YEAR 20 DECEMBER 2017/ **ISSUE 74**

INFOSECURA

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. All rights reserved. No part of the publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording or use in any information storage or retrieval system without the express prior consent of the publisher. 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

Looking at both sides

This issue of Infosecura seems to have some articles that take positions which contradict each other. There is the article on page 3 about the Europol Internet Organized Crime Threat Assessment (IOCTA), which - very gently and politely - complains that privacy concerns, sometimes anchored in national or EU legislation, hamper vigorous investigation of cyber criminals. “A combination of legislative and technical factors, which deny law enforcement access to timely and accurate electronic communications data and digital forensic opportunities, such as lack of data retention and criminal abuse of encryption, are leading to a loss of both investigative leads and the ability to effectively attribute and prosecute online criminal activity.”

The article about ‘Facial recognition and privacy’ gives voice to opposite concerns and quotes the fears of the American Civil Liberties Union, one of the most vigorous defenders of the rights to privacy of citizens. Both the criticism of the investigative restraint that international agencies such as Europol and national police agencies experience when investigating cyber crimes and the fear of the ACLU that law enforcement may be in danger of overstepping the red lines that protect privacy, are, although contradictory, reasonable and probably justified. However, in a society that subscribes to the idea of checks and balances and the independence of the judiciary, as most real democracies do, these issues are solvable. As the IOCTA states, although in a somewhat narrower context: “Such issues require a coordinated and harmonised effort by law enforcement, policy makers, legislators, academia, civil society and training providers to effectively tackle them.”

The other article that reports on an event that employed this “devils advocate” technique, is the one that describes the symposium by the Banque de France on “Looking at banknotes through the eyes of counterfeiters”. Here it was the Banque de France itself that played the part of the devil, in creating perfect counterfeits with commercially available means. Counterfeiters will always be with us and it is therefore useful not only to know how they work, but how they think.

While one can imagine that counterfeiters, such as Czesław Bojarski, mentioned in the article on the Banque de France symposium, took some pride in their work and felt satisfaction of having fooled the mighty central banks for so long, modern counterfeiters - and those in the past as well - are ‘in it for the money only’ and will always choose the easiest and most direct way to that money. If that means counterfeiting banknotes or documents, that’s what they will do, if hacking electronic means of payment and electronic documents is easier and poses fewer risks, that will be their choice. For the ‘good guys” this means constant vigilance in every area.

The Editor

The year cybercrime hit home

The keynote speech at Intergraf's 2018 Security Printers Conference and Exhibition will put the fight against cyber-criminality into a prominent place. Scientists, such as the keynote speaker and national law enforcement agencies as well as international ones, such as Interpol and Europol, are doing valuable work to identify the threats and to find ways to combat them. Europol's Internet Organized Crime Threat Assessment (IOCTA) provides a useful update on the issue.

Europol said that 2017 was the year that cybercrime hit close to home. We can even extend that time back to 2016 when 'unauthorized cyber interference' tried - and possibly succeeded - in threatening and destabilizing our democratic systems. It has probably now dawned on everybody that cybercrime is a threat to our way of life, our security and our material wellbeing. The European Union again officially pointed to that threat when EU Commission President Jean-Claude Juncker stated in his annual State of the Union Address: "In the past three years, we have made progress in keeping Europeans safe online. But Europe is still not well equipped when it comes to cyber-attacks."

Cybercrime has many facets, from political destabilization through false information, child pornography and drug dealing to payment fraud, facilitating document and even currency counterfeiting, money laundering, people smuggling and many other crimes. Intergraf is also focusing attention on it by asking noted cyber-psychologist Prof. Dr. Mary Aiken to give the keynote speech at the Security Printers Conference in Dublin in March 2018. An interview, in which Prof. Aiken will talk about the psychological make-up and the modus operandi of cybercriminals, will be published in the next issue.

The Internet is the tool that made the dreams of organized crime syndicates come true. Last year, there were more than 4,000 ransomware attacks per day and 80 per cent of European companies experienced at least one cyber-security incident. The economic impact of cyber-crime has risen fivefold over the past four years alone. Countries have reacted individually and there is a concerted effort by the European Union to fight cybercrime, with a proposal to set-up a EU Cybersecurity Agency to assist Member States in dealing with cyber-attacks. 2017 was also the year, Europol issued a new Internet Organized Crime Threat Assessment (IOCTA), which identifies the main cybercrime threats and provides key recommendations to address the challenges.

INTERNET ORGANIZED CRIME THREAT ASSESSMENT

Europol's IOCTA states that while many aspects of cybercrime are firmly established, other areas have witnessed a striking upsurge in activity, including attacks on an unprecedented scale, as cybercrime continues to take new forms and new directions. Because of the similar tools and techniques used, it is sometimes difficult to attribute cyber-attacks to particular groups, for example, financially motivated cybercriminals or Advanced Persistent Threat (APT) groups, which may point to political motifs. Some of the reported cyber-attacks from mid-2017 illustrate this trend. For genuine financially motivated attacks, extortion remains a common tactic, with ransomware and Distributed Denial of Service (DDoS) attacks remaining priorities for EU law enforcement.

The number of criminal groups specialising in direct, complex attacks on ATMs and banks is also increasing, resulting in dramatic losses for the victims. Direct attacks on bank networks to manipulate card balances, take control of ATMs or directly transfer funds, known as payment process compromise, represents one of the serious emerging threats in this area. The US and Southeast Asia are still key locations for cashing-out compromised EU cards.

Card-not-present (CNP) fraud continues to dominate non-cash payments fraud, hitting the retail sector heavily. Airline ticket fraud continues to have significant impact across the EU and facilitates a wide range of other crime types, from drug trafficking to illegal immigration. Card-present (CP) fraud accounts for a much smaller portion of non-cash payment fraud, yet the number of reported cases has reached record numbers. Payment fraud generally is characterised by a high volume of low value crime incidents, the full scope of which cannot be envisioned by local reporting and the investigation of individual single illegal transactions. A more coordinated and intelligence-led approach to combatting payment fraud is required throughout the EU.

A HEADACHE FOR LAW ENFORCEMENT

The fact that possession of stolen or compromised sensitive online payment credentials is not a criminal offence across all EU member countries makes it more difficult for national law enforcement as well as for agencies such as Europol to investigate such crimes and to bring them to the courts. 'A combination of legislative and technical factors, which deny law enforcement access to timely and accurate electronic communications data and digital forensic opportunities, such as lack of data retention and criminal abuse of encryption, are leading to a loss of both investigative leads and the ability to effectively attribute and prosecute online criminal activity. Such issues require a coordinated and harmonised effort by law enforcement, policy makers, legislators, academia, civil society and training providers to effectively tackle them.' The latter statement in IOCTA shows that the possible conflict between privacy protection and the fight against cyber criminality needs to be resolved without weakening either of them.

THE INTERNET OF VULNERABLE THINGS

There is also a large potential for the abuse of insecure Internet of Things (IoT) devices. By the end of 2016 we had witnessed the first massive attack originating from such devices, as the Mirai malware transformed around 150 000 routers and CCTV cameras into a DDoS botnet. This botnet was responsible for a number of high profile attacks, including one severely disrupting Internet infrastructure on the west coast of the United States.

While sophisticated cyber-attacks against European critical infrastructures are a real threat, attacks using commonly available cybercrime tools such as booters/ stressers appear to be much more likely, and easier to achieve.

A growing amount of illicit trade now has an online component, meaning that cybercrime investigative capabilities are increasingly in demand in all serious organised crime investigations. Darknet markets remain a key crosscutting enabler for other crime areas, providing access to, amongst other things, compromised financial data to commit various types of payment fraud, firearms, counterfeit documents to facilitate fraud, trafficking in human beings, and illegal immigration. Compared to more established Darknet market commodities, such as drugs, the availability of cybercrime tools and services on the Darknet appears to be growing more rapidly.

Cryptocurrencies continue to be exploited by cybercriminals, with Bitcoin being the currency of choice in criminal markets, and as payment for cyber-related extortion attempts, such as from ransomware or a DDoS attack. However, other cryptocurrencies such as Monero, Ethereum and Zcash are gaining popularity within the digital underground.

