February 2018

POLICY INSIGHTS

Exposing Idemia

The Push for National Biometric IDs in America

Written by Twila Brase
and Matt Flanders*

Key Points:

- Collection of biometric data from Americans (e.g. fingerprints; facial scans) is facilitated by Idemia.
- Idemia produces state driver's licenses and IDs for 42 states, and is prepared to create REAL IDs.
- REAL ID cards are required for any federally-defined "official purpose," which could eventually include patient access to medical treatment ('no card, no care').
- Biometric IDs are being advanced for everyday transactions.
- Idemia equipment has been used by federal agencies to pilot facial recognition on cruise ships and at American airports.
- Federal legislation requiring all workers in the U.S. to have a National Biometric ID was proposed in January 2018.

Risks to privacy and security rise every year. The advance of globalization and the growth of information technology across most sectors of the economy, including health care, have exposed individuals, governments and corporations to hacking, ransomware, data-mining, data breaches and more.

Serious questions emerge in this era of rapid technological advancement. Can government infringe on personal privacy rights by claiming safety and security purposes? Can government claim 'the common good' outweighs the individual's constitutional guarantee of freedom?

With these questions in mind, how should Americans respond to the growth of biometric identification mandates such as the facial-scan biometric requirement in REAL ID, the nation's new 'de facto' national identification system?

Benjamin Franklin, understanding this tension, prioritized freedom:

> Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.[1]

161 St. Anthony Ave, Ste 923
St. Paul, MN 55103
www.cchfreedom.org

CITIZENS' COUNCIL FOR Health Freedom
SECURING HEALTH FREEDOM FOR ALL

Safety and security must be viewed through the American lens of individual freedom, including privacy rights.

Although Mr. Franklin could not have foreseen our technological world, including computers, the Internet, smartphones, and electronic health records, his sentiment still rings true. Safety and security must be viewed through the American lens of individual freedom, including privacy rights. Unlike other countries that have imposed national ID systems, Congress and the federal government are limited by protective provisions in the Constitution of the United States. The danger of biometric identification schemes is summarized concisely in an Electronic Frontier Foundation publication called "Mandatory National IDs and Biometric Databases:"

> National ID cards and the databases behind them comprise the cornerstone of government surveillance systems that creates risks to privacy and anonymity. The requirement to produce identity cards on demand habituates citizens into participating in their own surveillance and social control.[2]

Freedom lost is not easily regained. The authors of the U.S. Constitution and its Bill of Rights understood the importance of privacy to freedom and security. The Fourth Amendment enshrines personal security by protecting privacy: "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." The loss of the individual right to be free would be the greatest insecurity of all.

Idemia, the focus of this report, is not a household name, despite its reach into the private and commercial affairs of most Americans. The company's advance of biometric data strategies, databases and scanning devices for access and entry control—"augmented identification"—are also likely unknown. However, this global company is acquainted with most American citizens, whose private information flows through its equipment, databases, and software products. That said, it is unclear whether Idemia actually stores this data long-term. One news article on TSA PreCheck, the program that speeds clearance at airport security, says the data and fingerprints of program applicants are not stored by Idemia. The company simply collects them for the program and sends them to the FBI, which destroys them or sends them back.[3]

This report seeks to acquaint Americans and their elected representatives with Idemia and biometric ID cards—and draw attention to our organization's concern that current or future augmented identification requirements could negatively impact individual freedom and patient access to medical services.

In addition, as we often say, "He who holds the data makes the rules." Third parties that collect, store or have the power to access personal data on Americans without their consent also have the power to use that data to interfere in the personal lives and private choices of individuals. This report will add weight to that reality.

INTRODUCING IDEMIA & BIOMETRICS

Imagine sitting at a bank applying for a credit card and waving your hand through a scanner, allowing the bank to capture a biometric scan. Or imagine being required to scan your fingerprint to use that card for payment. Picture your identification documents being stored on your mobile or digital devices and being unlocked with a biometric face scan, similar to how Face ID, Apple's new technology, unlocks iPhones.[4] Visualize walking through an airport and having scanners capture your facial, iris, and fingerprint biometrics as you go through each phase of security or reach your gate. Pick out a rental car online and imagine using your biometric ID to unlock and operate the car instead of a key.

Idemia, which calls itself "the global leader in trusted identities," has imagined it already. These augmented identification systems using individual biometrics for entry, access and commercial transactions are portrayed in a video found on Idemia's website, and available on YouTube.[5] The company considers itself "the world number one" in the biometric algorithm and sensor technology market.[6]

What is biometrics? According to Idemia's website, biometry means "measurement of life." Biometrics "refers to all processes used to recognize, authenticate and identify persons based on physical or behavioral characteristics." Idemia lists five attributes of these characteristics: "Universal + Unique + Invariable + Recordable + Measurable." Biometric types include: biological (e.g. DNA), morphological (e.g. fingerprints) and behavioral (e.g. keyboard strokes).[7]

A majority of Americans, including their lawmakers, have probably never heard of Idemia—unless they've enrolled in TSA PreCheck and read the fine print, which until recently said "MorphoTrust" (now called Idemia).

CCHF discovered Idemia as we tried to derail REAL ID in our home state of Minnesota. As a national organization focused on protecting freedom for patients and doctors, CCHF recognizes REAL ID as a national ID system, which will likely lead to a national patient ID that could limit access to medical care ('no card, no care').

CCHF's discovery came in the form of a photo sent by a concerned citizen. The photo included a larger envelope with the return address of MorphoTrust, a company located in Massachusetts. Inside the envelope, according to the photo, was a smaller envelope with Minnesota Driver and Vehicle Services listed as the return address. And inside that envelope, according to the sender, was a Minnesota driver's license. The sender asked why a Minnesota state driver's license had been sent by a company in Massachusetts and who and what is MorphoTrust. In the time it has taken to figure that out, MorphoTrust became Idemia.

Idemia's history is complex. There have been many corporate mergers, transitions and name changes over the past few years,[8] however the short answer to the origin of Idemia is that it's the new name of a company formerly known as Morpho-OT, which was formed by the merger of two major European technology and biometric companies: Oberthur Technologies (OT) and Safran Identity and Security (Morpho), the parent company of MorphoTrust USA and a former subsidiary of Safran, a French company.[9] On May 31, 2017, these two companies were merged by their new owners (U.S. private equity firm Advent International and the French government investment bank Bpifrance) to create OT-Morpho[10]—which on September 28, 2017 changed its name to Idemia.[11]

GLOBAL REACH

Idemia collects personally identifiable data and provides identification strategies

Biometrics refers to all processes used to recognize, authenticate and identify persons based on physical or behavioral characteristics.

for border management, law enforcement, aviation, retail, banking and more.[12] It serves clients in 180 countries in the areas of financial institutions, mobile operators, connected objects (the Internet of Things),[13] citizen identity, and public security.[14] Its RapidHIT system is capable of producing DNA profiles "in any environment, including in the field" in a fraction of the time required by forensic laboratories—two hours instead of up to six months.[15]

Augmented Identity uses the biometric characteristics of each person as a unique signature of individual identity, thus facilitating exchanges.

