes and ID documents or replacing them by immaterial, electronic versions carried on smartphones or credit and debit cards is raging on as before, without any side conceding ground. However, the Editor has detected a growing consensus towards the co-existence of both, which seems to be a very sensible solution, considering the increasing frequency of natural disasters which leave large areas without electricity. But we have to admit that developing, designing printing and distributing banknotes, that is, keeping the cash cycle going, is expensive and the decision by a small central bank, the Eastern Caribbean Central Bank (ECCB), to try-out Central Bank Digital Currency (CBDC) seems eminently rational. In the string of islands that make up the Organisation of Eastern Caribbean States, the infrastructure to safely move cash to where it is needed is expensive and difficult to secure. On the other hand, the islands are part of the notorious 'hurricane belt' and every year some of its member states are hit by disastrous hurricanes that destroy lives and property and often leave the islands without electricity. So, to rely entirely on an electronic currency would not be rational. The experience the ECCB makes will be instructive to all central banks.

There are many countries the world over that face similar dilemmas in upholding the principle that money - in whatever form - has to be available to all. There are obvious differences in the cost of supplying a small town in Canada's Northern Territory, with cash, or in Mali, in Africa's Sahel, to doing the same in densely populated European or American countries with good infrastructure. But in such remote areas, CBDC is not the answer either, as the technical infrastructures is often not there. The answer? Much to ponder over the summer.

The Editor

IN CONVERSATION WITH DR. DIETER SAUTER

The preparations for the next SecurityPrinters conference in Copenhagen in October are in a 'high energy' phase. The Committee of Experts is putting the finishing touches on the programme. Infosecura talked to its chairman, Dr. Dieter Sauter about the industry and the conference.

Dr. Sauter, to begin with, a few personal points. You are a physicist, having studied in Tübingen and Stuttgart in Germany and you obtained your PhD at the Max Plank Institute for Metal Research in Stuttgart, Germany. These are good qualifications for any top job, but did they qualify you for work in the security printing industry?

Yes, they did. Not that physics is absolutely necessary to work in security printing, but my studies taught me the importance of structure, logic, to be solution oriented, to respect the environment and to accept the necessity for change. All these helped me in my jobs in several different positions.

You have recently changed from a private banknote and passport producer to a state-owned one. How do you judge the future of - especially smaller - private producers versus state owned ones?

Conditions have become more difficult for smaller banknote producers, especially if their home market is not large enough to sustain them. But one of the main problems of smaller banknote producers is lack of flexibility. With only one printing line and without a robust cooperation agreement with another printer, it is more difficult for a company to offer the necessary flexibility to central banks, who increasingly insist on good BCM (Business Contingency Management) arrangements. Delivery times are also being squeezed, although the total time to issue a new series has not changed much. Central Banks take longer to evaluate all aspects of an issue, which is good, but this means that the time to actually produce a series is getting shorter. And with one printing line only, while one issue is being produced, another has to wait.

In northern Europe and North America, but also in China, cash seems to lose attractiveness. Will there be a point when developing and producing a new issue of banknotes will simply become too expensive in relation to the use of cash?

Fortunately, in many countries volumes of banknotes produced are still rising, although in some, especially northern European countries, they are falling. The elimination of high-value denominations, such as the €500 note, could also help to increase the number of lower denominations to be printed, although that was probably not the intended result. It is not only the production of banknotes, it is also keeping cash in circulation that is expensive, especially in geographically large countries with relatively small populations. If cash is available, it has to be available to all. Central banks and our industry must find ways to keep the availability and distribution of cash sustainable. And it seems that non-cash payment systems are not robust enough to replace cash yet, especially in situations of natural or political catastrophes. In such situations it is again those far-out areas where it is expensive to provide cash now, that would be hit hardest in the case of wide-spread power failures, etc. Urban centres are usually back to normal fairly quickly, but rural areas need means of payments just as much. Here cash buffers are an absolute must and electronic means of payment are not the optimal answer.

Considering there are now more channels of information within the security printing industry (Cash Matters, Currency News, etc.) and between the industry and the wider public, what do you think is the role of security printing conferences, and has this role changed?

Conferences such as SecurityPrinters are necessarily focussed on our industry, if not necessarily mainly on the printing part. However, we have to look beyond our specialty and try to learn from the challenges and threats to our industry. In fact we have been doing that already. It is indeed the purpose of our conference to recognize challenges early on and to evaluate how to react; to resist them or to go along with them and try to drive them. The industry has also improved its outreach to the wider public. It founded the ICA - International Currency Association - mainly because it realized that it was not enough to convince the central banks about the need for and the advantages of our products but the whole of society as well, as it is individuals that

either use cash or try to use alternatives. And the same applies to physical ID.

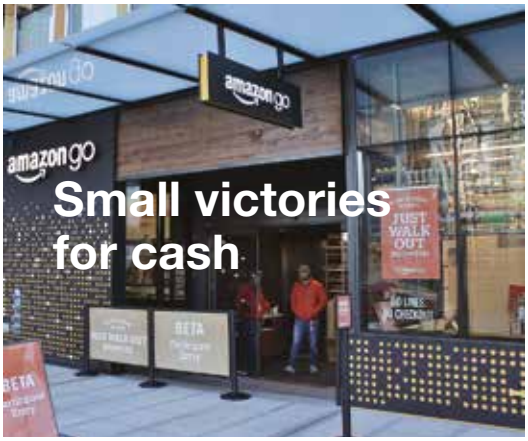
For us it is important to speak for both the currency and the ID sector. Although, technically there is some divergence between the two, the link between both sectors is security, which is the core of our industry and our conference.

Looking at how 'SecurityPrinters' is organised, with a small staff and a very diversified 'Committee of Experts', of which you are the chairman, would you regard this model of organisation as one of the major strengths of the conference?

It undoubtedly is one of the major strong points of SecurityPrinters. The 'Committee of Experts' has become very diverse, both in the breadth of expertise it offers and in the variety of industry players it represents, from security printers and central banks to police organisations to companies in the ID area. And in combination with the small and very experienced organizing staff it means that the SecurityPrinters conferences are reliably one of the top events in the industry.

Should our industry point out the dangers and costs of card and contactless payments more vigorously to the public?

Rather than pointing out the shortcomings of our competitors, we should stay optimistic and improve our own products. Our products are very robust and already at a very high technical level, but that does not mean that they cannot change or be improved. We have to work on the economics of the cash cycle as well as making cash 'cool' again. And we have to stay vigilant in the ID area, to offer the authorities the security and the operational efficiency they need. ■



Small victories for cash

Image: SounderBruce, Wikipedia

Earlier in the year, worried about an increasing number of shops accepting electronic payments only, the council of the US city of Philadelphia passed a law that would require retail shops to accept cash and prohibit them to charge cash-paying customers higher prices. New York and New Jersey passed similar laws. The reason behind the Philadelphia law is, according to the councilman who proposed it, that 6 per cent of the city's residents are unbanked. For the whole of the US that figure stood, in 2015, at 7 per cent and 43 per cent of American households have credit card debt. Allowing only credit and debit cards for payment "negatively affects poor people and immigrants who are unable to obtain credit cards, and do not have a bank account. Businesses who use credit only are sending a message to poor people that they do not want their business. People should have a right to use cash if they so choose," the proposing councilman Bill Greenlee said.

When the local law was first proposed, one of the first and fiercest objectors was Amazon. The vast Internet company told the city it would not consider bringing Amazon Go to Philadelphia - its cashless brick and mortar store that would employ about a hundred workers. Amazon touts AmazonGo as its most advanced shopping technology where customers would simply pay, using its wired mobile app – thus never needing to wait in line for check-out. Although there are at the moment only about ten of these shops across the US, Amazon plans to open about 3000 by 2021. The point of these shop it precisely that cameras and sensors record every item a customer puts into a shopping basket and instead paying at a check-out, the shopper simply swipes an app, leaves and still gets charged accordingly.