Most of the information in this article has been taken from the Europol Internet Organized Crime Threat Assessment, which can be downloaded from: https://www.europol.europa.eu/iocta/2017/index.html ■

THE NEW FACE OF INTERGRAF'S CERTIFICATIONS

Doris Schulz-Pätzold, Customer Relations & Certification Manager

At latest count, 115 production sites in 46 different countries have been certified according to ISO 14298 and CWA 15374. Intergraf has developed standards for security printers and their suppliers for over 15 years and initiated the development of the CWA 14641, CWA 15374 and, most recently, ISO 14298 standards in cooperation with representatives from standardisation bodies and industry experts from 25 countries on 5 different continents. There is now a growing trend for companies to consider compliance to standards such as ISO 14298 and CWA 15374 as a requirement for doing business. Intergraf has a dedicated Certification Officer to serve as the link between Intergraf, the certification bodies and the certified or to be certified companies.

After Patricia Engler, Intergraf's last Certification Manager left to start a family, Intergraf's certification efforts have a new face: Doris Schulz-Pätzold, who joined in September as Customer Relations & Certification Manager. Doris is a Business Economist, who has been a part of the security printing and card technology industry since 1992.

Before joining Intergraf in 2017, she held various sales, marketing and project management roles at Challenge Card Design, a LaserCard company, Bundesdruckerei and HID Global, with a focus on highly secure documents.

Doris has built up extensive experience in the fields of security features, printing procedures, manufacturing and personalisation processes, and has supported numerous customers in the implementation of their ID card, ePassport, driver license and access control projects.

As Customer Relations & Certification Manager, Doris acts as the contact person for security printers, suppliers and customers for all questions related to Intergraf's certifications. ■

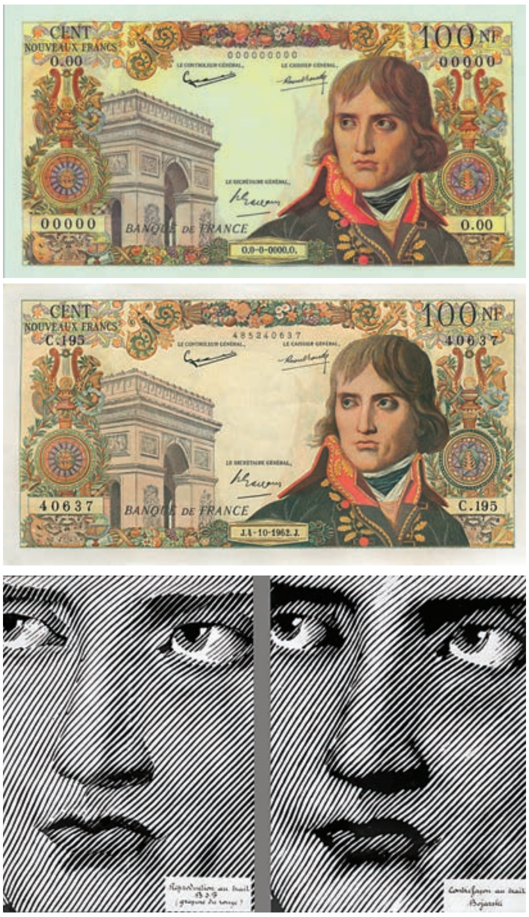
Looking at banknotes through the eyes of counterfeiters

'Anything can be counterfeited eventually' is a truism one hears at any gathering of anti-counterfeiting experts. While not able to prevent all counterfeiting, the unit founded by the Banque de France 30 years ago has been fighting to make the life of counterfeiters more difficult and risky.

The European Central Bank, Interpol, Europol, the US Secret Service and many central banks all over the world invest much in fighting counterfeiting. The Banque de France, thirty years ago, founded a special agency, the Counterfeit Research Centre, not only to detect counterfeit currency, but to find out how counterfeiters think and act, to play, in effect, the role of a 'devil's advocate' to detect present and prevent future counterfeiting. The 30th anniversary of the Counterfeit Research Centre, which was marked with a symposium in Paris, provided a welcome opportunity to celebrate the unique and valuable work of this agency and to look at the whole subject of counterfeiting, past, present and future in the magnificent setting of the headquarters of the Banque de France in Paris.

When the Counterfeit Research Centre was founded, its aim was to protect the French Franc. Today it is part of a network of research organisations, including the European Central Bank's Counterfeit Analysis Centre, which coordinates technical and statistical information on counterfeits. The information stored in the centre's database is shared with national police forces and other bodies involved in combating counterfeiting.

A look to the past, provided by a temporary exhibition at the Hôtel de Toulouse, the bank's imposing 17th century Paris residence, shows clearly that counterfeiters had many of the qualities that their successful law-abiding contemporaries also had. They were resourceful, inventive, observant, open to new developments and inventions, etc. Unfortunately, they applied their talents to criminal ends. Shortly after details of Nicéphore Niépce's and Louis Daguerre's invention of (black-and-white) photography were published in 1839, the first banknote counterfeit using this process was found. And so it went on, after every important technical invention in paper making, printing or reproduction, counterfeits using the latest technology appeared.



On top, the real Napoleon note, below Bojarski's handywork, with the original line engraving on the left and Bojarski's engraving on the right.

Among the exhibition's impressive collection of historic counterfeits, one of the exhibits showed the persistence and ingenuity of one particular counterfeiter. Czesław Bojarski, a Polish emigré, recreated a complete banknote factory in his basement. He made his own cotton banknote paper, complete with an (almost) perfect watermark, engraved the intaglio printing plates and rigged-up a makeshift intaglio press, and printed the rest of the notes on a professional letterpress machine. The result was almost perfect and he was only caught through the clumsiness of one of his distributors. Bojarski had spent his apprenticeship years in the 50s counterfeiting the 1000 Franc notes, graduating in 1958 to the Ffr. 5000 notes. The period in which he became known as the " Cézanne of counterfeiters" began in 1962, when the Banque de France issued the new "100 Nouveau Franc type Bonaparte" note. His counterfeits of the new note were so good, that when he was finally arrested, the judge recognized the quality of his work, but added “this brilliance does not reduce his culpability”. He printed 30 000 counterfeit notes and even about 40 years later, in 2015, one of his counterfeits sold for € 7 173 at auction.

Today’s counterfeiters do not need to be artists or even craftsmen and the Banque de France did not create the Counterfeit Research Centre specifically to fight against ‘artisanal’ counterfeits of the type Bojarski. The threat the Banque de France and indeed all central banks feared thirty years ago, came from the new colour copiers.

In the past thirty years, colour copiers have vastly increased in sophistication, but so have banknotes. The Central Bank Counterfeit Deterrence Group, CBCDG, to which now around 50 major currency issuing central banks belong, has developed very effective counter measures to prevent copying and printing banknote images by electronic means. So are our modern banknotes safe from counterfeits with their arrays of highly complex security features? Well, no, as counterfeits do not aim to deceive experts, but ordinary, preoccupied and distracted users of banknotes and modern colour copiers are well capable of producing easily acceptable notes. There are laser printers that offer white toner - for printing the background of polymer notes - and special colours. Even OVDs can be simulated with everyday products such as nail varnish and even the most complicated hologram stripes and patches are available on the ‘dark net’. The latter would only be used for the highest category of counterfeits, professional, rather than for semi-professional or ‘casual’ counterfeits.

He knows which one is the fake: Fabrice Capiez, Counterfeits Unit Manager, Banque de France and organizer of the Symposium

To give a tangible example of the threat of counterfeiting, the Counterfeit Research Centre had produced a sample note both on a paper and polymer substrate using only technology readily available to counterfeiters. The face of this note shows a classic French banknote design inspired by the Ffr. 5000 note of the 1940s, while the reverse shows a modern, riotous explosion of colour and shapes. In a final demonstration of the dangers of every day reproduction technology, and to fulfil the promise of the title of the symposium ‘to look at banknotes through the eyes of counterfeiters’, the team of the Counterfeit Research Centre reproduced, or counterfeited, its own sample note, using commercially available equipment and materials. But of course, like the rest of the content of the seminar, how it was done remains highly confidential. The face on both sides of the note is that of the Roman god Mercury, the god of travellers, traders and of thieves, and apparently, also of those that pursue them. ■

A LOSS TO BANKNOTE PRINTING

Life for smaller currency printers has become more difficult. One of the oldest of such companies has just exited the market. This is a loss for the whole industry.