American clients include individual state governments,[16] the U.S. Department of Defense (DoD)[17], the U.S. Department of State,[18] the U.S. Department of Homeland Security (including U.S. Customs and Border Protection),[19] and the Federal Bureau of Investigation (FBI).[20] In 2013, Robert Eckel, then CEO of MorphoTrust and now regional president following Advent International's acquisition of Morpho, said his company considered itself "a trusted partner to DoD and other government agencies."[21]

At a 2015 Association of American Motor Vehicle Administrators (**AAMVA**) conference, speakers from the U.S. Department of Homeland Security (DHS), the Vermont Department of Motor Vehicles (DMV) and MorphoTrust came together to support REAL ID. Their slides include a graphic demostrating data moving between a smartphone, the cloud and a locked file. Privacy was equated with security. For example: "care and management of PII is core to ensuring privacy can be assured."[22]

Didier Lamouche, CEO of Idemia, says as a result of its work, citizens can exchange, connect, pay, travel and vote in confidence:

> The accomplishment of this promise is what we call Augmented Identity. It is about using the biometric characteristics of each person as a unique signature of individual identity, thus facilitating exchanges. It fosters confidentiality and trust and guarantees secure, authenticated and verifiable transactions. This is a decisive step towards a more frictionless, safer world.[23]

However, as **WikiLeaks founder Julian Assange** told *Fox News*, "Everything is almost completely insecure now. Computer systems have become so complex that it is not possible to understand all the parts, let alone secure them. It's just impossible."[24]

Hundreds of millions of Americans had their information stolen when Equifax, Target, Anthem, Yahoo and the U.S. Office of Personnel Management, to name a few, were hacked.[25] As Americans have discovered, centralized data collections, particularly in digitized and online-accessible forms, threaten privacy and present serious risks to personal, corporate and national security.

Driver's licenses (DLs) and identification cards (IDs) in 42 states, as well as 100 percent of American passports, are created by Idemia.[26] Therefore, the majority of people with DLs and IDs in the U.S.—80 percent according to Idemia—have their personal information, which increasingly includes biometric data, sent to this corporation, likely without their knowledge.

No single comprehensive federal law restricts the collection or use of biometric data in the United States.[27] However, several states—Illinois, Texas and Washington—have passed state laws requiring individual consent for the storage and collection of biometric data. Colorado is also considering legislation to protect "personal information," which would include medical and biometric data.[28] Only Illinois gives a private right of action, allowing individuals to sue.[29]

DIGITAL DRIVER'S LICENSE

The next step, according to Idemia, involves transitioning state driver's licenses and IDs to the digital realm—to a cell phone, which would enable remote access and control.

In June 2016, Iowa completed the first phase of a digital driver's license (DDL)—also known as a mobile driver's license (mDL). Idemia describes the Iowa project on its website and states that officials will be able to "make real-time updates to the mDL without needing to enter an office." More troubling, they can suspend or revoke a license at any time.[30]

Six states—Iowa, Colorado, Idaho, Maryland, Washington, D.C. and Wyoming—will begin DDL trials in 2018.[31] Other states such as Illinois,[32] California,[33] Louisiana,[34] and New Jersey[35] are also considering DDLs. Iowa has already completed at least one DDL trial with technology developed by Idemia and will make DDLs available to the public as early as the middle of 2018.[36] The DDL, as reported by *PhillyVoice,* would allow police officers to "**wirelessly pull up a driver's identification without having to leave their patrol cars**."[37] Will it allow identification of the passengers as well? The publication notes that Iowa will try using DDLs to collect other data on drivers, such as alcohol and tobacco purchases.[38]

As cybersecurity expert Minnesota state Rep. Eric Lucero (R-Dayton) discussed during a CCHF public forum, applications housed on cell phones are designed to collect data from the phone owner. Location, phone usage, searches, and more provide a rich data set for application ('app') developers to collect, mine and sell.[39] A state DDL app could possibly give similar access to personal data, allowing unwanted government intrusion and tracking in American lives.

DIGITAL IDS OVERSEAS

The movement toward 'all things digital' outside of the United States provides additional insights. In Great Britain, a DDL prototype is already in place with release of a digital license expected in 2018. In addition, the British are currently working on a **"paperless passport,"** which means, "soon enough, all your identification cards could be stored on your smartphone," reports *BetaNews*.[40]

In Saudi Arabia, biometrics are required to buy a mobile phone, attend a university, secure a visa, and testify in court. [41]

In the United Arab Emirates (UAE), Idemia is testing technology that allows a moving law enforcement vehicle to automatically scan the biometrics of other drivers as well as pedestrians.[42] In addition, the UAE has incorporated Idemia's "Iris At a Distance" technology that allows scanners to read both facial and iris biometrics to identify passengers from more than a meter away.[43]

By the end of 2017, Idemia had issued over **3 billion identification documents** across the world.[44] It has used biometrics to "secure" identities in countries like Chile, India, Brazil, Mali, and Kenya—to name a few.[45] In Albania, multiple levels of biometrics are used to verify identity.[46] In Paraguay, Idemia supplied the iris scanners to assist in the collection of information

Six states —Iowa, Colorado, Idaho, Maryland, D.C. and Wyoming —will begin DDL trials in 2018.

Personal information is a rich target for hackers who wish to exploit the monetary value of such data.

for the national ID.[47] In India, Idemia boasts that it has collected over **one billion biometric identities** (17% of the world population) for the national identification project called Aadhaar.[48] As Idemia writes on its website:

> The Aadhaar program assigns a unique 12-digit identification number, called Aadhaar number, to all residents of India, based on the secure registration of their biometric data: fingerprints, iris and facial recognition. Aadhaar enables all residents to access their fundamental right of being recognized by the Indian government, giving them access to numerous services: **social benefits, medical care, opening a bank account**, etc.[49] [Emphasis added.]

In early 2018, a journalist revealed a breach in the Aadhaar program. Rachna Khaira, a reporter at *The Tribune*, was able to pay an unknown person 500 rupes ($8) for access to personal information in the Aadhaar database including names, addresses, photos, phone numbers, and email addresses. For 300 additional rupes, she was able to print out new Aadhaar cards by entering a unique Aadhaar number.[50] Although biometric information was not exposed in this case, personal information remains a rich target for hackers who wish to exploit the monetary value of such data.