It was therefore quite unexpected that Amazon had a change of heart and decided to accept cash after all. In March, Amazon's senior vice president of physical stores, Steve Kessel, told employees that Amazon Go stores will have "additional payment mechanisms" in the future, CNBC first reported. An Amazon spokesperson confirmed to 'Business Insider' that the new mechanisms would include paying with cash.

Whether this would be direct cash payments, which would require a check-out cashier after all, or the possibility to convert cash into Amazon Cash, which uses a personal barcode or smartphone telephone number, the company has so far not said. Large tech companies that operated only with electronic payments seem increasingly to value cash. Ride-share giant Uber is also stepping-up the acceptance of cash in its many locations. ■

WHAT IF? IS CENTRAL BANK DIGITAL CURRENCY THE ANSWER TO CASH?

Banks would love to get rid of cash - some more so than others - but even some pro-cash central banks would not miss the bother of producing and managing cash amit falling use of banknotes. So what is the alternative? If it is Central Bank Digital Currency (CBDC), the Eastern Caribbean Central Bank is the first one to put a toe in the water.

In Infosecura we talked about the Swedish Riksbank mulling over issuing e-Krona, and Finland and Norway, as well as several other central banks examining the possible effects of Central Bank Digital Currency (CBDC). So far, none of these central banks has taken the next step of actually issuing CBDC. But on March 6, the Eastern Caribbean Central Bank (ECCB) announced that it had signed a contract with the Barbados-based fintech company, Bitt Inc. to conduct a block-chain-issued CBDC pilot within the Eastern Caribbean Currency Union (ECCU). In a press release, ECCB claimed that this would be the world's first block-chain based central bank digital currency. The aim of this move is to eventually reduce the use of cash by about 50 percent (but not to replace it). That aim seems very reasonable when looking at the geography of the area the ECCB serves.

The ECCB is the Monetary Authority for the Organisation of Eastern Caribbean States and controls monetary policy in eight countries; Anguilla, Antigua and Barbuda, Commonwealth of Dominica, Grenada, Montserrat, St Kitts and Nevis, Saint Lucia and St Vincent and the Grenadines, a string of islands on the outer south-eastern edge of the Caribbean, with a total population of 615,724 and a total area of 2700 km2. The distance between the most northerly to the most southerly point is, however, about 600 km and supplying these island with sufficient EC dollars is undoubtedly expensive and cumbersome and can pose logistical challenges.

The ECCB said that the digital EC dollar (DXCD) will be distributed and used by financial institutions in the Eastern Caribbean Currency Union (ECCU) for financial transactions between consumers and merchants, including peer-to-peer transactions, all using smart devices. The Governor of the ECCB, Timothy N. J. Antoine, emphasised that "this is not an academic exercise. Not only will the digital EC Dollar be the world's first digital legal tender currency to be issued by a central bank on block-chain but this pilot is also a live CBDC deployment with a view to an eventual phased public rollout." As of March 2019, there will be a development and testing phase for about twelve months, followed by rollout and implementation in pilot countries for about six months.

Aside from the mentioned logistic difficulties of moving cash between these islands, the ECCB governor earlier pointed to another reason for introducing central bank digital money: "We should also acknowledge that small business face real constraints ... when they are required to pay as much as 3.5 per cent on every credit card payment, which removes the incentives for businesses to offer customers electronic options." It may be wise that a small central bank will be the first one that will test CBDC, rather than expecting a larger central bank to take the first step.

BLOCK-CHAIN OR NOT?

The ECCB pointed out repeatedly, that their future digital currency will be based on block-chain, also called distributed ledger technology. There are different kinds of central bank digital currencies. A paper entitled "Central bank digital currency: concepts and trends" published in March 2019 by VoxEU.org, the policy portal of the Centre for Economic Policy Research (www.cepr.org), gives a concise overview of the various possibilities.

Cash can be viewed as central bank money and it has well-known characteristics: its use is anonymous, it provides a peer-to-peer settlement form, is available 24 hours a day and 365 days a year, and is usable anywhere within an economy. However, the paper states that cash handling costs are high when considering not only the direct fees (i.e. the cost of paper, printing and design) but also the security and personnel cost of providing cash and payment services by commercial banks, companies, and individuals.

Central banks issue another type of money to commercial banks in the form of reserve balances at the central bank (reserve deposits). Sweden's central bank, the Riksbank, has also been investigating the possibility of issuing deposit accounts to the general public. Reserve deposits, still only available to designated financial institutions such as commercial banks, are used for managing the real-time interbank payments and settlements system. As an account-based system they are non-anonymous and they are non-peer-to-peer settlements, as transactions between commercial banks are intermediated by a central bank. From the perspective of a central bank, the difference between cash and reserve deposits is that the former is an interest rate-free instrument, while reserve deposits carry a positive or negative interest rate.

The most important private sector money are bank deposits, used for internet banking, credit and/or debit cards. Digital wallets and payment apps on smartphones are all linked to deposit accounts. While bank deposits are not legal tender, their values are denominated in legal tender and can be exchanged at a one-to-one value. Similar to reserve deposits, bank deposits are non-anonymous and transactions are traceable and they carry a positive or negative interest rate. The size of bank deposits is much larger than the size of central bank money due to the large number of financial institutions and money creation activities, which generate deposits and loans.

There is another form of private sector money, based on distributed ledger technology – often called digital tokens or crypto currencies. These tokens are generally issued by independent 'miners'. As they only exist in digital form, a mechanism is needed to verify that a token has been spent or received. This is done by unknown, independent third parties without relying on a central manager. Block-chain is a type of distributed ledger where each transaction is verified using encryption keys and digital wallets; the numbers of the transactions are recorded on a new electronic distributed ledger, which is then connected through a chain to previous, proven distributed ledgers using the proof-of-work process. There are currently over 2,000 digital coins with features that vary substantially. Digital tokens are similar to cash since peer-to-peer transactions can be made instantaneously, all-day and all-year. All the transactions are anonymous but are technically traceable. A positive or negative interest rate can also be applied.

DIFFERENT FORMS OF CENTRAL BANK DIGITAL CURRENCY

The paper states that several central banks have considered issuing their own digital tokens and Sweden's 'Riksbank' has suggested to let the public open central bank accounts. These proposals can be classified into a) retail CBDC and b) wholesale CBDC, and further into c) CBDC not based on distributed ledger technology and d) CBDC based on distributed ledger technology.

The Riksbank's eKrona project is of the 'not on distributed ledger technology based' kind and it is designed to be account based - a direct account at the central bank - or value based, by storing the CBDC in a card or phone app. All transactions of both proposals are traceable and non-anonymous, since an underlying register enables the recording of all transactions and identification of the rightful owner of the digital eKrona. An exception to the non-anonymous characteristic is the prepaid card on which eKrona are already stored and which can be used as cash and handed from one user to another. However, there would be a limit on the value that can be stored, which is €250, to be lowered to € 150 in 2020 and, this being 'money', it would not attract any interest, according to the E-money Directive.

Most central banks have not shown any interest in the Swedish model, mainly because it is thought that commercial banks might suffer losses to their retail deposits if private central bank accounts prove to be successful, thus depriving commercial banks of sources of loan finance to extend credit to companies and individuals. The paper suggests that this concern could be mitigated if the central bank were to pay a lower interest rate to the general public than commercial banks do to their retail customers.

RETAIL CBDC BASED ON DISTRIBUTED LEDGER TECHNOLOGY

A further variant of CBDC using distributed ledger technology, features anonymity, traceability, and day- and year-long availability, and makes interest rates feasible. This proposal is relatively popular among emerging economies (such as the ECCU), because it offers a lead in the rapidly emerging fintech industry, to promote financial inclusion and to reduce cash printing and handling costs. Some countries – including Ecuador, Israel, Uruguay, Lithuania, the Marshall Islands, Tunisia, China, and Venezuela – have examined and/or conducted related experiments.