We have known about it since December last year, but any thought of a white knight suddenly appearing out of the blue to rescue one of the most venerable members of our industry, finally had to be laid to rest: the banknote printing division of Royal Joh. Enschedé had stopped printing. On September 28 , the company not only closed its banknote printing division, but it also auctioned off much of the equipment in the plant. Although the website of the auctioneer featured an impressive looking KBA Notasys machine, it was a Notaprotector varnishing and sheet finishing unit - with an opening bid of € 350 000 - that would not be very useful in the hands of counterfeiters. To make doubly sure, the Dutch national police and Interpol, in line with its S-Print Project, were monitoring the auction, to be certain, that no sensitive equipment would fall into wrong hands.

A DUTCH GOLDEN AGE

Ending banknote printing in the Netherland is also the end of a very long chapter in the country’s history. Joh. Enschedé in Haarlem was already a venerable company when it started printing banknotes. Founded in 1703 by Izaak Enschedé as a newspaper and book printer, the company printed the very first Dutch banknote, the “Roodborstje” (Robin Redbreast) in 1814. At that time, the Netherlands had a far-flung empire and the colonies, such as Java or Surinam, etc. as well as the Netherlands itself had their banknotes printed in Haarlem. And it was very good business. In 1866, after the death of Johannes Enschedé III, Joh. Enschedé sold the family’s book business and also began printing stamps, an activity, the company carries out until this day.

The company also became one of Europe’s leading type founders, an activity that started in the 19th century and endured until after the demise of lead

250
de nederlandsche bank
tweehonderd vijftig
gulden

The 250 Guilder note of 1985, designed by R.D. Oxenaar (top) and the 10 Guilder note of 1997 by Jaap Drupsteen.

type. The typefaces designed by Jan van Krimpen between 1925 and 1952, for example, are regarded as outstanding, even today.

In 2003 Joh. Enschedé en Zonen celebrated its 300th anniversary in grand style and Queen Beatrix of the Netherlands even bestowed the designation "Royal" on the company.

Until the arrival of the Euro banknote, Dutch banknotes were at the forefront of banknote design. While the Guilder notes looked rather conventional until 1966, after that date the design became simpler, bolder and more geometric. Between 1977 and 1985, the striking sunflower, snipe and lighthouse motifs married bold figurative and abstract geometric design and strong colours to great effect. In the years 1989 to 1997 the design became even more dense and geometrical. Guilder notes had become an expression of Dutch modernity and culture, which the Euro notes that replaced the Guilders could not even hope to emulate, as these had to appeal to a much larger and culturally much more diverse audience without offending anyone. They indeed did not offend anyone, but they probably did not excite anyone either.

DE NEDERLANDSCHE BANK
10
IJSVOGEL
TIEN GULDEN

A NEW ECONOMIC REALITY

A decade or so after the anniversary, the fortunes of the company began to turn to the worse and in 2014, 95 per cent of the company was sold to the investment company Nimbus. The Enschedé family, which had not only owned but also managed the company for about 300 years, only retained a 5 per cent share. Royal Joh. Enschedé said it will now be focusing as a High Security Printer on the international market for stamps, visas and tax labels, together with interesting growth markets such as 'brand protection' and 'anti-counterfeit'.

JOH. ENSCHEDÉ AND INTERGRAF

The relationship between Intergraf and Royal Joh. Enschedé has been close for decades. For many years, Johan Wotte, the technical director of the banknote printing division of the company, was a member of the committee that organized the Security Printers conferences, now called the Committee of Experts. After the death of its first chairman, Count Ferdinand von Waldburg-Wolfegg, Johan served as the Committee Chairman until the Security Printers Conference in Montreux, Switzerland in 2003. ■

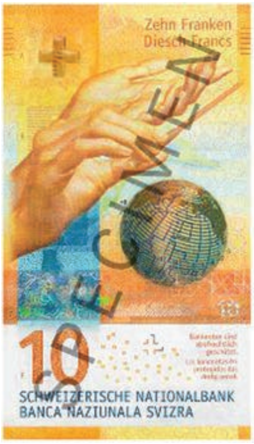
10
amsterdam 25 april 1968
secretaris
president
de nederlandsche bank
TIEN GULDEN
10

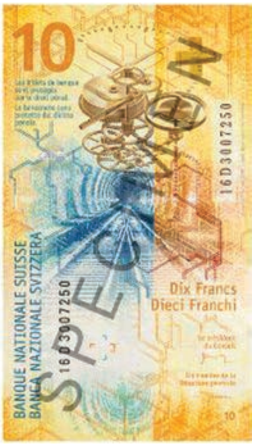
R.D. Oxenaar's 10 Guilder note of around 1966, with his fingerprint hidden in the portrait of Frans Hals.

WHEN BANKNOTE DESIGN WAS PERSONAL

Almost as a final full stop to the end of banknote printing at Royal Joh. Enschedé, the designer of the famous 250 Guilder note (see above left), Robert Deodaat Oxenaar, died in June, aged 87, in Massachusetts, USA. Oxenaar's designs were a breakthrough in banknote imagery. He designed two series of banknotes for the 'Nederlandsche Bank' from 1966 to 1985, which were bold, irreverent and very memorable. The first series featured key figures from the history of the country, with simple strong portraits in strong colours against a white background. Oxenaar was not only a brilliant designer but also a joker or a rebel, although an extremely discreet one. In the 10 Guilder note, he smuggled his fingerprint into the portrait of Frans Hals. Oxenaar revealed in an interview that "on the 1000 Guilder note it became a sport for me to put things into the notes that nobody wanted there. I was proud to have my fingerprint in this note - and it was my middle finger! It was too late when they found out and though the director saw it, he said he would not stop the whole production".

In the second series, Oxenaar replaced colonial figures, such as Admiral de Ruyter on the 100 Guilder note, with an endangered bird, the water snipe, and featured a sunflower on the 50 Guilder and a lighthouse on the 250 Guilder notes. All of these became a resounding popular success. The lighthouse note also featured his last jokes. On the top of the structure he placed the names of a friend, his girlfriend and his granddaughter. He also managed to smuggle a watermark of his girlfriend's rabbit into the note, so that people would walk around with her rabbit in their pocket. (Source: International Banknote Society Journal) ■





MAKING THINGS RUN ON TIME

The third note of the Swiss National Bank's ninth series again depicts a typical Swiss characteristic, in this case 'organisation' with the key motif of 'time'.

The only people more famous for punctuality and precision than the Germans are the Swiss. While such generalisations have to be taken with a pinch of salt, there is enough truth in these myths to shape expectations, those of the Swiss themselves and those of their neighbours.

Punctuality and precision imply organisation and that is the theme of the new 10 Swiss Franc note that was unveiled on 11th October and entered circulation one week later. Organisation as a subject is difficult to visualize and the Swiss National Bank chose time and diverse things associated with time to tell the story of organisation. As on the two first notes of the 9th Swiss series, the Sfr 50 and Sfr 20, the most striking elements on the face of the new Sfr 10 are hands and a globe. Here, they are the hands of a - female - conductor, setting the tempo of the music with the baton. The globe, as in the previous new notes with a striking Spark feature, shows the world's time zones.

The broad transparent security stripe on the front shows the Swiss rail network and lists the longest rail tunnels. When tilted, red and green numbers appear on four lines and move in opposite directions. The background of the note is, on closer inspection, made up of clock faces. On the back the theme of time continues. Tunnels form part of Switzerland's complex rail network, which runs smoothly thanks to good organisation and precise time-keeping, the SNB explains on its website. Above the image of such a tunnel, the other traditional symbol of Swiss time keeping is placed, the movement of a mechanical watch.

The security features of the note follow exactly those of the new 20 and 50 Franc notes, although there seem to be slightly fewer of them. The substrate is again Landqart's three-layer Durasafe and there is a plethora of features, from a window in the shape of the Swiss cross, to the same image micro perforated and as a tilt image as well as a watermark and a see-through register feature. With 70mm x 123mm the Sfr 10 note is the smallest in the series. All notes keep to the same width, but the length increases from the lowest to the highest denomination by 7 mm each. ■

TWO COMPETITORS TO SUPPLY BANK OF ENGLAND WITH POLYMER FOR NEXT £ 20 NOTE

The Bank of England announced in October, that it has entered into 10-year contracts with both CCL Secure Limited and De La Rue to supply the polymer substrate for the next £20 banknote, to be issued in 2020.