Aadhaar has been challenged thirty times in India's courts, according to *The Wire*.[51] During a January 24, 2018 hearing, the Supreme Court of India said it is necessary to "strike a balance between a citizen's right to privacy and state interest," reported *Times of India*. It also said government and private companies can't use the private data to track people in the private domain, but the data can be used for national (public) interests, in particular stopping terrorism and money laundering. An opponent of Aadhaar, Shyam Divan, argued in court that the government should be protecting citizens' fundamental right to privacy and that Aadhaar, "continues to violate the right to privacy by requiring individuals to part with demographic as well as biometric information to private enrolling agencies."[52]

BIOMETRIC SURVEILLANCE 24/7

In China, Idemia is expanding the use of biometrics for border security, public safety, banking and mobile purchasing—in addition to providing biometric identification systems to the Chinese police and government.[53] In 2015, the Chinese Ministry of Public Security called for a nationwide video-surveillance network that is **"omnipresent, completely connected, always on and fully controllable."**[54]

Facial recognition is being employed in China to use an ATM, order food at a restaurant, enter/exit work, and even to limit toilet-paper use and theft.[55] It's also a tool of surveillance used to catch jaywalkers. IHS Markit Ltd. says China is the "largest video surveillance market in the world."[56] It's expected to have roughly 570 million surveillance cameras by 2020, reports *TechCrunch*. Demonstrating the power of its technology in a test for BBC News, China's CCTV surveillance system helped police track down and 'capture' BBC reporter John Sudworth in only seven minutes.[57]

DIGITAL DATABASES

In the field of biometrics, few corporations rival Idemia.[58] Its technology is purchased and used across the globe. Idemia contracts with the U.S. Department of Defense (DoD) to provide **Automated Biometric**

Identification System (ABIS) software, which supports "the DoD's mission of identifying and providing intelligence on persons of interest who could potentially pose a threat to national security or those engaged in warfighting missions."[59] To verify identities, it uses an "identity search engine" to register and compare biometric features against data on file. By 2018, Idemia plans to bring ABIS into the cloud with a product called Identix.[60]

Using Idemia's handheld devices and software, the U.S. Army collects fingerprint, iris, and facial scans across the world, creates a unique data file, and transmits the data to a DoD storage facility in West Virginia. These biometric files are shared between various agencies and used to set up watch-lists.[61]

The FBI has worked with Morpho (now Idemia) since 1974 when its subsidiary MorphoTrak (then known as Rockwell Autonetics) developed the first **Automated Fingerprint Identification System (AFIS)**.[62] Idemia also works with the FBI as a third-party approved Channeler for Americans to get their rap sheet[63] – essentially a self-initiated background check. Individuals enter an Idemia location and submit data, including fingerprints, which are digitized and sent to the FBI.[64] Idemia also provides ABIS software for the FBI's biometric facial and iris scan database called **Next Generation Identification (NGI)**.[65] It was created and is maintained by Idemia.[66] With over 244 million non-criminal (civic) and criminal records, NGI includes a FBI **Universal Control Number** for each person registered in the database. [67]

LAWSUIT FILED

In December of 2017, Pulitzer Prize reporter Chris Hamby broke a story of two former employees of Morpho: Philippe Desbois (former CEO of Morpho's operations in Russia) and Georges Hala (former Morpho business development team member in Russia). These former insiders claimed that when Morpho created the software for the FBI's fingerprint analysis portion of NGI, it secretly inserted code provided by Papillon AO—a Russian firm with known connections to the Kremlin. These men allege that Morpho purposely hid this fact from the FBI in order to win the U.S. contract for the software.[68]

As proof, the men provided an unsigned copy of the licensing agreement between Safran's subsidiary company Sagem Sécurité (now Morpho) and Papillon that allowed Morpho to "incorporate the Papillon code into the French company's software and to sell the finished product as its own technology," *BuzzFeed* reported.[69]

Desbois, who has filed a whistleblower lawsuit in U.S. federal court, accuses Safran of fraudulent collections and alleges that he was told to keep the deal secret to prevent jeopardizing U.S. contracts: "They told me, 'We will have big problems if the FBI is aware about the origin of the algorithm.'"[70]

U.S. Congressman John Kline, a former Republican member of the U.S. House Intelligence Committee, was worried about foreign influence in 2009 when the FBI was evaluating companies that specialize in fingerprint software. In a letter to then-FBI director Robert Mueller, he wrote, "Allowing a foreign government to provide services regarding sensitive information to our law enforcement and intelligence communities could potentially pose a grave counterintelligence threat to the U.S. government."[71]

Idemia also works with the FBI as a third-party approved Channeler for Americans to get their rap sheet.

Safran denies any legal responsibility for the use of the Russian code in FBI fingerprint software—because it was designed by the subsidiary company (Morpho) that it recently sold. The case is on appeal.[72]

Idemia claims it is number one in civil identity solutions with over three billion IDs in over 135 citizen ID programs.

FACES AND FINGERPRINTS

Facial recognition scanning, similar to the kind found in the 2002 American movie, **Minority Report**, is getting easier. In late 2017, the U.S. Customs and Border Protection (CBP) agency "utilized IDEMIA's facial capture and recognition solution" to identify passengers on **Royal Caribbean Cruises.**"[73] CBP had received all-in-one biometric identification kits in the spring of 2016.[74] Passengers disembarking in New Jersey "had their faces scanned by Idemia's hardware. Their faces were immediately matched to biometric information collected when they boarded the ship, confirming their identities," reports Find Biometrics, a global identity management company.[75] In the summer of 2017, CBP began employing facial recognition scanning in airports, starting with Chicago O'Hare and McCarren International Airport in Las Vegas.[76]

Idemia also contracts with a number of states in the U.S. For example, it provides fingerprinting services for those applying for jobs or licenses in New York and West Virginia.[77] In 2015, Georgia and North Carolina reached a deal with Idemia to develop "High-Trust Electronic ID for Tax Collection Agencies."[78]

REACHING INTO AMERICA

Idemia's website reports 3 billion euro in revenue, more than 14,000 employees in over 55 countries, and branches across 5 continents.[79] The company's largest business unit, located in Massachusetts, has over 3,200 employees and $1.2 billion in annual revenues.[80] Idemia's brochure claims it is number one in civil identity solutions because it issues over three billion IDs in over 135 different citizen identification programs.[81]

How did this global corporation, formerly owned by a French company, secure major contracts with state and federal government agencies in the United States for the identification of Americans?

In 2011, Safran Inc., a military contractor based in Paris, France and partially owned (15 percent) by the French government,[82] acquired the **American company L-1 Identity Solutions**—a $1 billion acquisition—and L-1 became MorphoTrust USA.[83]

At the time of purchase, L-1 Identity Solutions boasted a staff of 1,000 specialists with **93 percent holding high-level government security clearances**. In addition, former Central Intelligence Agency (CIA) chief, George Tenet, was a board member. [84]

In 2007, Tim Shorrock, the author of a book on intelligence outsourcing, wrote in *Salon*:

> Tenet sits on the board of directors of L-1 Identity Solutions, a major supplier of biometric identification software used by the U.S. to monitor terrorists and insurgents in Iraq and Afghanistan. The company recently acquired two of the CIA's hottest contractors for its growing intelligence outsourcing business.[85]

Today, Idemia is using algorithms to process and match finger and palm prints to meet "the public safety needs of more than

18,000 local, state, tribal, and federal law enforcement agencies nationwide."[86]

DIGITAL REAL ID?

Idemia will likely find its work enhanced by the REAL ID Act. In 2005, without a single Senate hearing, the U.S. Senate passed the REAL ID Act in the middle of the night using an amendment to a defense and tsunami relief bill.[87] The law, signed by President George W. Bush, gives the U.S. Department of Homeland Security (DHS) sweeping control over identification documents nationwide, including state driver's licenses and identification cards[88]—but only if States submit to federal control.

In the early years, state legislatures refused, many passing state laws that prohibited compliance with the federal REAL ID Act.[89] Congress' attempt to commandeer the states was a direct violation of individual and state Tenth Amendment rights under the U.S. Constitution. Organizations and policymakers from both sides of the political aisle also expressed concerns about the impact of REAL ID on individual privacy and personal autonomy.