The paper states that central banks in advanced economies are not enthusiastic about this proposal, as existing retail payments and settlements systems have become more efficient and faster. Also, the use of cash is not yet declining and because almost everyone is banked, financial inclusion is not an urgent issue for central banks. Many central banks do not wish to create competition between central bank money and private sector money and finally, central banks in advanced economies are generally more cautious than those in emerging economies because they fear harming their reputation should an initiative prove unsuccessful. Limited public interest and support for the proposal is another factor discouraging these central banks from actively considering the proposal.

WHOLESALE CBDC BASED ON DISTRIBUTED LEDGER TECHNOLOGY

Because it has the potential to make existing wholesale financial systems faster, less expensive, and safer, this variant of CBDC is the most popular among central banks. Even the Bank for International Settlements thinks that it could be beneficial. In order to learn more about the distributed ledger technology systems and how

they could be applied to the existing wholesale financial markets, the central banks of countries including Canada, Singapore, Japan, Brazil, South Africa, and Thailand, as well as the Euro area, have conducted experiments since 2016. Most of these experiments showed that using this technology, digital tokens on a distributed ledger could be successfully transferred in real time and in reasonable volumes. Nevertheless, the banks have not taken further steps towards implementation because the current technology is seen as not yet sufficiently advanced to cope with privacy protection issues. The central banks also believe the process of verifying transactions could be faster and most cost-efficient if the verifier is centralised (either through a group of selected commercial banks or a central bank), but this approach would not necessarily be superior to the existing system. In addition, their current wholesale payments and settlements systems are already sufficiently efficient, so no strong gains can be expected from a CBDC initiative, the paper concludes.

While most central banks thus adopt a wait and see attitude, South Korea's central bank, Bank of Korea (BoK) came out against CBDC and issued a warning saying that if the public could access the theoretical digital currency directly, commercial banks' demand deposits, or reserves, could be reduced – leaving them with a cash shortfall. That could eventually force them to compensate by raising interest rates on loans. "This has negative effects on financial stability, which increases the likelihood of bank panic in which commercial banks are short of cash reserves to pay out to depositors."

On the other hand, IMF Managing Director Christine Lagarde, at the Singapore Fintech Festival in November 2018, was much more positive towards CBDC, saying "My message is that while the case for digital currency is not universal, we should investigate it further, seriously, carefully, and creatively." ■

UK ACCESS TO CASH REPORT

It's not just ATMs

The final version of the UK's access to cash report not only examines the cash infrastructure and the cash cycle in Great Britain, it also makes a number of sensible suggestions to enable cash to be available as long as users want it.

In the last issue of Infosecura, we wrote about a British preliminary study on the use of cash, which asked the question "is Britain ready to go cashless?" Even the preliminary report answered with a firm no. The final report that came out in March this year confirmed this finding and offered a set of recommendations to ensure that when the end of cash finally does come - and the report leaves little doubt that it will - no-one will be left behind. The report acknowledges that digital payments still don't work for everyone and that the consequences to society and individuals of not having a viable way of paying for goods are potentially severe. Consumers need a guarantee that they can access and use cash for as long as they need it. But as use of cash is undeniably going down and our present cash infrastructure has ben designed for "100 per cent, large scale" utilisation, a radical review of the cash infrastructure is necessary, as cracks in the system are already showing.

It is probably not enough to decry individual symptoms such as the decline in the number of ATMs (the report was funded by LINK, the UK's largest cash network, but is independent from it). It is true that in certain, especially rural, areas, people may find it increasingly difficult to access cash, but conversely, where there are plenty of ATMs, they are used less than before because people rely more on digital payments. Examples from countries that also experience a decline in the use of cash show that refusal of merchants accepting cash is a more important factor in the decline of cash use than the access to it. As one consumer group said, 'there is no point protecting access to cash if you can't use it'.

But merchants don't like to inconvenience customers without reason either and their refusal to accept cash is linked to the rising costs of handling and banking it, driven in turn by the underlying economics of cash handling and distribution. One of the biggest imperatives to keeping cash viable over the coming years, therefore, is to rethink the economic model underpinning it. The present cash infrastructure is fast becoming unsustainable, with largely fixed costs and declining income. A whole-system view and set of solutions is necessary. Simply addressing one part of the issue – such as ATMs – is very unlikely to work in a sustainable way.

CASH IN THE SHADOW ECONOMY

The report places some importance on the role of cash in the grey (informal) and black (illegal) economies, citing that in the UK, 36 per cent of those questioned believe that a cashless society would reduce crime. That may reflect a sentiment in the population, but central banks, e.g. the German Bundesbank, are more cautious. In this issue,

Infosecura looks at "cash in the shadow economy" as examined in a report by the Bundesbank.

The UK report also adopts a more cautious note by stating that there are undoubtedly benefits from the reduction in cash in terms of lower crime and higher tax revenues, but we must not demonise those who operate in cash, when many have no choice. Solutions adopted by other countries, such as Sweden, to bring the grey economy into the formal economy through tax breaks and peer-to-peer payment technology, thereby isolating the black economy to attack it more directly, might be an option for UK policy makers to consider.

CASH AS PART OF NATIONAL INFRASTRUCTURE

In order to keep cash viable, the report suggests to make cash a core part of Britain's national infrastructure, and not just a commercial issue. Consumers should be offered a 'guarantee' of cash access by banks and regulators, by encouraging innovative ways of accessing cash, rather than just protecting increasingly unviable ATMs or, worse, charging consumers for access. If banks are helped to keep the costs of cash down as its use declines, and to innovate around cash deposit solutions, then there will be fewer commercial incentives for retailers to stop taking cash. And overall, a better-designed wholesale cash infrastructure could significantly reduce the costs of running the cash cycle, making providing cash commercially viable for the banks on an ongoing basis.

FIVE RECOMMENDATIONS

The report makes five recommendations, which, it suggests, will keep cash viable for the foreseeable future, as well as eventually including everyone in a society where digital payments dominate. These recommendations work together, because cash is a system, and needs to be treated as such, the authors insist.

The review's first recommendation is to guarantee consumer access to cash – ensuring that consumers can get cash wherever they live or work. Importantly, this is about access to cash, not just access to ATMs, as the authors see huge potential for new ways of providing cash access which could both widen access and help keep the high street alive. This guarantee needs to be agreed by regulators, in consultation with industry and consumer groups. It may well need legislation in the medium term, but could be set up swiftly, initially on a voluntary basis. The proposed mechanism also gives the right to local communities to 'bid' for increased cash access through their local authorities, which would help address the issue of cash deserts.

The second proposal suggests that the best way to preserve consumers' ability to pay with cash is to make it affordable for retailers, charities and service providers to accept cash, to ask utility and monopoly suppliers to ensure that they will access cash (whether directly or through a partner) as well as to remind suppliers of their wider societal responsibilities to meet the needs of vulnerable customers. This could be achieved through targeted technological innovation such as deposit-taking ATMs and 'smart safes', led by government and regulators.

The third recommendation is to call for radical change to the wholesale cash infrastructure, moving from a commercial model to more of a 'utility' approach, which will keep cash sustainable for longer. The UK cash infrastructure was built for an age of high cash volumes and now it runs at far higher cost than is required today. The Bank of England could convene a group to redesign this model, making it both more resilient and lower cost. The lower cost of a redesigned cash infrastructure will make it more tenable for the banks to provide free consumer access to cash for longer.

As a fourth recommendation, government, regulators and the industry need to make digital inclusion in payments a priority, ensuring that solutions are designed not just for the 80 percent, but for 100 percent of society. This should remain an ongoing priority, and not a one-off activity.

A fifth and final recommendation calls for a clear government policy on cash, supported by a comprehensive regulatory approach, which treats cash as a system. Market forces alone won't make any of this happen. This issue needs leadership, the report insists. Financial services regulators probably have most or all the powers needed to make this happen, at least in the short term – but no one regulator can do this alone. This is also an ongoing action, as they will need to monitor the cash system over the next decade and refresh their approach as the situation changes. This recommendation is the most urgent, as without this leadership, change is unlikely to happen.