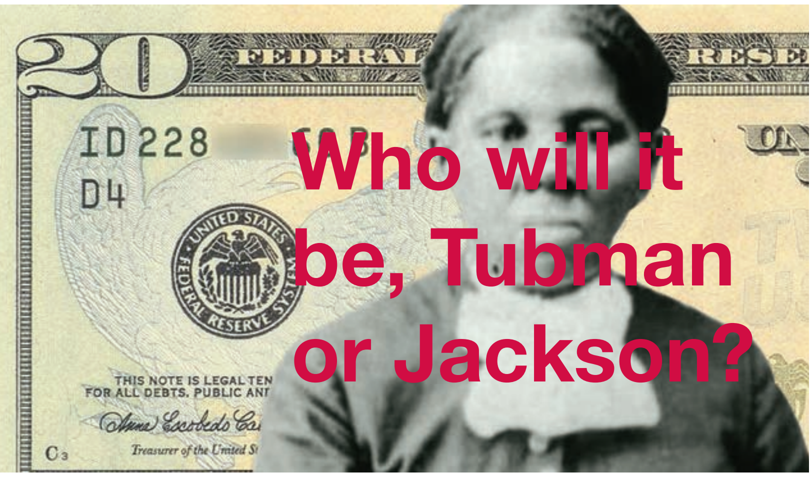
The Bank of England started a formal public procurement process in March 2016 for the supply of polymer substrate for the £20. The final decision to award contracts to two competing companies with production facilities in Great Britain, CCL Secure and De La Rue, was taken by the Court of the Bank of England. Supply of polymer under the new contract will commence in 2018.

CCL Secure, formerly Innovia Group, will supply 75 per cent of the first call-off. The company has been the sole supplier for the polymer substrate for the Bank's current £5 and £10 notes for over four years. CCL Secure's Guardian polymer substrate for the £20 will also be produced in the facilities in Wigton, built specifically to support the Bank of England's new polymer family. The Wigton plant was part of an overall investment programme of over £40 million, which included Innovia Films' new ClarityC production line – the base film used to make Guardian.

Under the terms of the contract, De La Rue will supply the Bank of England its Safeguard polymer substrate for 25% of the first call-off volume. De La Rue added that the company already has the contract to design and print the notes.

De La Rue launched its Safeguard polymer substrate in 2012, and it is now used by 15 issuing authorities across 21 denominations. De La Rue is the only vertically integrated producer of polymer banknotes, which is one of the Group's fastest growing product lines. Production volume of Safeguard nearly quadrupled last year and is expected to double again this year. ■

Who will it be, Tubman or Jackson?


20
FEDERAL
RESE
ID 228
D4
UNITED STATES FEDERAL RESERVE SYSTEM
THIS NOTE IS LEGAL TEN
FOR ALL DEBTS, PUBLIC ANI
Treasurer of the United St
C3

Is it important who is depicted on a banknote? The answer to this question is more political and more fraught with ambiguity than what one would immediately think. Banknotes are used and handled daily by everyone, regardless of gender, ethnicity or religious or political orientation. If they show a face, it has to be accepted by everyone and ideally should refer to a shared admiration or even to a shared ambition. And that makes it difficult.

Real women, with a name and a character - dead or alive - on banknotes are attracting attention, not least for their rarity. In the last issue we wrote about the new £ 10 note issued by the Bank of England, which features the English 18th/19th century writer Jane Austen. She made it onto the banknote because the previous female on a Pound Sterling note - Elisabeth Fry on the £5 - lost her place to Winston Churchill. The ensuing public protest - not only by women - made the Bank of England examine its policy regarding portraits on its banknotes, other than that of the ruling monarch. Since 2014, a Banknote Character Advisory Committee appointed by the Bank of England selects the field that is to be represented and the Bank asks the public to nominate people from the chosen field. In 2015 the Bank announced that someone from the visual arts should be on the next £ 20 note. Over 29 000 nominations came in covering 590 different people. Focus groups and further research lead to a shortlist, of which the Bank's governor made the final selection.

Among countries that put portraits of real people on its banknotes this policy is rather enlightened. The USA has only portraits of rather dour looking presidents or founding fathers on its banknotes, although Benjamin Franklin on the $100 looks a little more jolly, and no female face came anywhere near the front of a recent US Dollar note. That seemed to have changed in 2016.

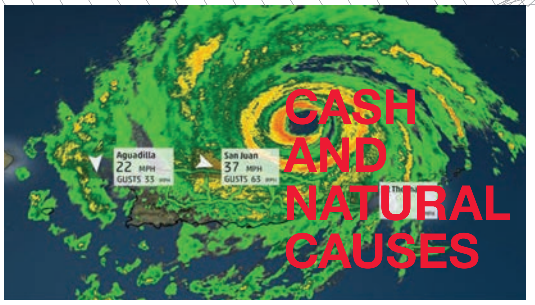
In the June issue 2016 of Infosecura we entitled an article "Tubman's in, Jackson's out", reporting on the decision of then US Treasury Secretary Jacob Lew to place abolitionist and slave liberation fighter Harriet Tubman on the front of the US$ 20 note and move Andrew Jackson to the back. Well, it looks as if our rather triumphalist heading was perhaps premature. We did not take much notice of the remark by, then, Republican presidential candidate Trump, that "I would love to leave Andrew Jackson and see if we can maybe come up with another denomination," after the decision was announced. At the time, Trump mentioned the $2 bill for Tubman, with the smallest volume of any bill, about seven times less than the $20. "I think it would be more appropriate," he said.

It is known that Mr. Trump is an admirer of President Jackson, who was an ardent anti-abolitionist and a slave holder, and who instigated the infamous "Trail of Tears", the removal of native Americans from their homes in the US South-East. Jackson also caused one of the deepest recessions in American history by preventing a new charter for the forerunner of the Federal Reserve and he strongly opposed the use of paper money.

in August 2017, US Treasury Secretary Steven Mnuchin declined to endorse the plan for a 2020 redesign of the $20 bill featuring Harriet Tubman, that was announced by the Obama administration last year. "People have been on the bills for a long period of time," Mr. Mnuchin told CNBC. "This is something we'll consider. Right now we've got a lot more important issues to focus on."

Former Treasury Secretary Lew was aware when he made the decision to redesign the currency that its fate would rest with Mr. Obama's successor. But he said then that he doubted it would be reversed. "I don't think somebody's going to probably want to do that — to take the image of Harriet Tubman off of our money? To take the image of the suffragists off?" he said. He might have been too optimistic. The US Treasury had earlier removed its "Modern Money" website that the Obama administration created to highlight its plans for the redesigned bills. But the end result is still not certain.

The Republic writes that the fight to put Harriet Tubman on the face of the $20 bill by 2020 has been revived with the introduction of bipartisan legislation in the House co-sponsored by Rep. Elijah Cummings, D-Baltimore. On September 20, *Bloomberg* wrote that the Bureau of Engraving and Printing, the agency that prints the US currency notes, hasn't been instructed to take the Harriet Tubman's picture off new $20 note redesign project and is proceeding with the Obama administration's plans. To quote a frequent remark of President Trump: "let's see what happens". ■



CASH AND NATURAL CAUSES

How much people appreciate cash depends on where they live. But even in 'safe' areas, holding on to cash is a very sensible idea.

There are no hurricanes in Sweden and even with a lot of snow, electricity supply is pretty well guaranteed in Norway or Denmark. So, if you live in Scandinavia, it would be extremely unlikely that lack of electricity or Internet access would prevent you from paying with your credit card or smartphone. Not so if you live in Puerto Rico or in any of the other areas around the Caribbean that have been hit by natural disasters or indeed in India.

BLAME THE WEATHER

"Fewer than half of Puerto Rico's bank branches and cash machines are up and running, still crippled by diesel shortages, damaged roads and severed communications lines. Bank officials say they are struggling even to find employees who can get to work when there is no public transportation and gasoline is hard to find," the *New York Times* wrote on September 29th, nine days after Hurricane Maria struck the US Territory of Puerto Rico and leaving all of the island without power. Four weeks after the disaster, on October 20th, the same newspaper wrote that 80 per cent of Puerto Rico still did not have electricity. For many, the main problem was not lack of money but lack of cash.

BLAME POLITICIANS

The very graphic confirmation of the continued need for cash does not always depend on unfortunate natural events. Less dramatically, politics can also play a role. When last year, India's prime minister Narendra Modi suddenly 'demonetized' the 500 and 1000 Rupee notes, making 83 per cent of India's cash worthless, he justified the move by saying that he wanted to flush out untaxed money from the 'black' economy and to rid the country of counterfeits. And he wanted to 'modernize' the Indian economy by setting it on the path to a cashless society and have Indians pay electronically.