As **U.S. Senator Lamar Alexander** (R-TN) said on the floor of the U.S. Senate in 2005:

> This really is a national identification card for the United States of America for the first time in our history. We've never done this before and we shouldn't be doing it without a full debate.[90]

Many compliance deadlines came and went with a majority of states refusing to submit to the federal government.[91] This changed dramatically after DHS began issuing public threats in 2016 saying people without REAL ID would not be able to fly using their state driver's license or ID card.[92] One by one, states began submitting to REAL ID and its federalized driver's licenses and ID cards.[93]

However, state legislators continued to express strong opposition to REAL ID.[94] In 2017, more than 100 Pennsylvania lawmakers wrote a letter to President Trump objecting to federal commandeering and sharing data with what they called a **"National Identity Registry."**[95] In 2017, more than 100 Missouri legislators told President Trump that REAL ID is "a de facto national ID" that "increases the potential for fraud and identity theft."[96]

Federal commandeering of states and federal control of individual movement and commerce is clearly the goal. The law states that "a Federal agency may not accept, for any official purpose, a driver's license or identification card issued by a State to any person unless the State is meeting" all REAL ID requirements.[97]

The REAL ID Act requires standardization of driver's licenses and identification cards according to federal specifications. This requirement includes the "for federal purposes" card—often called the REAL ID card—and the "not for federal purposes" card. According to the REAL ID Act, *both* cards must be compliant with REAL ID.[98]

The law also mandates state sharing of personal cardholder data with a private national database run by AAMVA called **SPEXS** (State Pointer Exchange Services), which is located in Virginia. As a private organization, AAMVA is not subject to the federal Freedom of Information Act.[99]

In December of 2015, Missouri Lieutenant Governor Peter Kinder issued a statement regarding Homeland Security's threat to

Federal commandeering of states and federal control of individual movement and commerce is clearly the goal of REAL ID.

Nothing prohibits Homeland Security from requiring additional biometric identifiers or radio frequency identification (RFID) chips for REAL ID.

enforce REAL ID in the state. He revealed that Missouri's Department of Revenue in 2013 violated state law as it tried to secretly begin complying with REAL ID. Legislative hearings revealed that Missouri citizens' **biometric data was being shared with MorphoTrust (now Idemia)**[100]–without the knowledge or consent of the public or the legislature.

Required data elements under the REAL ID Act include: full legal name, date of birth, gender, driver's license or identification card number, address, **digital (biometric) photograph**, signature, "physical security features designed to prevent tampering," and a "common machine-readable technology, with defined minimum data elements."[101] This technology—the PDF417 barcode—is capable of including text, images, and fingerprints.[102]

DHS determines these security features and data elements, and nothing prohibits DHS from requiring additional biometric identifiers and/or radio frequency identification (RFID) chips. Case in point: in 2007 DHS issued a proposed rule on REAL ID, and asked for public comments on how States would or could incorporate a separate technology for driver's licenses and identification cards to serve the Western Hemisphere Travel Initiative (WHTI), "such as an RFID-enabled vicinity chip technology, in addition to the REAL ID PDF417 barcode requirement."[103] However, after "many commenters said that RFID technology, the proposed technology for WHTI documents, should not be used on REAL IDs," the final 2008 rule required only the bar code. But that could change in a future rule.

Enhancing the threat to citizen privacy rights, the REAL ID Act requires that states copy, archive and digitize the original documents individuals submit as proof of identity, such as birth certificates, Social Security cards and other documentation.[104] States must also "provide electronic access to all other States to information contained in the motor vehicle database of the State."[105] This takes place using the SPEXS hub and the State to State (S2S) Verification Services, both created by AAMVA.[106]

The REAL ID ("for federal purposes") card must be used for any official purpose designated by DHS. The term "official purpose" is defined as: "includes but is not limited to accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and **any other purposes** that the Secretary shall determine."[107] [Emphasis added.]

To be clear, the Secretary of Homeland Security has **unilateral authority** to deem any activity, including hotel registration, purchasing firearms, and accessing medical care as an "official purpose" for which REAL ID is required. The Secretary need not ask Congress.[108] The longer the list of purposes, the greater the control and the greater the potential for data collection on individual movement and activity.

Idemia is ready for REAL ID. In 2016, MorphoTrust (now Idemia) announced the following: "MorphoTrust's security printing management system complies with relevant laws and regulations in force, and also demonstrates MorphoTrust's commitment to assisting customers in becoming compliant with the REAL ID Act."[109]

NATIONAL BIOMETRIC ID?

On January 10, 2018, U.S. Congressman Bob Goodlatte (R-VA) introduced legislation that would require Americans to carry a government-approved ID containing biometric features. This national biometric ID would be a requirement for working in the U.S. According to the legislation, the ID would be "evidence of authorization of employment in the United States."[110] According to U.S. Senator Rand Paul, H.R. 4760[111] "would give DACA [Deferred Action for Childhood Arrivals] recipients a 3-year renewable legal status while forcing a biometric National ID card on virtually everyone else."[112] It would also:

- create a biometric exit data system
- capture "biometric exit data at the time of departure" from the U.S. using "multiple modes of biometrics"
- "utilize facial recognition technology or other biometric technology . . . to inspect travelers at United States airports of entry"
- "match biometric information for an individual, regardless of nationality, citizenship, or immigration status, who is departing the United States against biometric data previously provided to the United States Government by such individual for the purposes of international travel"[113]

Although a report must be issued annually regarding data collection, including the number of U.S. citizens "subject to inspection" and timeframes and protocols for "storing, erasing, destroying and otherwise removing such data from databases," the legislation includes no requirement to remove the data.

Furthermore, if enacted, **"Nothing . . . may be construed as limiting the authority of the Secretary to collect biometric information in circumstances other than as specified in this section."**[114] [Emphasis added.] Idemia's current work with state and federal government agencies and experience in providing other foreign governments with biometric national IDs makes it a likely contractor if this bill becomes law.

NATIONAL PATIENT ID?

Many doctor's offices and hospitals require patients to show identification, typically scanning the driver's license or ID card into the electronic health record (EHR) and its billing system.[115] These EHR systems often share patient data through Internet-based corporate or state health information exchanges[116]—or the National Health Information Network, now called the eHealth Exchange, established and funded by the federal government.[117]

Demands for proof of identification likely began with the 2008 Federal Trade Commission's "Red Flag Rules" to prevent identity theft.[118] However, Congress clarified in 2010 that these rules do not include health care providers.[119] Shortly thereafter, a court ruled that the American Medical Association's lawsuit against the FTC was no longer necessary due to the "Red Flag Program Clarification Act of 2010," which excluded health care providers from being deemed as 'creditors.'[120] Yet some clinics still claim an ID is mandated by the Red Flag Rules.[121]

In other cases, as one 89-year old Maryland woman in pain and barely able to walk discovered in January 2018, some clinics insist patients present a current ID. The clinic refused to see her because she did not have a REAL ID. Her expired driver's license was not accepted as proof of identity. She had to leave the clinic

H.R. 4760 would give DACA recipients a 3-year renewable legal status while forcing a biometric National ID card on virtually everyone else.

untreated, and because she and her daughter couldn't find her original birth certificate as required by the federal REAL ID law, it took a visit to the Social Security Administration that day to obtain a special letter, which she then used to apply for a REAL ID.[122] Presumably, she had to reschedule the doctor's appointment she missed.