A CALL TO ACTION

The report concludes with a call to action: If government regulators and industry work together, they can keep cash viable to avoid leaving people behind, but only if action is taken now. Cash can no longer just be seen as a commercial issue – it is a matter for public policy. And it will need everyone involved in the system – government, regulators, the Bank of England, retail banks and consumer groups – to work together to take the recommendations forward. ■

IN DEFENCE OF BIG MONEY

As the words of the Vice Chairman of the Swiss National Bank at the presentation of the new 1000 Swiss Franc note show, it is almost an act of defiance to issue a high-denomination banknote. But even the European Commission and the German Bundesbank had to admit that hard evidence for the claim that high-denomination banknotes foster crime and terrorism is just not there.

Statistics show that the number of banknotes in circulation worldwide is still rising, in spite of the occasions when cash is used in real transactions becoming fewer and fewer, especially in northern European countries and in China. The answer to this riddle is, that it is the number of large denomination banknotes is rising, because people like to keep a money reserve at home, or to put it more bluntly, people like hoarding money. More suspicious types will insist, that large denomination banknotes are used to facilitate the grey (in-official) and the black (illegal) economies, as well as different forms of crime, because cash transactions are anonymous and large denomination notes are most handy to transports large amounts of money. The European Central Bank accepted this argument and as of 27 January 2019 has no longer issued the €500 note, the highest value in the Euro line-up. Many national governments also issued limits to cash payments.

The demonization of large value banknotes is, however, not universal. On March 13, 2019, the Swiss National Bank defiantly issued a new Sfr 1000 note, implicitly rejecting the argument that high value banknotes encourage crime. “The SNB is following discussions about illicit use very closely, but there were no indications that criminals used the 1,000 franc note more frequently than other notes”, Vice Chairman of the SNB, Fritz Zurbruegg said.

“The choice of the denomination is a matter for the SNB, but the current denominations are appropriate and correspond to what people want,” Fritz Zurbruegg told a news conference. “The 1,000 franc note is used for payments and also has a function as a store of value. Cash is still very popular in Switzerland, it is a cultural phenomenon.”

Research by the Swiss economist Yvan Lengwiler and quoted in the Zürich daily NZZ shows, that illicit use of the Sfr 1000 is less an international issue than a domestic one. That research showed that there is a rush on 1,000-franc notes in December every year as people move their assets to cash. The money is then deposited in bank accounts again in the new year. In other words, the notes could be being used in the process of avoiding wealth tax. Misuse of that kind would of course not show up in any crime statistics about high denomination cash. The Swiss National Bank issued about 48 million pieces of the banknote, representing 10.2 per cent of all Swiss banknotes in circulation and accounting for just over 60 per cent of the total value of Swiss Franks. The Sfr 1000 note is the penultimate note of the new series to be released, the last one, the Sfr 500 will be released in September 2019.

This series, the 9th, has won great praise for design and security features. The Sfr. 10 won the ‘Banknote of the Year Award’ from the International Banknote Society in 2017, as did the Sfr. 50 in 2016. In 2018 the Sfr 200 was nominated, but the final award went to the Canadian CAN$ 10 instead.

Switzerland is one of the few remaining high-denomination issuing countries left. The Sfr 1000 is dwarfed by the Singapore S$ 10 000 (about € 6 545,00) but the Singapore Central Bank stopped printing the banknotes in 2014, although it is still in circulation, leaving the S$ 1000 as the highest issued denomination, worth about € 654,00. Most other countries have relatively puny top denominations. The UK’s £50 is worth about € 56 or US$ 63, while Norway’s NOK 1000 exchanges for € 103 and US$ 116 and Sweden’s 1000 Krona for € 93 and US$ 105. Sometimes the denomination seems mainly aspirational. The highest value banknote in Venezuela is the Bolivar soberano 500. According to the official rate on April 20, 2019, it needed over ten of those notes, or Bs 5203 to buy one US Dollar.

A WEAK CASE AGAINST BIG BILLS

An oft-voiced opinion in the public debate is that cash promotes the shadow economy and is used as a means of financing crime, a new report by the Bundesbank, the German central Bank (2019-03-bargeld-data.pdf) states in its introduction. But an opinion, however widely stated is not proof and the report “Cash demand in the shadow economy” tried to get as close as possible to the truth, acknowledging that it is “very difficult to provide hard research-based evidence about the scale of the cash demand resulting from the shadow economy and criminality” and “empirical studies of the shadow economy are therefore subject to more than average uncertainty, meaning that all results should be interpreted with caution.” The study also warns “cash is not the sole payment instrument used either in the shadow economy or to finance crime. As part of the general trend towards digitalisation, alternative payment instruments are gaining significant ground, particularly in connection with settlement via the internet or darknet.”

SO WHAT IS THE STUDY SHOWING?

At the end of 2018, €1,230 billion worth of euro banknotes were in circulation, of which just over half were issued by the Bundesbank representing a volume growth of 4.9 per cent p.a. over the past decade, faster than nominal economic output in the Euro area. Demand for Euro banknotes at the Bundesbank can be divided into foreign demand, domestic transaction balances and domestic hoarding. An estimated two-thirds of the Bundesbank issued Euro banknotes were in circulation abroad at the end of 2017. Domestic cash users were hoarding just over 20 per cent of net issuance, while slightly less than 10 per cent was being held as transaction balances.

The paper considers different methodologies in trying to define the size of the shadow economy and the part, large denomination banknotes play in it. These notes make up a significant part of cash in circulation in the Euro area as well as in other currency areas. However, the demand for large denominations alone cannot be used to support the conclusion that cash is being used for illegal purposes, since these denominations are equally suitable as a legal store of value or for legal and illegal high-value payments. In particular, interpreting the Bundesbank's cumulative net issuance is made more difficult by the fact that the banknotes that it issues also circulate abroad. In summary, anecdotal evidence drawn from the volume of cash in circulation or the demand for large-denomination banknotes is not appropriate for quantifying illegal cash holdings, the paper states.

The European Commission, to combat terrorism financing, recently looked into the introduction of an EU-wide standard ceiling for cash payments, but concluded that such a measure would not address the problem of terrorist financing and announced that the issue would not be taken any further for now.

It based its decision on two public consultations in which just under 95% of those surveyed came out against an EU restriction on cash payments. The EC concluded that ceilings on cash payments will not deter criminals from committing a criminal act in connection with tax evasion or terrorist financing, but they could risk a possible loss of confidence in the currency on the part of the general public. It is clear that the European Central Bank decided to stop issuing the € 500 note following the "public debate", although there is still a lack of empirical evidence as to whether measures such as abolishing large-denomination banknotes or introducing upper limits for cash payments, would be an effective means of combating tax evasion and other criminal activities. ■

Counterfeits and funny money

image: Bundeskriminalamt

There were some unexpected movements in the number and kind of Euro counterfeits found in Germany and the European Union as a whole, but overall, the picture is encouraging.

The reason for the existence of the security printing industry is that since paper banknotes and paper documents began, they were also counterfeited. The police organisations fighting counterfeiting have a good idea about the scale of the problem but so far there have been few comprehensive surveys of the extent of counterfeiting in one country. The German Bundeskriminalamt in cooperation with other German and European police organisations and the German and the European Central Bank have just published a report entitled "Falschgeldkriminalität, Bundeslagebild 2018", which gives a Germany-wide picture of criminality involving counterfeit money.

Some figures are encouraging: in 2018 there were 3469 relevant police inquiries, down by 4 percent, involving 3077 suspects, down by 5 percent. However, the number of Euro counterfeits counted went up by 10 percent to 99.912, representing a nominal value of €17 million, an increase of 146 percent.

In Europe as a whole, 1.17 million counterfeits were found, up 30 percent, representing a nominal value of €102 Million, an increase of 82 percent. To see what these figures actually mean, we have to look at the denominations and origins of the counterfeits.