That seems to have happened up to a point. Apparently, many Indians had switched to electronic payments, more rapidly than many experts had predicted. The government even ordered banks to add one million card terminals by March 2017, a two-thirds increase from the 1.5 million before that date. But almost one year later, the picture looks more patchy. Hyderabad's *Deccan Chronicle* wrote on October 9th, that the initial enthusiasm for cashless transactions had faded within 10 months due to poor Internet connectivity in semi-urban and rural areas. Another factor is that as cash is again easily available at ATMs and banks, people return to cash. In December 2016, the chief minister of the new federal state of Telangana directed officials to make it the first state in India to become a 'cashless transaction state'. To this end he ordered awareness programmes to be held and the government even launched TS-Wallet, its own mobile application, to enable people to make cashless transactions without service charges. By March, point of sales (POS) machines were installed in all government offices and many retail shops. 380 villages had gone cashless. But the drive lost steam soon after. In the mentioned 380 villages PoS devices were lying unused. "The PoS devices are encountering problems due to poor connectivity. The transactions could not be completed as they are blocked midway. We are facing problems with consumers. We are forced to return to cash transactions," said the secretary of the State Small and Medium Retail Traders Association.

A WARNING FROM EUROPE

The march towards cashlessness finds plenty of critics in Europe as well, even in the general press. Starting again with the example of Sweden, Brett Scott, a campaigner and former broker, writes in the *Guardian* that "in leading the world in cashlessness it also leads the world in opening its citizens up to fine-grained financial surveillance. If financial corporations have complete control over the money system, every economic interaction ends up in their database for analysis." But is this development not driven by consumer demand? True, to a point. People wish to be able to use digital payments but they also wish to retain cash. We like new options, but we don't like having options removed, Scott wrote.

The digital payments industry tries to paint cash as old-fashioned, as the horse-drawn carriage of payments. But cash is more like the bicycle, more flexible, resilient and convenient in certain settings, especially informal ones. It is still very relevant and if people think of the darker side of digital payments, the complete surveillance, massive increase in financial cybercrime and the exclusion of people who cannot access the formal banking system, they will probably try to hold onto cash.

Scott warns that the public is subtly being manipulated into consenting to cashlessness. People may indeed enjoy a new payments app or contactless card, but financial institutions then use that to justify the gradual removal of the cash infrastructure – such as ATMS – in order to deliberately make cash harder to use, which in turn makes using digital payments more convenient, etc. The limits on cash payments above a certain threshold, used in several countries, are another subtle way of making cash look sinister. If you wanted to slowly create a cashless society, thresholds would be the ideal way to incrementally implement it. By gradually lowering the threshold over time, authorities slowly wean people off cash by making it increasingly harder for them to use it. It acts as a ratchet mechanism, pushing them into the arms of the digital payments industry. ■

RISING VOLUME OF CASH AND RISING ELECTRONIC PAYMENTS: A CONUNDRUM

While more and more people use electronic means of payment, the amount of banknotes in circulation is rising. The UK and Australia looked at the figures to try to explain the supposed contradiction.

In a speech in October, Victoria Cleland, the Chief Cashier of the Bank of England, reflected on the supposed contradiction that the amount of banknotes in circulation is rising, while more and more people pay for everyday purchases with cards or with contactless systems or shop online. She said that the use of contactless cards tripled in 2016 and accounted for 7 per cent of payments, while average weekly spending on online shopping in the UK was £1.1 billion in August 2017; an increase of 16 per cent p.a. Does that mean that cash is on the way out?

Looking at Bank of England figures suggests it is not. In 2016 the value of Bank of England notes in circulation increased by 10 per cent, reaching over £70 billion in the run-up to Christmas: the fastest growth in a decade. Cash remains the most widely used payment method in the UK. It accounted for 40 per cent of all payments and 44 per cent of payments made by consumers in 2016. And the UK is not unique in this. In a recent international survey by ING, 79 per cent of people in the UK said they would never go completely cashless, similar to the European average of 76 per cent.

Cash use in the UK is not shrinking: 2.7 million people in the UK rely almost entirely on cash transactions – a number that has increased by 0.5 million since 2015. Apart from a medium of exchange, cash is a store of value and a 2014 survey commissioned for the Bank of England estimated that 18 per cent of people hoard cash, the primary reason being to provide comfort against potential emergencies. In addition there is a strong overseas demand, for example from tourists and expats.

For retailers, cash is still the cheapest payment method to accept. According to the British Retail Consortium, in 2016, the average cash transaction cost a retailer 0.15 per cent of turnover, compared to 0.31 per cent across all payment types. There are many alternatives to cash and with time more people will probably move to them. But the rate of change is uncertain, and depends in part on how effectively the cash industry is able to innovate, to maximise efficiencies, and to keep the cost of cash competitive in an environment of declining transactional volumes, Cleland said. There are some big issues to address: ascertaining the level of demand that would necessitate a significant change in the cash centre footprint; identifying whether there are more innovative approaches to wholesale cash circulation; understanding whether greater cooperation could increase efficiencies in cash distribution; and considering how different the landscape would be if cash demand plummeted but everyone wanted to be able to rely on it in a business continuity scenario. The cash industry should embrace technology to help develop an infrastructure that is flexible and scalable, she urged.

THE AUSTRALIAN EXPERIENCE

In a report published in September, the Reserve Bank of Australia looked at the same conundrum as the BoE. The overall trends are the same as in Britain, although the figures are different.

While survey data indicate that the share of Australian consumers' payments made with cash continues to fall, from around 70 per cent in 2007 to around 37 per cent in 2016, the number (and value) of banknotes in circulation continues to grow at around its trend pace of 6 per cent per year. There are several reasons behind these diverging trends, including: population, inflation and real income growth; a slower decline in total (rather than relative) cash payments; high cash users not captured by survey data; and the increasing stock of banknotes held for non-transactional purposes.

Currently, the total value of banknotes in circulation in Australia is around AUS$ 74 billion, with growth in all denominations, but higher growth in higher denominations. In the long term, the demand for banknotes in Australia is determined by the size of the Australian economy (nominal GDP), the interest rate and access to the payments system (the number of ATMs and bank branches in Australia). The size of the economy is the most important driver of banknote demand, with a 1 per cent increase in nominal GDP associated with a 1 per cent increase in cash demand over the long term. Nominal GDP simultaneously captures the effect of population growth, inflation and real income growth, which suggests that these factors are important drivers of cash demand. In fact, these three factors can explain much of the growth in circulation over the past 10 years, the report states. Cash payments comprise a smaller share of total payments when measured by value rather than by number. This is because cash is more commonly used in low-value payments. The share of cash payments by value has fallen since 2007, but was stable between 2013 and 2016 at around 18 per cent. Importantly, because total payments have increased – due to factors such as population, inflation and income growth – the fall in the total value of cash payments has not been as large as what is suggested by the changing share of cash payments, which declined by more than half.

But measures like this, which come from the Consumer Payments Survey (CPS) do not cover all users of Australian currency. CPS does not cover cash use by businesses, nor is it likely to fully capture the use of cash in the shadow economy (e.g. to avoid reporting income to the authorities or to finance illicit activities). Another important source of cash demand not captured by the CPS comes from overseas. Foreign citizens and institutions may hold Australian banknotes for both transactional and non-transactional purposes and many tourists arriving in Australia carry cash, which for the most part, they exchanged abroad. In 2016 cash expenditure by overseas visitors was estimated to be around $11 billion.