The move to create a National Patient ID has a long history. Although the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires a unique patient identifier (UPI) for every American, public opposition in 1998 led to a longstanding congressional prohibition on funding and development of the UPI.[123] However, in May 2017, a federal appropriations law provided funding to establish a national patient-matching strategy. Proponents of a national patient ID cheered.[124] Thus, the march toward a national patient ID system continues.

CONCLUSION

National IDs, digital tracking, state and national electronic data systems and biometric databases threaten individual privacy and constitutional liberty.

In the future, these data systems could include private medical information and the **ultimate biometric, citizen DNA**. Most Americans do not know that many state governments store the DNA (dried blood spots) of newborn citizens collected as part of state newborn (genetic) screening programs.[125] Approximately four million babies are born each year in the United States. Some states retain the DNA of these children indefinitely (essentially as state government property)—and use and share it— without parent consent.[126]

Government contracts with Idemia to create digital driver's licenses, REAL IDs and biometric identification systems enable surveillance, eviscerate privacy rights and advance a national ID system in the United States of America.

Under biometric identification mandates, Americans lose control over this sensitive data, which is uniquely theirs and, unlike a password, cannot be altered to protect against intrusions. As Adam Schwartz at the Electronic Frontier Foundation says, "biometrics are a menace to privacy. . . . Credit-card numbers can be changed, but faces and fingerprints can't."[127] The Foundation further notes, "Once biometric data is captured, it frequently flows between governmental and private sector users."[128]

Biometric IDs are not science fiction. Augmented identification, biometric mandates, and biometric databases are in place, being used, and expanding without public discussion or awareness.

In India, the national ID system is already being used to control (and track) patient access to treatment. Biometric-based identification is required for access to social benefits, medical care, banking, and more.[129]

Before biometric identification, REAL ID or digital driver's licenses are fully established or further imposed, we offer this report to enable informed legislative decision-making and encourage active citizen engagement to protect individual privacy, personal security, and patient autonomy.

** Twila Brase is president and co-founder of Citizens' Council for Health Freedom.*
Matt Flanders is CCHF's legislative specialist.

ENDNOTES

[1] "Benjamin Franklin Quotes," Benjamin Franklin, Goodreads.com, n.d. Accessed January 19, 2018: https://www.goodreads.com/quotes/140634-those-who-would-give-up-essential-liberty-to-purchase-a.

[2] "Mandatory National IDs and Biometric Databases," Electronic Frontier Foundation, n.d. Accessed December 29, 2017: https://www.eff.org/issues/national-ids.

[3] "Applying for PreCheck? Here's Where Your Fingerprints Go," Josh Noel, *Chicago Tribune*, March 1, 2014.

Accessed January 19, 2018: https://www.seattletimes.com/life/travel/applying-for-precheck-herersquos-where-your-fingerprints-go/.

4 "What is Face ID? Apple's New Facial Recognition Tech Explained," Michael deAgonia, *Computerworld,* November 1, 2017. Accessed December 29, 2017: https://www.computerworld.com/article/3235140/apple-ios/what-is-face-id-apples-new-facial-recognition-tech-explained.html.

5 "Idemia: Enter the World of Augmented Identity," Idemia, Sept. 28, 2017. Accessed December 21, 2017: https://www.youtube.com/watch?v=9pwlgLq4hg0.

6 "Biometric Terminals Add Security to a Variety of Processes," Idemia, n.d. Accessed January 4, 2018: https://www.morpho.com/en/biometric-terminals-add-security-variety-processes.

7 "What is Biometrics," Idemia, n.d. Accessed January 19, 2018: https://www.morpho.com/en/biometrics.

8 "Timeline | Idemia - OT-Morpho, n.d. Accessed January 4, 2018: http://www.morpho.com/en/timeline?showBackButton=1.

9 "OT-Morpho Becomes Idemia, the Global Leader in Trusted Identities," Idemia, n.d. Accessed December 21, 2017: https://www.idemia.com/press-release/ot-morpho-becomes-idemia-global-leader-trusted-identities-2017-09-28.

10 "Advent Acquires MorphoTrust Parent," Hiawatha Bray, *Boston Globe*, June 1, 2017. Accessed December 29, 2017: https://www.bostonglobe.com/business/2017/06/01/advent-acquires-morphotrust-parent/ILBtz49WjErAWebdzK3gDO/story.html.

11 Because of the merger of these two companies and their new name, there are currently three websites: Morpho.com, Oberthur.com, and Idemia.com. Additional online changes or a merger of all three websites could occur after publication of this report.

12 "Advent Said to Lead Bids for Morpho with $2.7 Billion Offer," Francois De Beaupuy, Manuel Baigorri, and Ruth David, *Bloomberg*, September 22, 2016. Accessed November 28, 2016: https://www.bloomberg.com/news/articles/2016-09-22/advent-said-to-lead-bidding-for-morpho-with-2-7-billion-offer.

13 "Connected Objects," Idemia, n.d. Accessed January 22, 2018: https://www.idemia.com/market/connected-objects.

14 "OT-Morpho Becomes Idemia, the Global Leader in Trusted Identities," Idemia, n.d. Accessed December 21, 2017: https://www.idemia.com/press-release/ot-morpho-becomes-idemia-global-leader-trusted-identities-2017-09-28.

15 "DNA Identification: RapidHIT," Idemia, n.d. Accessed January 29, 2018: https://www.morpho.com/en/public-security/law-enforcement/dna-identification/rapidhit.

16 "Georgia and North Carolina Partner with MorphoTrust to Reduce Tax Fraud," Business Wire, September 23, 2015. Accessed January 2, 2018: http://www.businesswire.com/news/home/20150923005895/en/Georgia-North-Carolina-Partner-MorphoTrust-Reduce-Tax; see also "MorphoTrust Adds Three States, 700,000 Applicants and $25.2 Million to Enrollment Business," Safran: MorphoTrust USA, February 23, 2014. Accessed January 2, 2018: http://www.morphotrust.com/Portals/0/02-03-14_Fingerprinting_Momentum.pdf.

17 "MorphoTrust Wins Identity Technology Contract Renewal with DoD," Safran: MorphoTrust USA, November 3, 2015. Accessed January 2, 2018: http://www.morpho.com/en/media/morphotrust-wins-identity-technology-contract-renewal-dod-20151103.

18 "Morpho in the US," Safran, n.d. Accessed January 17, 2018: https://www.morpho.com/en/country/morpho-us.

19 "Idemia Tech Aids CBP Trial of Biometric Screening at Sea Port," *FindBiometrics.com*, November 14, 2017. Accessed December 29, 2017: https://findbiometrics.com/idemia-cbp-biometric-screening-sea-port-411144/.

20 "Morpho in the US," Safran, n.d. Accessed January 17, 2018: https://www.morpho.com/en/country/morpho-us.