COUNTERFEITS: WHERE AND BY WHOM

In Germany, there are certain counterfeiting hotspots. Most counterfeit Euros are found in North-Rhine-Westphalia (NRW), Bavaria and the south-western state of Baden Württemberg, but in NRW there were 5000 fewer cases in the reporting period, a decrease of 27 percent. It is

also remarkable that there were relatively few cases of counterfeiting in the states of the former DDR. Overall, the number of suspects under investigation fell, but among them, the proportion of young people under 21 rose by 120 percent in the last four years from 364 to 800. The report puts this down to the interest of young people in the Internet and specifically in the Darknet, the instructions and the material for counterfeiting offered there and the – naïve – belief that the Darknet is anonymous. Most of these counterfeiting instructions on sale there are for the € 50 note of the first series and on them holograms of Chinese origins are used. 40 percent of counterfeit Euros found, fall into this category.

Counterfeits are not only passed on randomly to unsuspecting people but are used directly for substantial private purchases as well, the report states, such as for buying used cars or smartphones, where the values are between €500 and €1000. When in these transactions any ID is demanded, those presented are usually counterfeited as well.

In contrast to the number of cases and suspects, the number of counterfeit banknotes found in Germany increased by 10 percent in 2018 to 99.900. However, this figure includes a large seizure of 22 000 notes, so called VBNA notes, low quality counterfeits of €500 Euro notes, often with additional imprints, sometimes with Cyrillic letters or Chinese writing, identifying them as “souvenir notes” or “not for purchases”. They were obviously not destined to be used in commerce or to fool anyone, but they were nevertheless included in the number of counterfeits seized. They are sold through Russian, Ukrainian and Asian souvenir shops and through digital channels.

While in 2017, 80 percent of counterfeits were found in circulation, having caused real economic damage, in 2018, only 58 percent had been circulated, the rest were seized in police operations at manufacturing sites, without causing economic damage.

Every second counterfeit Euro note seized in 2018 was a €50 note (53 percent) a reduction from 61 percent in 2017. Counterfeiters concentrate on the €50 because it is very popular in everyday use and is perhaps less checked than a higher denomination.

Generally all denominations except the €10 and – for reasons mentioned – the €500 showed a decrease in counterfeits. It remains to be seen if the introduction of the €100 and €200 notes in May, which have improved security features, will change the denomination distribution of counterfeits. The second Euro series also eliminated the €500 note, but as it continues to be legal tender, there may well be some further counterfeits in circulation.

The nominal value of counterfeits seized in 2018 in Germany was the lowest since 2014. It fell from €4.1 million in 2017 to €3.4 mill, a decrease of 17 percent. As banknote counterfeiting is a truly international business, it is to be expected that in Germany foreign nationals are to be found among the perpetrators. However, in Germany the largest group among counterfeit criminals were Germans, with 63 percent, followed by Turkish nationals with 13 percent and Italians and Romanians with 9 percent each. The organisational level is also very diverse, whith single operators buying equipment, materials and knowledge on the Internet to well organised international criminal groups. In 2018, as in the year before, of three large international crime groups one was dominated by Turks, one by Italians and one by Germans.

EURO COUNTERFEITING IN THE EU

In 2018, the European Central Bank registered 1.2 million counterfeit euro notes, 47 percent of them had been in circulation and 53 percent were seized before they were circulated and although this is an increase of 30 percent this is still below the average of the last five years. Compared to the total volume of Euro notes in circulation, 2 billion notes, this figure is small.

The largest number of inner EU Euro counterfeits were found in Italy, France and Germany, about three quarters of the total. And the highest number of counterfeits – 602 000 – came from Italy, where the previous year only 297 000 had been found, which puts Italy with of 51 percent of the total on the top of the counterfeit league table. Most were seized before circulation (494 000 notes), proof of large and successful police operations dismantling manufacturing sites and counterfeit depots. In Italy, good quality offset counterfeits came predominantly from the Naples area, but now, good quality copy-counterfeits of €20 and €50 are produced there as well, which are distributed – often by mail - in large quantities all over Europe. The number of offset counterfeits is going down, due to the large number of counterfeit notes available on the Darknet.

With 168 00 counterfeit notes or 14 percent, mostly found in circulation, France is on place two, as there are only few and small counterfeit manufacturing sites in France. On place three is Germany, with 100 000 fake notes found - 9 percent of the total - 50 percent so-called hologram notes, traded on the Darknet, while in France, mainly ‘Napoli-notes’ are found.

In the whole of the EU, mainly counterfeits of €50 and €100 were detected, the latter showing a rise of 651 percent. This is due to two important counterfeit seizures in Italy and Bulgaria, where a total of 385 00 counterfeits of €100 were found. While the nominal value of counterfeits found in circulation has been relatively stable in the last five years,

the average was 36 million and in 2018 it was € 31 million, the total nominal value of counterfeit Euros, varied considerably over the years from over 135 million in 2016 to 56 million in 2017 to 102 million in 2018.

NEW DISTRIBUTION AND LEARNING PATTERNS

The rise of the Darknet made the availability of counterfeits for re-selling universal throughout Europe (the survey does not mention any Euro counterfeit seizures outside Europe, but as the Euro is one of the most important trade and reserve currencies, there must be many). Digital copy technology also enables counterfeiters to adapt quickly to design changes. The survey expects that even the improved security features if the new €100 and €200 notes will have only a temporary effect of dampening Euro counterfeit criminality. ■

Under President Barak Obama, the old custom that any portrait on a Dollar bill had to show a dead, white, male politician seemed finally to have been buried. But new presidents make new rules and the one that there should be - some - gender equality, even on US banknotes, got buried instead.

In March 2016 we ran a short article with the heading: "Tubman's In. Jackson's Out"quoting a New York Times article, which said that after inviting the public to suggest the name of a woman to appear on the next $10 bill, and after a grassroots campaign won support for having a woman's portrait on the $20 bill instead, then Treasury Secretary Jacob Lew announced that the black slave liberation fighter Harriet Tubman would be on the front of the US $20 note and Andrew Jackson would be relegated to the back. The overhaul of the $20 note would mark the first time a black woman would grace US currency. Tubman would also be the first woman in over 100 years on a paper note. The Treasury Department announced in April 2016 that it would work on getting the new bill out "as quickly as possible."

After President Trump took power, his new Treasury Secretary Steven Mnuchin was very noncommittal about the plan, which he inherited from his predecessor. "We haven't made any decisions as to whether we'll change the bill, or won't change the bill," CNN quoted Mnuchin at the start of his tenure. Then Mnuchin said nothing further about the new banknote for over 18 months. In 2017, speculation began that President Trump might scrap Jacob Lew's plan for the $20 bill when mentions of it were scrubbed from the Treasury Department's website.

Then, that August, Mr. Mnuchin made clear that Tubman's future on the bill was in doubt. "People have been on the bills for a long period of time," he told CNBC. "This is something we'll consider. Right now, we've got a lot more important issues to focus on." At the time of the original announcement, the redesign of Tubman on the $20 bill was expected to be unveiled in 2020.

But on May 23, CBS News quoted Mnuchin saying that it won't be happening under the Trump administration. "It's not a decision that is likely to come until way past my term, even if I serve the second term for the president," Mnuchin told the House Financial Services Committee. "So I'm not focused on that for the moment." Mnuchin said a redesign of the bill's security features will still come out in 2020. But the issue of changing how the bill looks "most likely" won't come up again until 2026, he said, and the new $20 bill won't be printed until 2028.

Mnuchin did not explain why the Tubman bill won't be produced on his watch, but it is reasonable to assume that the displeasure of the President played a role. President Trump said during the 2016 campaign that he did not support putting Tubman on the $20, calling the plan "pure political correctness." He suggested instead having Tubman on "the $2 bill" or "another bill."

Replacing Jackson with Tubman was both filled with symbolism and marred by controversy. Trump is an admirer of President Andrew Jackson, a slave owner, who orchestrated the removal of Native Americans from lands to the east of the Mississippi River and sent them marching west on the infamous and deadly Trail of Tears. Trump even had a portrait of Jackson put in the Oval Office. Early in his administration, Trump visited Jackson's grave and subsequently tweeted: "We honour your memory. We build on your legacy."