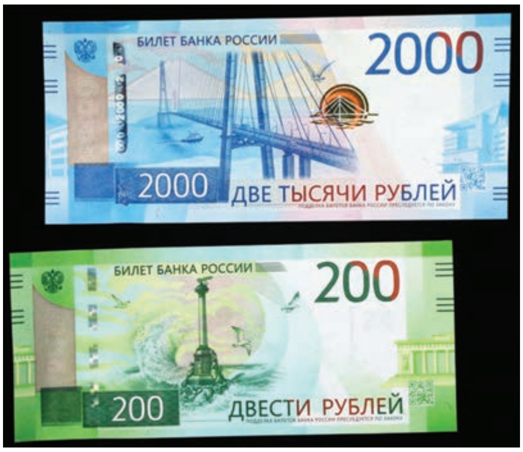
DOMESTIC STORE OF VALUE

In addition to its function as a means of payment, cash is also a store of value, which, although difficult to measure, has to be regarded an important component of cash demand. As part of the CPS, participants were not asked to specify their exact cash holdings. Instead, they selected which range of cash holdings they fall into from a set of pre-specified ranges. While most tend to hold less than $100, around 3 per cent of respondents reported holding amounts greater than $1 000, and 1 per cent hold more than $5 000 (the highest category). These results suggest that a large amount of wealth held in banknotes is concentrated in a relatively small number of households, which is broadly consistent with the distribution of wealth more generally. ■

In the last issue of Infosecura, a technical error in reproduction led to the Ruhlamat ad not being printed correctly. Please note the correct image below.

A RUSSIAN STATEMENT: THE NEW 200 ROUBLE NOTE

Sometimes issuing a new banknote resembles a stage managed show designed to impress the local audience, even if it annoys the neighbours.



In March 2016 we wrote about a new 100 Rouble commemorative note issued by the Central Bank of the Russian Federation (CBR) that was completely dedicated to the Crimean peninsular, which had been 'transferred' to Russia in 2014, following an internationally unrecognized referendum. Since that date, Russia had to endure sanctions and the disapproval of the international community but, defiantly, and judging from the CBR's latest banknote issue, the country sees the Crimea and what it puts on its banknotes as exclusively domestic issues. A new 200 Rouble note (about €3.00), which was presented on October 12, shows the 'memorial to the sunken ships' in Sebastopol on one side and the ruins of the ancient Greek settlement of Chersonesos as well as a map of Crimea on the other. Not surprisingly, Ukraine, to which the Crimean peninsular had been transferred by Nikita Khrushchew in 1954, strongly disagreed with the choice of motif and declared that the banknote would be illegal in Ukraine and banned banks and currency exchanges from accepting it.

At the same time, the CBR presented a new 2000 Rouble note which shows images from the other side of the country, the Far East, with Russkij Bridge – a cable bridge in Vladivostok connecting Russkij Island to the mainland and, on the reverse, "Vostochnij" cosmodrome in the Far East Amur region. The choice of motif for both notes, the CBR subtly pointed out, was not political, but reflected the popular choice, as all landmarks featured on the new notes were selected via a public vote.

Last year, the CBR held a three-stage contest for the selection of images on the new banknotes, somewhat similar to the way the Bank of England selects its banknote portraits. Over 3 million people participated. The first stage invited citizens to propose cities and their symbols, the traditional image on Russian banknotes, via a special website. At the second stage, the Public Opinion Foundation conducted an opinion poll to select the 10 most popular cities out of which the two most popular were chosen. Finally, last October, Rossiya 1 TV broadcasted a show where the audience made the final selection via sms message.

The Russian news agency TASS commented that the new notes looked more like Euros than the traditional Rouble notes. That may be a matter of opinion, but they do have a number of features the Euro has not: one is a QR-code in the right bottom corner, that, when scanned takes one to the CBR's website, where several layers of security features are described. According to the CBR, to increase durability, the new notes are printed on "white cotton paper with increased density and polymer treatment providing high wear-resistance and increased durability, up to one-and-a-half times that of standard cotton notes". Goznak, the printer of the notes, is especially proud of its own-developed security thread, which combines three security features that become visible when tilted, viewed from a certain angle and in transmitted light. Goznak also mentions that machine-readable features have been improved. ■

NEWS

The International Currency Association (ICA) has appointed Guillaume Lepecq as its new Director General. Lepecq has written a number of publications and reports detailing the role of cash in society including: "Cash Essentials - Beyond Payments", "The Future of Cash", "The Future of Smart Payments" and "Managing the Changeover to the Euro". Barna Barabás, Chairman of the ICA, said "Guillaume will play a key part in driving the currency industry's advocacy activities on global key policy issues affecting the industry."

Oberthur Technologies–Morpho becomes IDEMIA

Following the merger of Oberthur Technologies (OT) and Safran Identity & Security (Morpho) on 31 March 2017, the OT-Morpho group has been re-named IDEMIA, Didier Lamouche, Chairman CEO of OT-Morpho announced in late September. IDEMIA has a workforce of 14,000 employees, including 2,000 in the Research and Development department. The company is active in the identification and authentication sector, and serves clients in 180 countries. It provides services to five main customer segments: Financial Institutions, Mobile Operators, Connected Objects, Citizen Identity, and Public Security.

Passenger information and travel security

ICAO's 2017 TRIP Symposium was centred around the theme of "Making Air Travel more Secure and Efficient", reflecting the fact that well-designed security technologies also support the improvement of the passenger experience and the efficiency of facilitation processes more generally.

The main premise of the ICAO's thirteenth Symposium and exhibition on the Traveller Identification Programme (TRIP), held in Montreal in late October, was the centrality of having accurate and timely information on every person that crosses a border by land, air or water. Behind this is of course the fear of terrorism and the problem of illegal immigration. Every one of the five sessions of the three-day event dealt with one aspect of traveller identification. Implementing ePassport validation at border control and national PKD systems, a roadmap for TRIP implementation by member states, supporting improved national identity management practices, how to combat latest trends in fraudulent documents, advances in passenger information, inspection systems and tools in border control, border control management and future travel and finally advance passenger information.

The last subject, advance passenger information or API, is not without legal and political frictions, as it may run up against privacy regulations in some countries. API originated in the USA and was established in 2008 by the US Customs and Border Protection (CBP). In the context of border management and of the increased flow of passengers, especially as seen by the US, one of the key requirements is to ensure security by identifying each individual as soon as possible. ICAO organised a special workshop on this subject, which aimed to provide more information to support countries in establishing national API systems in accordance with the Standards and Recommended Practises (SARPs) in Annex 9 to the Convention on International Civil Aviation. Data capture and transmission, interactive systems to exchange (iAPI) but also internal stakeholders collaboration were especially highlighted in the presentations and discussions. One of the papers given at the workshop illustrated well the scope of the task.

DIGITAL BORDERS: ENHANCING SECURITY IN TRAVEL

Lauren Uppink of the World Economic Forum started her talk with a quote from the founder and chairman of the World Economic Forum, Klaus Schwab, who said that "the changes unleashed by the fourth industrial revolution are so profound that from the perspective of human history, there has never been a time of greater promise or potential peril." She said that the world is experiencing unprecedented change driven by technological shifts. We live in an interconnected system of systems and it is necessary to have dialogue and cooperation across domains and stakeholder groups. The big issues facing us require co-operation and expertise across many different fields. We have to ensure that policy changes contribute to positive outcomes rather than negative ones. The challenges include the widespread geopolitical insecurity, the rising numbers of civilian travellers as well as illegal immigrants and the legacy infrastructure, countries have to cope with. But many of the challenges can also imply opportunities.

Uppink asked, how much does emerging technology impact the global systems governing the movement of people and goods? The Aviation and Travel Industry has been at the forefront of digital disruption, changing the way we travel in recent years. However, the sector should brace itself for another wave of digital transformation, or indeed, disruption. Disruption will be fuelled by the manner in which new technologies build on, combine with and transcend traditional technologies. This new digital transformation will enable change that will scale exponentially to create both benefits and challenges for society. Such technologies specific to travel security include distributed ledger technology, advanced data analytics, biometrics and machine learning. Some of these technologies are already widely used in the industry.