21 "DoD Selects MorphoTrust to Maintain Key Biometrics Platform," Morphotrust.com, March 11, 2013. Accessed November 28, 2016: http://www.morphotrust.com/portals/0/press releases/03.11.13_dodabis.pdf.

22 "REAL ID," Nathaniel "Ted" Sobel, Robert Ide, and Mark DiFraia, 2015 AAMVA Region 1 Conference, July 14, 2015. Accessed January 2, 2018: http://www.aamva.org/uploadedFiles/MainSite/Content/EventsEducation/Event_Materials/2015/2015_Region_I/REAL ID - July 14 from 11 to 12 - Merged Presentations.pdf.

23 "OT-Morpho Becomes Idemia, the Global Leader in Trusted Identities," Idemia, n.d. Accessed December 21, 2017: https://www.idemia.com/press-release/ot-morpho-becomes-idemia-global-leader-trusted-identities-2017-09-28.

24 "WikiLeaks Founder Assange on Hacked Podesta, DNC Emails: 'Our Source is Not the Russian Government,'" *Fox News*, December 16, 2016. Accessed January 2, 2018: http://

www.foxnews.com/politics/2016/12/16/wikileaks-founder-assange-on-hacked-podesta-dnc-emails-our-source-is-not-russian-government.html.

25 “Beyond the Yahoo Hack: Other Major Data Breaches,” *AP Business*, n.d. Accessed July 10, 2017: https://apnews.com/3967c0e7c8ce49ee95a53bddc79e87fe/beyond-yahoo-hack-other-major-data-breaches; see also “Equifax Hack: What We Learned,” *Fox Business*, December 27, 2017. Accessed December 29, 2017: http://www.foxbusiness.com/markets/2017/12/27/equifax-hack-what-learned.html.

26 “MorphoTrust Enrolls over One Million Americans in TSA Pre✓®,» Safran Identity & Security, March 24, 2015. Accessed November 28, 2016: https://www.morpho.com/en/media/morphotrust-enrolls-over-one-million-americans-tsa-prer-20150324; see also “Multi-Modal Biometric Platform,” ABIS Search Engine, MorphoTrust USA, n.d. Accessed December 29, 2017: http://www.morphotrust.com/Portals/0/MorphoTrust_ABIS.pdf.

27 “Biometric Data and the General Data Protection Regulation,” Gemalto, December 14, 2017. Accessed January 23, 2018: https://www.gemalto.com/govt/biometrics/biometric-data.

28 “Colorado Data Privacy Law Updated, Includes Medical Information,” Elizabeth Snell, Health IT Security, January 24, 2018. Accessed January 24, 2018: https://healthitsecurity.com/news/colorado-data-privacy-law-updated-includes-medical-information.

29 “Washington Biometric Privacy Law Lacks Teeth of Illinois Cousin,” Paul Shukovsky, Bloomberg Law: Privacy and Data Security, July 18, 2017. Accessed January 23, 2018: https://www.bna.com/washington-biometric-privacy-n73014461920/.

30 “Mobile Driver’s License (mDL) Pilot in Iowa,”Morphotrust.com, n.d. Accessed January 18, 2018: http://www.morphotrust.com/mDL/IowaPilot.aspx; see also “Emerging Mobile Technologies and the REAL ID At: Legal Challenges and REcommended Approaches,” Scott P. Boylan et al (MorphoTrust USA), Issue Brief #2017-02, Center for Cyber & Homeland Security, The George Washington University, February 2017. Accessed February 1, 2018: https://cchs.gwu.edu/sites/cchs.gwu.edu/files/downloads/Emerging_Mobile_Tech_and_The_Real_ID_Act.pdf

31 “Six States Will Trial Digital Driver’s License Tests in 2018,” Justin Lee, *Biometric Update*, October 24, 2017. Accessed January 19, 2018: http://www.biometricupdate.com/201710/six-states-will-trial-digital-drivers-license-tests-in-2018.

32 “Illinois Exploring Digital Driver’s Licenses,” *Chicago Tribune*, December 5, 2015. Accessed July 10, 2017: http://www.chicagotribune.com/news/local/breaking/ct-illinois-digital-drivers-licenses-20151205-story.html.

33 “What’s in Your Wallet? California Driver’s Licenses Closer to Going Digital,” *CBS Los Angeles*, n.d. Accessed November 28, 2016: http://losangeles.cbslocal.com/2015/02/05/whats-in-your-wallet-calif-drivers-licenses-closer-to-going-digital/.

34 “Digital Driver Licenses Soon to Be a Reality in Louisiana,” *ArkLaTexHomepage (KTAL NBC 6)*, n.d. Accessed November 28, 2016: http://www.arklatexhomepage.com/news/local-news/digital-driver-licenses-soon-to-be-a-reality-in-louisiana.

35 “New Jersey Considering Move to Electronic Driver’s License,” Michael Tanenbaum, *PhillyVoice*, January 10, 2016. Accessed November 28, 2016: http://www.phillyvoice.com/new-jersey-considering-move-electronic-drivers-license/.

36 “Six States Will Trial Digital Driver’s License Tests in 2018,” Justin Lee, *Biometric Update*, October 24, 2017. Accessed January 19, 2018: http://www.biometricupdate.com/201710/six-states-will-trial-digital-drivers-license-tests-in-2018.

37 “New Jersey Considering Move to Electronic Driver’s License,” Michael Tanenbaum, *PhillyVoice*, January 10, 2016. Accessed November 28, 2016: http://www.phillyvoice.com/new-jersey-considering-move-electronic-drivers-license/.

38 Ibid.

39 End of Legislative Session discussion hosted by Citizens’ Council for Health Freedom in Saint Paul, MN on June 7, 2016.

40 “UK Will Introduce Digital Driver’s License in 2018,” Sead Fadilpasic, *BetaNews*, 2016. Accessed January 2, 2018: http://betanews.com/2016/05/17/uk-digital-drivers-license-2018/.

41 “Tag Archives: Saudi Arabia,” Justin Lee and Stephen Mayhew, *Biometric Update*, n.d. Accessed November 28, 2016: http://www.biometricupdate.com/tag/saudi-arabia.

42 “Patrol Cars Will Now Scan Your Face Ministry of Interior Taps Futuristic Tech to Make Country Safest Place in the World,” Joseph George, *Emirates 24/7*, November 1, 2015. Accessed November 28, 2016: http://www.emirates247.com/news/emirates/patrol-cars-will-now-scan-your-face-2015-11-01-1.608819.

43 “UAE Airports Implementing Morpho’s Iris at a Distance Technology,” Justin Lee, *Biometric Update*, April 25, 2016. Accessed November 28, 2016: http://www.biometricupdate.com/201604/uae-airports-implementing-morphos-iris-at-a-distance-technology.

44 “Idemia: Our Journey,” Idemia. n.d. Accessed January 2, 2018: https://www.morpho.com/en/file/download/idemia-corporate-brochure.pdf.

45 “Biometrics Serving the Citizen,” Safran Identity & Security. n.d. Accessed February 17, 2017: http://www.morpho.com/en/media/20140519_biometrics-serving-citizen.