Tubman was born into slavery, escaped and then returned to the South, where she led other slaves to freedom. She was a Union scout during the Civil War and later advocated women's voting rights. ■

COLOURING-IN THE BANKNOTE

Contactless cards, mobile phones, the Internet, cryptocurrencies, m-pesa; the list of alternative means of payment grows every year and yet, as we enter the third decade of the 21st century, cash remains with us. The reasons are many and have been debated at length. This article seeks not to explore or explain why every nation and every culture still have and still use cash, but instead to examine the ways in which banknotes have evolved to stay competitive, and how these changes have challenged their design, manufacture and use.

by Nick Nugent,
Technical Director,
Luminescence
Sun Chemical Security

The finished banknote defended with security features drawn from Level 1 (overt), Level 2 (covert) and Level 3 (forensic)

BUILDING THE SECURITY

A banknote has just a few key characteristics. It must look good, be easy to verify yet difficult to copy, survive in circulation environments that are uncontrolled and often severe, and of course it must be cost effective. These characteristics are connected but not always working together and must be designed holistically. The security features can be considered as colouring pens, used in the right way to build layers of integrated defences into the banknote.

PUTTING MORE INTO LESS

Banknote security is paramount, however many of the changes that notes have undergone in the last five decades are cost driven, and reducing their size is certainly an effective cost-reduction strategy.

Over the same period the security content of a note has exponentially increased, with extra functionality being demanded at overt, covert and forensic levels. Security threads have widened, additional printing processes have been introduced, diffractive devices and windows have become more popular, and machine-readability has increased to support the ever-increasing automation of the cash-cycle. The result is overcrowding, and there is a danger that security may become less effective when trying to cram more function into less space. Overcrowding is a threat to all aspects of document security: resistance to counterfeiting and ease of verification.

LONGER LIFETIME

Circulation lifetime of banknotes is another factor which directly impacts cost, and many technologies are being introduced, especially by substrate manufacturers, to keep a banknote circulating in an acceptable condition for longer.

The most obvious is the use of polymer substrates, which reduces the opportunity to use some strong security features, such as mould-made watermarks, but enables a longer lifetime as well as a host of new printed and stamped features within the window area. As well as banknotes made of polymer, there are several paper/polymer hybrid offerings which compete in the durable substrate arena. These “novel substrates” present further challenges to security printers and their component suppliers, as increasing substrate lifetime requires that the print and applied feature durability must keep pace. There’s little cost benefit in the use of more durable substrates if the printed and applied features don’t last as long!

SOLUTIONS TO THE NEW CHALLENGES

It is clear that more is being demanded of banknotes today than ever before. They must be more secure, have increased functionality and last longer, and they must achieve this whilst being smaller and cheaper. And in an environment where criminals are as sophisticated and ingenious as they have always been but now have access to high resolution digital equipment and are even more knowledgeable and organised, thanks to the internet.

The success of banknotes in meeting these challenges can be seen by the continued growth in banknote issuance globally, and a corresponding fall in incidence of counterfeiting. So how is this being achieved?

HOLISTIC DESIGN

In the same way that densely populated cities function best when designed from the ground up, rather than gradually evolving and growing as new suburbs are added over time, a banknote works best when its functionality and features have been considered as a whole at the design stage. The suppliers of the various components; substrate, threads, inks, applied features etc. need to work with the issuer and banknote designer from Day-1 to ensure optimal functionality and cost-effective security. Afterthoughts and 11th hour changes result in features being “bolted-on” which usually compromises the banknote.

TECHNOLOGICAL INNOVATION

Without innovative technology pushing the boundaries it would simply be a matter of time before criminals caught up and overwhelmed the cash

cycle with counterfeits. However, technology is not the whole solution but is just a part of it. If not married closely with strong design principles, technology can be a costly and ineffective addition to a banknote.

LEVEL 1, PUBLIC RECOGNITION FEATURES.

Traditional substrate features such as watermarks and threads have stood the test of time, with the first patent for a mould-made watermark originating over 200 years ago.

Watermarks remain strong Level 1 security features

Intaglio print – although probably not consciously recognised by the public – has also proven itself as a strong security technology and particularly recognisable in a counterfeit by its absence. Intaglio is also a useful vehicle for more covert security features, and infra-red, magnetic, colour-shift and luminescent materials may all be applied using intaglio.

Raised intaglio print enables multi-layer security

Diffractive foil devices, sophisticated windowed threads and colour-shift inks are relative newcomers, appearing in the last 30 or so years. Colour-shift effects are available in print that has sufficient film thickness and are therefore typically utilised in intaglio and silk-screen print. Gravure and flexo print processes are also used to apply colour-shift pigments, appearing within threads or other devices.

Colour shift ink applied using silkscreen

LEVEL 2, DETECTED BY DEVICE OR READER.

The use, at retail outlets, of ultra-violet (UV) lamps to excite luminescent components within the banknote to produce colourful emissions remains a popular verification method, and the incorporation of fluorescent materials in inks, diffractive devices and threads has grown over the years. The majority of such fluorescent checks involve excitation using long wave UV (365nm) and a simple human-readable validation that an ink glows the colour it should. Here the marriage between technology and design becomes apparent again as it is of the utmost importance that any luminescent feature is easily verifiable with confidence by the cashier; i.e. the authenticator should almost automatically know that what is visible is correct.

Banknote viewed from different angle

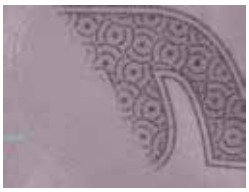
Of course, there is a great deal more sophisticated verification possible when one considers that the electromagnetic spectrum extends into shorter wave UV and longer wave infra-red wavelengths, and that not all fluorescence utilises George Gabriel Stokes' principles of high energy excitation producing lower energy emission.

UV fluorescence is widely used in a range of print applications

Many automated note verification systems, provided by the Banknote Equipment Manufacturers (BEMs), utilise infra-red wavelengths to validate currency.

A technological breakthrough in the world of infra-red absorbers came with the development of a new family of materials, Luminescence Sun Chemical Security's ASPECT range, which is an exceptionally effective absorber of infra-red radiation. The main benefits of this family of high-security inks are:

- Available for all banknote printing processes, including offset
- Increased design flexibility; a full colour gamut with many lighter shades is now available, offering designers more opportunities to integrate the feature into a more sophisticated overall design
- Future-proofed, as BEMs and high-speed sorters can utilise precise absorption spectra with both current and future detection systems
- Durable; proven to last the set lifetime on a diverse range of banknote substrates



Print viewed at infrared wavelengths showing ir-reflecting ink "drop-out" while ir-absorbing ink is visible as dark gray

These novel materials have been developed to function in combination with a wide range of other security pigments, thus enabling the printing of multi-functional security features. As well as adding security, this helps address the issue of feature overcrowding.

LEVEL 3, FORENSIC SECURITY FEATURES.

These features are typically utilised by high-speed banknote sorting systems and police authorities. Part of the security of such systems relies on their secrecy…

IN SUMMARY

Longer-life, lower cost banknotes with ever-evolving security are demanded by issuers globally, and meeting these challenges requires a strong marriage of Design and Technology.

Multi-functional print features have helped address the feature-overcrowding which has arisen from the need to cram more defences into less space. By working together, banknote designers and component technologists maximise available real estate, ensure cost-effective security and continue to deliver banknotes that are attractive, reliable, durable and fit for purpose. ■

Nowhere to hide?

Even in Europe, it is hard to escape CCTV cameras

Technology is neither good nor bad but it can be used for ends that are either good or bad. Facial recognition is one of those technologies where the public is not completely sure how it is used.

Artificial Intelligence, especially in connection with automatic identification, was already discussed in the last issue of Infosecura, when we concentrated on facial recognition. But the technology seems to be so much discussed, that it merits another look. In the context of our industry, facial recognition or 'biometric artificial intelligence application' is most commonly encountered at border crossings, such as airport ABC gates, where a passport or ID card photo is compared with the image of a person in front of the camera. As it is a one-to-one recognition, it is highly accurate and from a privacy point of view, largely uncontroversial as neither the image of the passport photo nor the one of the face in front of the camera need to be recorded nor held in a database. It is simple an automated version of the job done by real live border guards, who compare picture and face.