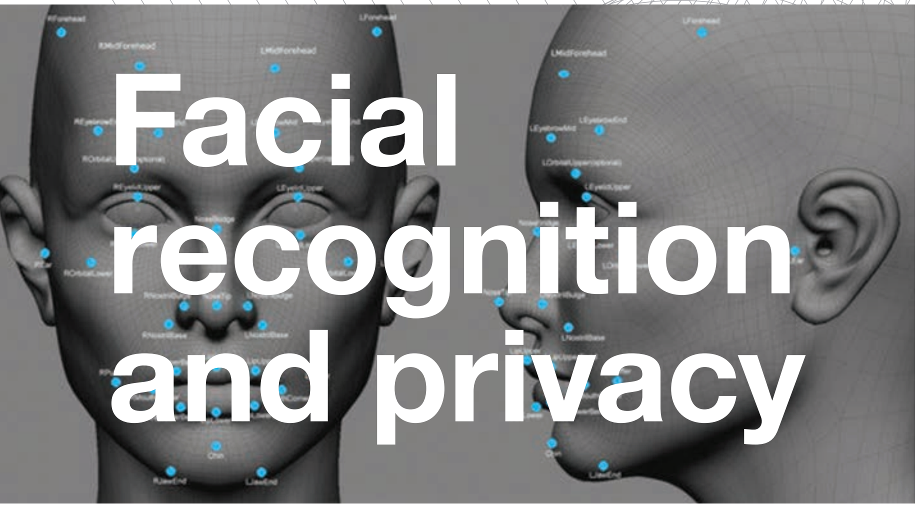
A VOLUNTARY, AUTOMATED TRIP PASS

For Ms. Uppink, the question was, if we can re-imagine the security process for greater collaboration between industry and authorities, with the passenger as a central actor? She described the "traveller journey of the future', whereby a traveller would register in a standardized system for "Known Traveller" profiles with participating governments. This digital profile facilitates booking and verifies eligibility to travel and it aggregates all travel information, passport information and syncs data from each booking interface. Data will be saved for future travel and family profiles can be linked. The traveller then forwards this digital profile to government agencies and the destination for pre-vetting and a smoother experience. Governments can verify eligibility to travel and "known" status. The resulting 'automated TRIP Pass' is a kind of digital 'concierge service' that manages a person's travel, develops the itinerary, remembers preferences, handles in-country service bookings and tracks international purchases (VAT refunds, customs). Use of biometrics will confirm that the traveller is a ticketed passenger and allows passage through security. No lines or removal of items - people are monitored on the way to the gate through frictionless security devices. Travellers are pulled aside if they pose any issue. The rest go ahead to the gate.

Luggage is tracked automatically with the digital profile, allowing for easy drop off and pick up and the check-in is seamless with the verification for travel prepared prior to airport arrival and instant recognition during the journey. To speed-up the customs/immigration procedure at the destination airport, the traveller can forward the digital profile to the in-country security agency. As the TRIP Pass has tracked all purchases the traveller can choose to digitally submit the data to the government for declaration forms.

The described scenario is building on the foundation of existing mechanisms and pilots such as MRTD, PKD, ePassports, API/PNR, Biometric Exit and Entry Systems and OneID and it would allow the passenger to build a "Known Traveller" digital identity. However, if such a system would be made obligatory, it would without doubt come into conflict with privacy regulations in different countries. It is therefore important to stress the voluntary nature of such a scheme: It would follow Digital Identity Principles, such as being secure, portable, traveller-owned and opt-in. It needs to include layered travel and itinerary data (incl. visas, etc.) and additional data to build the "known" profile. Incentives to enrol could include loyalty programmes and expedited processes.

Authorities could use the data provided by the traveller to request data from passengers further in advance, use individualised risk assessment and segment passengers and process known 'risk-free' passengers faster, allowing more attention and resources to focus on less known/higher risk passengers. ■



Facial recognition and privacy

Facial recognition technology is increasingly used for automatic border control and also for other law enforcement purposes. The technology is improving fast but concerns about privacy are mounting almost as fast.

Facial recognition technology got an enormous boost in September, when Apple unveiled its new iPhone X, which, instead of using a password or a fingerprint, simply requires the user to look at it to unlock it. The system is indeed very sophisticated. Instead of using flat-image scans that had allowed earlier laptops and phones like the Samsung Galaxy S8 to be fooled by a mere photograph, the iPhone X projects a grid of 30,000 infrared dots onto a face, and then uses an infrared camera to read the distortion of that grid, creating a three-dimensional model. The iPhone X means that sophisticated facial recognition technology has entered the mainstream. It is of course a fairly narrow implementation of the technology, comparing one stored image taken from a live source with one actual face and delivering a simple pass/fail verdict. The facial recognition systems employed at border crossings have to compare a photograph of varying quality with a face in front of a camera and check the result against any database the authorities require.

Facial recognition is used at an increasing number of airports and border crossings the world over and - on a different level - the iPhone example shows that the technology is developing fast. It is therefore useful to take a look at the subject.

Since 2015 facial recognition (FR) has been used most in Asia Pacific, followed by Europe, with the USA in third place. One of the largest companies offering FR services is Megvii, a Chinese company that started in 2011. Its face recognition technology, called Face++, is used by 300 000 companies and individuals worldwide.

Facial-recognition technology has two aspects: the underlying capability and the applications that make use of it. Megvii's Face++ belongs in the first category, as do similar offerings from SenseTime, another Chinese startup, NTechLab, a Russian firm, as well as Amazon, IBM and Microsoft. These companies provide face recognition as a cloud-computing service. Megvii's customers can upload a batch of photos and names, and use them to train algorithms, which then can recognise those particular people. Firms can also integrate the recognition service into their own offerings, for instance to control access to online accounts or to border crossings or airport gates, the *Economist* writes. The Chinese companies have the advantage that they have access to the Chinese government's image database of 700m citizens, who are each given a photo ID by the age of 16. Chinese government agencies are also valuable customers—more and more of the country's hundreds of millions of surveillance cameras will soon recognise faces.

In China and also in other countries, commercial applications, often using one of the cloud services, are growing fast. In several Chinese banks, ATM users can log in using their faces. The west is further behind. There are many plans and some industries are already using FR, such as casinos that want to turn away gamblers they don't trust, and it is used by border control in several countries, but the numbers are far below those in China. As more and more ABC or Smart-Gates appear at airports, numbers will rise.

The technology is already impressive and it is improving fast but it is not without its problems and many of these are linked to privacy.

WHO OWNS YOUR FACIAL IMAGE?

Unlike fingerprints or DNA, facial images can be taken without the consent of the owners. FindFace, an app in Russia, compares snaps of strangers with pictures on VKontakte, a social network, and can identify people with a 70 per cent accuracy rate. Social media such as Facebook, has huge banks of facial images linked to names and theoretically, advertisers could use images taken of visitors to a showroom to have Facebook send them ads for the products displayed there.

Of greater importance are images held by authorities. Paul Wiles, the UK biometrics commissioner, says in his annual report 2016 that the police's use of facial images has gone far beyond their original use for custody purposes and forces are using facial recognition software to try to identify individuals in public places, the *Guardian* writes.

As of July 2016 there were 19m facial images on the

UK police national database, of which 16.6m had been enrolled in a facial image recognition gallery and were searchable using recognition software. According to a UK high court ruling, the police may not retain images of innocent people they had arrested or questioned but who had never been charged or convicted of any offence. However, a Home Office review requires the police to delete images only on application from an individual "unconvicted person".

THE CASE FOR THE OPPOSITION

All of this applies to people who were not asked to submit their image. But what about facial recognition at borders or airports, were people submit voluntarily to have their image used for identification? It might be useful to hear what the most ardent privacy defenders have to say, the American Civil Liberties Union (ACLU).

Jay Stanley, Senior Policy Analyst at ACLU said that US Customs and Border Protection (CBP) has launched a "Traveller Verification Service" (TVS) that envisions applying face recognition to all airline passengers, including US citizens, boarding flights exiting the United States. This system raises very serious privacy issues. Currently being operated in six large airports around the country, the TVS program is part of a larger program called "Biometric Entry/Exit." That program is the attempt by the Department of Homeland Security (DHS) to comply with a congressional requirement that the agency use biometrics to keep track of visitors entering and exiting the United States, in order to identify individuals who overstay their visas.

ACLU said that DHS has chosen face recognition for TVS and calls this the most dangerous biometric because it has greater potential for expansion and misuse. Face recognition databases could be plugged in to every surveillance camera in America, creating a giant infrastructure for government tracking and control. The ACLU also is also against airlines supporting the use of FR. The airlines' participation is significant because without it, the plan could not go forward, or at a minimum, its implementation would be significantly hampered.

Given their role, the airlines have a responsibility to ensure that customers' rights are respected, yet they have not taken even some basic steps to fulfill this obligation. Until they have taken these steps—and received assurances from CBP that the agency will abide by certain privacy standards — they should not participate in these programs ACLU argues.

In August, according to a DHS briefing, the agency was still working out which tasks will be performed by the airlines—including whether the government or the airlines will own and operate the face matching cameras. DHS also says the airlines do not keep copies of the photos for their own use, but that there's nothing stopping them if they decide to start doing so. Publicly, the US airlines have largely framed their participation as an efficiency investment, with little mention of the programme's role in CBP's larger biometric tracking vision.