46 “Identity Solutions for Governments,” Safran, n.d. Accessed February 1, 2018: https://www.morpho.com/en/file/download/identity-solutions-for-government_0.pdf

47 “L-1 Identity Solutions Provides Software and Services to Paraguay Department of Identification for New National ID Card and Passport System,” Business Wire, January 14, 2009. Accessed November 28, 2016: http://www.businesswire.com/news/home/20090114006244/en/L-1-Identity-Solutions-Software-Services-Paraguay-Department.

48 “Aadhaar: A Unique ID Number for All,” Safran Identity & Security, n.d. Accessed January 2, 2018: https://www.morpho.com/en/media/aadhaar-unique-id-number-all-20151123.

49 Ibid.

50 “Aadhaar Data Leak: Edward Snowden Backs India Reporter Over Expose,” *BBC News*, January 9, 2018. Accessed January 10, 2018: http://www.bbc.com/news/world-asia-india-42601786.

51 “Aadhaar Isn’t Just About Privacy. There are 30 Challenges the Govt is Facing in Supreme Court,” Anoo Bhuyan, *The Wire*, January 18, 2018. Accessed January 24, 2018: https://thewire.in/215017/aadhaar-privacy-government-supreme-court/.

52 “Need to Maintain Balance Between Citizens’ Right to Privacy and National Interest, Says Supreme Court on Aadhaar,” Amit Anand Choudharyl, *Times of India*, January 25, 2018. Accessed January 25, 2018: https://timesofindia.indiatimes.com/india/need-to-maintain-balance-between-citizens-right-to-privacy-and-national-interest-says-supreme-court-on-aadhaar/articleshow/62638928.cms.

53 “Morpho in China,” Morpho, n.d. Accessed July 10, 2017: https://www.morpho.com/en/country/morpho-china.

54 “China’s All-Seeing Surveillance State Is Reading Its Citizens’ Faces,” Josh Chin and Liza Lin, *The Wall Street Journal*, June 26, 2017. Accessed July 10, 2017: https://www.wsj.com/articles/the-all-seeing-surveillance-state-feared-in-the-west-is-a-reality-in-china-1498493020.

55 “Smile to Enter: China Embraces Facial-Recognition Technology,” Yuan Yang and Yingshi Yang, *Financial Times*, n.d. Accessed January 2, 2018: https://www.ft.com/content/ae2ec0ac-4744-11e7-8519-9f94ee97d996.

56 “Top Video Surveillance Trends for 2017,” IHS Markit, Ltd., n.d. Accessed July 10, 2017: https://cdn.ihs.com/www/pdf/TEC-Video-Surveillance-Trends.pdf.

57 “China’s CCTV Surveillance Network Just Took 7 Minutes to Capture BBC Reporter,” Jon Russell, *TechCrunch*, Dec. 13, 2017. Accessed January 2, 2018: https://techcrunch.com/2017/12/13/china-cctv-bbc-reporter/.

58 “State Photo-ID Databases Become Troves for Police,” Craig Timberg and Ellen Nakashima, *The Washington Post*, June 16, 2013. Accessed November 28, 2016: https://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html.

59 “DoD Selects MorphoTrust to Maintain Key Biometrics Platform,” Morphotrust.com, March 11, 2013. Accessed November 28, 2016: http://www.morphotrust.com/portals/0/press releases/03.11.13_dodabis.pdf.

60 “Identity Search Engine Compares Biometrics to Watch Lists,” Stephanie Kanowitz, *GCN*, February 16, 2016. Accessed November 28, 2016: https://gcn.com/Articles/2016/02/16/identity-search-engine.aspx.

61 Ibid.

62 “A History of AFIS,” AVISIAN Staff, Secu*reID News*, December 2, 2014. Accessed January 22, 2018: https://www.secureidnews.com/news-item/a-history-of-afis/.

63 “List of FBI-Approved Channelers for Departmental Order Submissions,” Federal Bureau of Investigations, n.d. Accessed January 2, 2018: https://www.fbi.gov/services/cjis/identity-history-summary-checks/list-of-fbi-approved-channelers-for-departmental-order-submissions.

64 “Bamboozled: How to Get Your FBI ‘Rap Sheet’,” Karin Price Mueller, *New Jersey Advanced Media*, March 31, 2016. Accessed January 2, 2018: http://www.nj.com/business/index.ssf/2016/03/bamboozled_how_to_get_your_fbi_rap_sheet.html.

65 “ABIS,” Morphotrust.com, n.d. Accessed November

28, 2016: http://www.morphotrust.com/IdentitySolutions/ForFederalAgencies/Officer360/Investigator360/ABIS.aspx; see also “Multi-Modal Biometric Platform,” ABIS Search Engine, MorphoTrust USA, n.d. Accessed December 29, 2017: http://www.morphotrust.com/Portals/0/MorphoTrust_ABIS.pdf.

66 ABIS,” Morphotrust.com, n.d. Accessed November 28, 2016: http://www.morphotrust.com/IdentitySolutions/ForFederalAgencies/Officer360/Investigator360/ABIS.aspx.

67 “FBI Plans to Have 52 Million Photos in Its NGI Face Recognition Database by Next Year,” Jennifer Lynch, *Electronic Frontier Foundation*, April 14, 2014. Accessed November 28, 2016: https://www.eff.org/deeplinks/2014/04/fbi-plans-have-52-million-photos-its-ngi-face-recognition-database-next-year.

68 “FBI Software for Analyzing Fingerprints Contains Russian-Made Code, Whistleblowers Say,” Chris Hamby, *BuzzFeed News*, December 26, 2017. Accessed January 17, 2018: https://www.buzzfeed.com/chrishamby/fbi-software-contains-russian-made-code-that-could-open-a?utm_term=.kfobyP4RY#.osdJ8PZY2.

69 Ibid.

70 Ibid.

71 Ibid.

72 Ibid.

73 “Idemia Trials Biometric Verification Program with Royal Caribbean Cruises Ltd. and U.S. Customs and Border Protection, *BusinessWire,* November 14, 2017. Accessed February 1, 2018: https://www.businesswire.com/news/home/20171114005357/en/IDEMIA-Trials-Biometric-Verification-Program-Royal-Caribbean.

74 “CBP Orders Ruggedized Identification Kits from MorphoTrak,” *FindBiometrics.com*, May 18, 2016. Accessed December 29, 2017: https://findbiometrics.com/cbp-identification-kits-morphotrak-305183/.

75 “Idemia Tech Aids CBP Trial of Biometric Screening at Sea Port,” *FindBiometrics.com*, November 14, 2017. Accessed December 29, 2017: https://findbiometrics.com/idemia-cbp-biometric-screening-sea-port-411144/.

76 “CBP Brings Biometric Screening to Las Vegas Airport,” *FindBiometrics.com*, August 10, 2017. Accessed December 29, 2017: https://findbiometrics.com/cbp-biometric-screening-las-vegas-408103/.

77 “MorphoTrust Inks Two States, CrossMatch Deployed for Asylum Seekers,” Zach Martin, *SecureIDNews*, March 03, 2016. Accessed January 2, 2018: http://www.secureidnews.com/news-item/morphotrust-inks-two-states-crossmatch-deployed-for-asylum-seekers/.