THE EU THINKS RESEARCH INTO FACIAL RECOGNITION IS IMPORTANT

The European Union is currently updating its regulation on national ID cards to include, apart from the machine-readable zone, mandatory biometric identifiers, i.e. a photograph and two fingerprints stored on a contactless chip. The photo on a (EU member) national ID card is just that, a photo, and it is not linked to any EU database, but individual countries may decide differently. However, a photo is still the basic ingredient of any facial recognition system.

The EU is valuing privacy very highly and even for sensitive application, the least intrusive method of identification is used. For example for EURODAC, the European Asylum Dactyloscopy Database, an EU asylum fingerprint database used for identification of asylum applicants created in 2003, only fingerprints were collected (along with date and place of registration) and no other personal information. However, the system was more or less overwhelmed due to the migration and refugee crisis in 2015, and the European Commission proposed to strengthen EURODAC by a. o. including other biometric identifiers such as facial images and to use facial recognition.

Facial recognition may be the least reliable of the three common biometric identification systems - fingerprints, iris scans and facial recognition - but is has the advantage of being non-intrusive and its quality is fast improving. The EU is also spending research money to improve the accuracy of it, such as a €100 000 research grant to Istanbul Technical University for MMFP (multimodal face processing) completed in 2017, and an on-going project with Tel Aviv University called 'Deep Face' that started in 2017 and runs until 2022, which is financed with close to € 1 700 000 by the European Research Council . Another EU-funded project - to the tune of € 4,5m - that is even more ambitious and which will be finished in August 2019 is called *iBorderCtrl*. It is designed to develop an 'intelligent control system' to ease land border crossings into the EU and help border guards to spot illegal immigrants. iBorder Ctrl's system will collect data that will 'move beyond biometrics and on to biomarkers of deceit.' When operational, travellers will use an online application to upload pictures of their passport, visa and proof of funds, then use a webcam to answer questions from a computer-animated border guard, personalised to the traveller's gender, ethnicity and language. The unique approach to 'deception detection' analyses the micro-gestures of travellers to figure out if the interviewee is lying. This pre-screening step is the first of two stages.

The second stage takes place at the actual border. Travellers who have been flagged as low risk during the pre-screening stage will go through a short re-evaluation of their information for entry, while higher-risk passengers will undergo a more detailed check. Information will be automatically cross-checked with a hand-held device, comparing the pre-screening facial images to passports and photos taken on previous border crossings. After reassessing the traveller's documents, and fingerprinting, palm vein scanning and face matching have been carried out, the potential risk posed by the traveller will be recalculated. Only then does a border guard take over from the automated system.

Trials have started in Greece, Hungary and Latvia. In spite of these efforts, it is, however, unlikely that progress in the area of facial recognition as well as funding for it from Europe is anything to rival the efforts of China's universities and the state.

CHINA'S DOMINANCE IN THE FACIAL RECOGNITION SECTOR

Last year the South China Morning Post wrote about five AI start-ups that have become dominant in the realm of facial recognition. One of them is called Megviie, a company started in 2011, which last year raised $100m, giving it a valuation of nearly $2bn and turning it into the world's first billion-dollar start-up from the "facial-industrial complex". Over 300 000 developers in 150 countries use its face recognition technology which is called Face++. Megvii's technology is also used by the Ministry of Public Security, which oversees a facial scan database of more than 1.3 billion people in China.

Another company called Yitu Technology, based in Shanghai, has gained wide recognition for its Dragonfly Eye System, a facial scan platform that can identify a person from a database of at least two billion people in a matter of seconds. And then there is SenseTime from Hong Kong. The company became the city's first hi-tech unicorn – a start-up valued at US$1 billion or more. SenseTime has more than 400 customers and strategic partners.

The rapid rise of these companies implies that their services are finding eager customers, and one of the most important one is the state. Sky Net in China is the largest video surveillance system on Earth, Chinese government research institutes and a company involved in the project said. The Sky Net programme, now renamed Pingan Chengshi, or Safe Cities, claimed to have connected 170 million cameras across China last year. By 2020, another 400 million units will be installed. China has also started a vast surveillance programme to track and control the 11 million strong ethnic minority of Uighurs, who live mainly in the western province of Xinjiang. It is the first known example of a government intentionally using artificial intelligence for racial profiling, the New York Times wrote.

Of course not everything in AI goes without a hitch, at least as long as humans are involved. In summer last year, a Chinese developer of artificial intelligence security software systems left its database exposed online, leaving the personal information of Chinese citizens vulnerable. This included the gender, address, birthdate, and nationality of more than 2.5 million people in China. It also included each person's employer and a photo. This type of private information is linked to the ID card number that Chinese residents are required to have. That ID number was also exposed in this Chinese facial recognition debacle.

BEHAVE YOURSELF - YOU ARE BEING WATCHED

Shelley Kramer at Futurumresearch.com writes (20/3/2019) that in China, facial recognition technology is sophisticated and part of everyday life. Even the subway system in Beijing is getting ready to use this technology, and police officers use special glasses that let them quickly recognize faces, to aid in the rapid identification of suspects. The same author also wrote that the Chinese are currently testing a very controversial social credit scoring system, designed to monitor unattractive or unhealthy behavior (e.g. "frivolous spending, being wasteful, smoking where it's not permitted, or not being a "good citizen"). This system is expected to roll out in 2020 and may preclude Chinese citizens with low social credit scores from traveling, getting a loan, a good job, or having educational opportunities.

A BEGINNING PUSHBACK

In Europe and North America, all this smacks too much of George Orwell's novel 1984 and a certain resistance is building up. In mid May, San Francisco became the first U.S. city to ban the use of facial recognition by police and other city agencies, such as the city's transport authority. Similar legislation was pending in Oakland, California and in a town in Massachusetts. The California Legislature is considering a proposal prohibiting the use of facial ID technology on body cameras for the whole state of California. A bipartisan bill in the US Senate would exempt police applications but set limits on businesses analysing people's faces without their consent.

There is also a more private pushback. A group in Berlin that calls itself the Peng! Kollektiv, offers on its website a service that morphs photos to make facial images unusable, or at least very confusing, for facial recognition. The website Mask.ID (https://mask.id/en/) even claims that they have hacked the German Bundesdruckerei and had a passport printed in which two people can be identified: the EU Commissioner for Foreign Affairs and Security Policy, Federica Mogherini, and a person from its own team. The website states that its aim is "to empower us with our data, to shape our identity ourselves. To flood the databases with misinformation, to avoid automatic recognition, to bring administrators of these databases to our site, and to determine our own data." The website admits that legally it may be on very slippery ground but states that so far no court case has confirmed criminality. It insists however that this is a political issue, not a purely legal one. ■

FACIAL RECOGNITION: THE BACKLASH

The assumption that the use of facial recognition technology at airports would not raise too many heckles, turned out to be too lenient a view. *The Guardian* wrote (June 5) that privacy groups in the US started a website called AirlinePrivacy.com, that shows users which airlines use facial recognition technology to verify travellers identity before boarding. Instead of verifying passengers' details by scanning a boarding pass, the technology – which is provided by government agencies – scans passengers' faces and sends that information to border control to verify identity.

The airline JetBlue began using the technology in 2017 in partnership with federal agencies, after an executive order by Donald Trump pushing for the use of facial recognition technology in US airports. Soon after, other airlines followed. Although airlines say they do not store passengers' data, it is shared with federal agencies that are able to store it. US Customs and Border Protection said it retains biographic exit records for US citizens for 15 years and for non-citizens for 75 years. Photos are kept for 12 hours.

Though biometric boarding programs are not a security requirement for flights in the US, many passengers may not know they can decline its use. In most cases, the technology is implemented on an opt-out basis, meaning passengers are automatically enrolled unless they instruct otherwise. The opt-out basis of the programs puts the onus of maintaining privacy on the consumer, who may not know they are being tracked to begin with, Demand Progress, an activist group said.