ACLU demands that before further participating in the programme, airlines should provide transparency to their customers and demand that DHS do the same. Airlines should also demand that any data collected be purged in a timely fashion and not used for other purposes. Any passenger should be able to opt out of the programme and DHS should provide assurances that customers' rights will be protected. ■

ESTONIA BLOCKS CERTIFICATES ON 760,000 ID CARDS DUE TO IDENTITY THEFT RISK

On 3 November 2017, Estonia blocked the certificates of 760,000 ID cards because of the discovery of a security vulnerability in the Infineon-developed RSA library, which could be exploited by attackers to discover the RSA private key corresponding to an RSA public key generated by this library.

Estonian electronic ID cards have been manufactured by the Swiss company Trüb AG and its successor Gemalto AG since 2001. The flaw is present in the cryptographic chips included in Estonian ID cards issued after 16 October 2014.

"The functioning of an e-state is based on trust and the state cannot afford identity theft happening to the owner of an Estonian ID card. As far as we know, there has been no e-identity theft, but the threat assessment of the Police and Border Guard Board and the Information System Authority indicates that this threat has become real," Prime Minister Jüri Ratas said. "By blocking the certificates of the ID cards at risk, the state is ensuring the safety of the ID card."

The security threat is heightened because it was not a flaw of the Estonian ID card alone, but also of cards and computer systems around the world that use the chips by the same producer. This brought the safety flaw to the attention of international cybercrime networks.

"Our first priority is the protection of people's health data, which is why blocking the certificates is the only conceivable option. Over the past two months, a lot of work has been done to ensure the functioning of health and social services even in the case of the closure of the ID certificates. However, some disruptions may occur in hospitals in the coming weeks, which is why we ask for understanding from patients – this step will protect your data," said Jevgeni Ossinovski, Estonian Minister for Health and Labour. (source: Helpnetsecurity) ■

DOCUMENT FRAUD AND MIGRANT SMUGGLING

Driven from their homelands by insecurity, instability, and poverty, the influx of migrants into the European Union over recent years has reached "unparalleled levels." These circumstances have resulted in a serious humanitarian crisis but also given rise to various opportunities for transnational criminal networks.

Countries the world over are worried about illegal immigration. It is a huge and complex problem and in many cases it is linked to counterfeit documents. But document fraud is not only connected to immigration, it is also seen as an enabler for other criminal activities, including terrorism. The European Union is trying to come to grips with the problem. This year, the Council of the EU defined ten priorities for fighting organised and serious international crime between 2018 and 2021. One of these priorities is combatting document fraud and targeting the organised crime groups involved in producing and providing fraudulent and false documents.

As part of this task, two EU agencies, the European police organisation Europol and Frontex, the EU Border and Coast Guard Agency, arranged a meeting of their document experts to find a common way to meet this danger. In introducing the task, Europol's Executive Director Rob Wainwright said: "In the last few years document fraud has become a major criminal problem in Europe, helping to drive new shifts in the scale and impact of migrant smuggling, fraud, terrorism and other security threats. Professional criminal syndicates are now part of the large-scale production, trading and distribution of often high-quality identity and other official documents. Europol is pleased to support this new initiative between the Member States of the EU and other partners to crack down on this problem."

Fabrice Leggeri, the head of the other agency involved, Frontex, added: "Document fraud at the European Union's external borders can ultimately undermine its internal security. Frontex will do its utmost to support the Council initiative, also by providing the expertise gained in our operations. Right now, we have 74 specialised document experts deployed at Europe's borders."

The EU crime priority will be implemented through a common strategic goal in all relevant operational plans covering other criminal areas. This should make it possible to tackle the phenomenon in a comprehensive way by police, border and coast guard, and customs experts.

To streamline their work, the EU Council decided to create the Horizontal Expert Working Group on Document Fraud. The working group comprising Member States, Frontex and Europol experts, will provide support in fighting all types of document fraud, including travel and identity documents, 'breeder' documents (serving as a basis to obtain identification documents fraudulently), other types of ID fraud, administrative and official documents of any kind that are subject to fraud by organised crime groups. The first meeting of the group, led by France and supported by Europol and Frontex was held at Europol's headquarters in The Hague in September.

EUROPOL-INTERPOL REPORT ON MIGRANT SMUGGLING

The fight against document fraud is not new. Last year Interpol and Europol issued a joint report on migrant smuggling networks, which tried to provide some accurate and in-depth understanding of the wide range of illicit services offered by migrant smugglers, and their operating methods.

The report found that over 90 per cent of migrants coming to the EU are helped, or 'facilitated', mostly by members of a criminal network. The more difficult the countries along the migratory routes make entry, the higher the percentage of 'facilitated' entries rises. Facilitators are organised in loosely connected networks, stretched along the migratory routes. More than 250 hotspots for migrant smuggling have been identified in and outside the EU.

Migrant smuggling is a multi-national business, with suspects originating from more than 100 countries both inside and outside of the EU. The basic structure of networks includes leaders who loosely coordinate activities along a given route, organisers who manage activities locally through personal contacts, and opportunistic low-level facilitators. Migrant smuggling is a highly profitable business, with relatively low overall costs to run smuggling operations and persistently high demand for services. An estimate of the yearly turnover of migrant smuggling results in an average US$ 5 to 6 billion turnover in 2015. The main means of payment remains cash.

Intelligence collected in recent months suggests that polycriminality linked to migrant smuggling is increasing: suspects in migrant smuggling cases have previously been recorded in relation to other types of serious crime. Migrants who travel to the EU are potentially vulnerable to be targeted for labour or sexual exploitation as they need to repay their debt to smugglers. It is expected that these types of exploitation will increase in the coming years. Terrorists may also use migrant smugglers' resources to achieve their goals and reach their targets. There is an increased risk that foreign terrorist fighters may use the migratory flows to (re) enter the EU. ■

Security and Design in Perfect Harmony

The challenge of designing a new banknote series today is to comprehensively meet the requirements of all citizens as well as those of diverse commercial participants in the cash cycle. varifeye® ColourChange combines impressive functionality with appealing design that is clearly and instantly recognizable.

These days, banknotes must be as visually appealing as they are secure and functional, and fit smoothly into the cash cycle. The harmonization of several security features, based on different production steps like print, foil, and paper, enhances fast and unambiguous authentication by the user. With varifeye ColourChange, G+D Currency Technology has developed a very complex high-tech security feature that also relies on intuitive perception.

"With varifeye ColourChange, the interaction between the window in the substrate and the foil creates dynamic and colorful images, making the banknote truly eye-catching," claims Dr. Alfred Kraxenberger, Managing Director of R and D, Technology, and Operations at their Louisenthal subsidiary.

The banknote´s front is enhanced by foil with micro-mirror technology, colors and movement effects. On the back, a finely lasered window provides an additional motif. "If a person holds the banknote up to the light, the translucent window appears shimmery blue in the foil motif. This transforms the LaserCut and high-tech foil into a secure window, which is very easy to authenticate". The effects are visible even in poor light conditions.

Unlike most other foil elements, varifeye ColourChange is suitable for the integration of additional high-tech design elements on the foil. For security printers, the feature offers four key advantages:

DESIGN FREEDOM: Many security features can be used to supplement the design diversity of varifeye ColourChange.

PROVEN COMPATIBILITY: The feature can be integrated into all production processes and substrates.

PRINT EFFICIENCY: Sheet pile stability and processability have been proven.

SECURITY EFFICIENCY: Registered application ensures uniform positioning of the feature on the banknote, thus allowing recognition of the full feature area from the bottom to the top and even on the reverse side of the banknote.

> »The design beautifully supports the security elements.«

G+D Currency Technology is a proven global supplier that covers the entire banknote value chain. "We continuously see and understand what is required at each individual phase of the process, and anticipate emerging and future needs, which means we can continually improve the cash cycle," adds Kraxenberger. ■

varifeye® ColourChange offers:

- Attractive and easily recognizable effects
- Window translucency enables color change
- Customized window shapes for special design effects
- Design integration front to back
- Brilliant dynamics
- Excellent counterfeit resistance
- Striking color effects
- Double-impact image source front and back

For further information, details, and contact, please visit:

gi-de.com/ct

BORDER CONTROL
THE OFFICER'S BEST FRIEND
VIS • IR • UV
SINCE 1985
KINEGRAM
Two eyes are better than one