"If you are opting in, you are giving explicit consent for whatever is happening, but the fact that it is opt-out means the assumption is that everyone who is flying JetBlue wants to be in the facial recognition system, and that is just not true," said Jelani Drew, a campaigner at Fight for the Future, an other privacy activist group. Drew said, airlines' use of the technology marks a new frontier in privacy invasions. Airlines that are using the technology point out that it is used only at certain airports such as Los Angeles and Atlanta. But it is early days yet. ■

EU TRAVEL DOCUMENTS: FIT FOR THE FUTURE?

It is not only counterfeiters that make identity documents unsafe and obsolete, developing technology is an even stronger driver of change as a recent presentation by Silvia Kolligs-Tuffery pointed out at a recent conference in London

This article is based on a presentation by Silvia Kolligs-Tuffery , Team Leader, Document Security, European Commission

One of the most urgent problems facing the vast arc of so-called developed nations in Europe and North America is migration in its many forms. Born of wars, severe disruptions caused by climate change and corrupt and inefficient governments, the flow of people seeking safety and better living conditions have already disturbed the political balance in many democratic countries. Their number is the highest recorded since World War II. The global population of people displaced by conflict reached 70.8 million last year, up from a little over 43 million a decade ago.

Most of those uprooted by conflict worldwide in 2018 — around 41 million — remained displaced in their own countries, while close to 26 million fled across borders and 3.5 million were seeking asylum in third countries, such as in Europe or North America. Some countries opted for totally or almost totally closing their borders, and the number of welcoming countries is getting smaller. This is not only a political problem but humanitarian as well. Moreover, we should not forget that most migrants do not chose to leave their countries voluntarily but were forced out, directly or indirectly. We should also not forget that immigration carries a cost for the originating counties as well, as often the most educating and most enterprising people leave first.

Rather than closing its external borders, the European Union, while trying to protect its borders, has opted to manage migration and the movement of people into and out of its territory. One of the tasks connected with this is reducing or eliminating travel document fraud in all member states. The Commission regards travel document security as a key factor in better border protection and migration management and the move towards an effective and genuine Security Union.

To this end, new legislative proposals have been made and were passed (see article on p. 16) on June 6, 2019 to increase the security of ID cards and Emergency Travel Documents. The new regulation mandates minimum security standards in accordance with ICAO DOC 9303 and a uniform format for residence permits. Member states are free to add further security features. ID cards also need to have an integrated chip with the facial image of the bearer and 2 fingerprints. While the format is harmonized the layout is not, but the European symbol of the two letter country code of the issuing member state encircled by 12 yellow stars and printed in negative in a blue rectangle; is mandatory. The standard validity is a minimum of five and a maximum of ten years with some exceptions for old people. The ID card regulation does not force member countries that do not have mandatory ID cards to introduce them.

RESIDENCE DOCUMENTS

Residence documents for EU nationals (not necessarily in card form) living in another member state than their own have to have information, such as the title in at least two languages, reference to Union citizenship, document number, name, date of birth, issuing authority and the European symbol. Residence cards issued to non-EU family members of mobile EU citizens will be issued in the format of the residence permit according to Regulation (EC) 1030/2002.

The phasing out of existing ID cards is set to five years after the date of application of the Regulation (two years after entry into force) if they are not ICAO compliant and 10 years for compliant cards. For residence cards two and five years apply respectively.

EU EMERGENCY TRAVEL DOCUMENT

The current EU ETD dates from 1996 and needed to be modernised. A new Commission proposal for a Directive on a new ETD is agreed and will be adopted still in June. It provides for a new document consisting of a uniform threefold form and a sticker, similar to the current visa sticker, to be affixed on it. It will be issued to EU citizens who have lost their documents in a foreign country. It can also be used for own citizens within the EU. The technical specifications are to be set out by the Article 6 committee.

IMPLEMENTATION OF THE NEW VISA STICKER AND THE RESIDENCE PERMIT

The technical specifications for the new uniform format for visas have been adopted. The deadline for the production of the new visa sticker is 21 June 2019 and the date for using up the old visa sticker is 21 December 2019. Some Member States have already issued new visas such as Germany and Austria and unfortunately they were already

targeted by forgers. For the new residence permit, the electronic data have only be recently distributed so that all Member States are in the phase of preparation.

STUDY ON DIGITAL VISAS

COM was asked to explore how technologies provide new opportunities to simplify visa processing for both applicants and consulates. To this end a study was commissioned which looks into the possible options to digitalise the visa application process and the visa sticker. The idea is to check the visa holders data, which are already stored in the Visa Information System without a need of an additional sticker. The study will be finished in August this year and COM will decide on taking initiatives in this sense.

ICAO: DIGITAL TRAVEL CREDENTIALS!

ICAO is also working on the topic of Digital Travel Credentials (DTC) which are in essentially a copy of the digital part of the passport. A physical travel credential could be a mobile phone; it is just a different form factor but should be secured. A preferred solution would be a combination of virtual and physical travel credential, as virtual data are always linked to a physical device. Work on the technical report started, which will describe the different options for the creation of a DTC and foresees additional information for internal use, for example an additional picture.

SO, ARE OUR PHYSICAL DOCUMENTS FIT FOR THE FUTURE?

In the view of Mrs. Kolligs-Tuffery of the Commission, the way to digital documents is clear but it will still take some time until we are there. Therefore the use of physical documents will still be necessary in the near future. We can look at the different processes:

- The digitalisation of the application process: we need to make sure that it is secure to avoid identity fraud;
- The visa: as all information is already in the Visa Information System, it should be an easy way to the digital visa; we only have to think about rare situations where the system is not reachable such as controls in remote areas and provide for fall-back solutions.

For the passport it may take longer as it is used mainly for international travel and not all countries may implement DTC at the same time. Therefore it may be a good way to start with a combination of physical and digital documents in order to allow for adaptation on the side of the person checking but also on the side of the holder. It is crucial for the success to exchange information and work together so that we have interoperable standards which can be used worldwide. ■

EU TO IMPROVE SECURITY FEATURES OF ID CARDS

The Council and the European Parliament have reached an informal agreement on a regulation, proposed last year by the Commission, which will strengthen the security of identity cards and of residence documents issued to EU citizens and their non-EU family members. The Commission estimated that currently 80 million Europeans still only have non-machine readable ID cards without biometric identifiers. While there are common EU security standards for passports, visas and residency documents for non-EU nationals living or working in Member States, no such standards exist for national ID cards and residency documents .

Under the proposed new rules, identity cards will have to be produced in a uniform, credit card format (ID-1), include a machine-readable zone, and follow the minimum security standards set out by ICAO (International Civil Aviation Organisation). They will also include a cardholder's photo and two fingerprints, stored in a digital format, on a contactless chip. ID cards will indicate the country code of the member state issuing them, inside an EU flag.

Identity cards will be valid a minimum of 5 years and a maximum of 10 years. For persons aged 70 and above ID cards can have longer validity and for minors validity may be less than 5 years.

PHASING OUT OLD ID CARDS

The new rules will enter into force 2 years after adoption, and non-conforming existing ID cards will stop being valid 10 years later. The least secure cards, which do not meet the minimum security standards or do not have a machine-readable zone will expire within five years.

DATA PROTECTION SAFEGUARDS

The proposed new rules include strong data protection safeguards, to ensure the information collected does not fall into the wrong hands. In particular, national authorities will have to ensure the security of the contactless chip and the data stored in it, so that it cannot be hacked or accessed without permission.

In addition, the new rules refer only to the security and information to be stored in the ID cards. They do not provide the legal basis for the creation of new databases at national or EU level, which is a matter of national legislation that needs to be in full compliance with data protection rules.

The proposed rules do not require member states to introduce identity cards or residence documents if they are not foreseen under national law. ■

23-25 OCTOBER 2019

SecurityPrinters
Banknotes+Identity

INTERGRAF

www.securityprinters.org