78 “Georgia and North Carolina Partner with MorphoTrust to Reduce Tax Fraud,” Business Wire, September 23, 2015. Accessed January 2, 2018: http://www.businesswire.com/news/home/20150923005895/en/Georgia-North-Carolina-Partner-MorphoTrust-Reduce-Tax.

79 “About Safran Identity and Security: Leader in Biometrics and Digital Identity,” Safran, n.d. Accessed December 21, 2017: http://www.morpho.com/en/about-us.

80 “Robert Eckel,” LinkedIn, n.d. Accessed December 29, 2017: https://www.linkedin.com/in/roberteckel/.

81 “Idemia: Our Journey,” Idemia, n.d. Accessed January 2, 2018: https://www.morpho.com/en/file/download/idemia-corporate-brochure.pdf.

82 “Factbox: France’s Military and Defense Contractors,” Cyril Altymer and Alexandria Sage, *Reuters*, April 28, 2013. Accessed January 17, 2018: https://www.reuters.com/article/us-france-defence-factbox/factbox-frances-military-and-defense-contractors-idUSBRE93R01X20130428; see also “Advent Said to Lead Bids for Morpho with $2.7 Billion Offer,” Francois De Beaupuy, Manuel Baigorri, and Ruth David, *Bloomberg*, September 22, 2016. Accessed November 28, 2016: https://www.bloomberg.com/news/articles/2016-09-22/advent-said-to-lead-bidding-for-morpho-with-2-7-billion-offer.

83 “Timeline | Idemia - OT-Morpho, n.d. Accessed January 4, 2018: http://www.morpho.com/en/timeline?showBackButton=1.

84 “What We (Don’t) Know About the Companies,” Usha Ramanathan, *The Statesman*, October 31, 2013. Accessed January 3, 2018: http://www.thealternative.in/society/what-we-dont-know-about-the-companies/.

85 “George Tenet Cashes in on Iraq,” Tim Shorrock, *Salon*, May 07, 2007. Accessed November 28, 2016: http://www.salon.com/2007/05/07/tenet_money/.

86 “Biometric Technology Supplied by Morphotrak for FBI NGI to Transform Crime Solving,” Morpho, n.d. Accessed December 19, 2016: http://www.morpho.com/en/media/biometric-technology-supplied-morphotrak-fbi-ngi-transform-crime-solving-20130709.

87 “Minnesota’s Real ID Debacle, Explained,” Briana Bierschbach, *MINNPOST*, January 8, 2016. Accessed December

16, 2016: https://www.minnpost.com/politics-policy/2016/01/minnesotas-real-id-debacle-explained.

88 “The History of Federal Requirements for State Issued Driver’s Licenses and Identification Cards,” National Conference of State Legislatures, n.d. Accessed December 16, 2016: http://www.ncsl.org/research/transportation/history-behind-the-real-id-act.aspx.

89 “REAL ID: A State-By-State Update,” Jim Harper, Policy Analysis, Cato Institute, May 12, 2014. Accessed January 22, 2018: https://object.cato.org/sites/cato.org/files/pubs/pdf/pa749_web_3.pdf.

90 Remarks by Senator Lamar Alexander (TN) on the REAL ID ACT of 2005, *C-SPAN*, May 10, 2005. Accessed July 10, 2017: https://www.c-span.org/video/?186668-2/senate-session&start=12133.

91 “REAL ID – Federal Control Over Identification and Movement,” Citizens’ Council for Health Freedom, Accessed January 2, 2018: http://www.cchfreedom.org/issue.php/39.

92 “REAL ID Enforcement Update,” Countdown to REAL ID, National Conference of State Legislatures, October 14, 2016. Accessed January 3, 2018: http://www.ncsl.org/research/transportation/count-down-to-real-id.aspx.

93 “REAL ID,” US Department of Homeland Security, Last published date January 19, 2018. Accessed January 22, 2018: https://www.dhs.gov/real-id.

94 “Alaskans Shouldn’t Fall for Real ID Scare Tactics,” Rep. Chris Tuck (Majority Leader, Alaska House of Representatives), *Alaska Dispatch News*, April 22, 2017. Accessed May 31, 2017: https://www.adn.com/opinions/2017/04/22/alaskans-shouldnt-fall-for-real-id-scare-tactics/.

95 Letter to President Donald Trump, Reps. Daryl Metcalfe and Mike Turzai, House of Representatives, Commonwealth of Pennsylvania, January 24, 2017. Accessed on CCHF website May 31, 2017: http://www.cchfreedom.org/files/files/PA%20Letter%20to%20Trump%20-%20REAL%20ID%20-%20Condensed.pdf.

96 Letter to President Donald J. Trump, Missouri General Assembly, (pdf on Citizens’ Council for Health Freedom’s website): January 24, 2017. Accessed January 18, 2018: http://www.cchfreedom.org/files/files/2017%20REAL%20ID%20Pres_%20Trump%20Letter%20(signed).pdf.

97 REAL ID Act – Title II – Improved Security for Drivers’ Licenses and Personal Identification Cards, 2005. Accessed January 3, 2018: https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf.

98 “Vote NO on REAL ID – Big Government Dual-Track Bills,” Citizens’ Council for Health Freedom, n.d. Accessed January 2, 2018: http://www.cchfreedom.org/files/files/Dual%20Track%20-%20Why%20Vote%20NO%20wo%20Amendment.pdf.

99 “How the REAL–ID Act is Creating a National ID Database,” The Identity Project, February 11, 2016. Accessed May 31, 2017: https://papersplease.org/wp/2016/02/11/how-the-real-id-act-is-creating-a-national-id-database/.

100 “PR Lieutenant Governor Peter Kinder Urges Missouri to Reject Homeland Security Threats Over REAL ID,” Press Release, December 19, 2015. Accessed January 17, 2018: https://themissouritimes.com/25671/lieutenant-governor-peter-kinder-urges-missouri-to-reject-homeland-security-threats-over-real-id/.

101 REAL ID Act – Title II – Improved Security for Drivers’ Licenses and Personal Identification Cards, 2005. Accessed January 3, 2018: https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf.

102 “Uses of RFID Technology in U.S. Identification Documents,” Monica Nogueira and Noel Greis, Institute for Homeland Security Solutions, December 2009. Accessed May 31, 2017: https://www.kenan-flagler.unc.edu/~/media/Files/kenaninstitute/CLDS/IHSSResearchBrief_RFID.pdf.

103 “Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes: Notice of Proposed Rulemaking,” Department of Homeland Security, Federal Register, vol. 72, no. 46, March 9, 2007, p 10842. Accessed January 22, 2018: https://www.gpo.gov/fdsys/pkg/FR-2007-03-09/pdf/07-1009.pdf.

104 “REAL ID Raises Gold-Star Privacy Issues,” Bruce Siceloff, *The Charlotte Observer*, January 16, 2016. Accessed May 31, 2017: http://www.charlotteobserver.com/news/politics-government/article55080665.html.

105 REAL ID Act – Title II – Improved Security for Drivers’ Licenses and Personal Identification Cards, 2005. Accessed January 3, 2018: https://www.dhs.gov/xlibrary/assets/real-id-act-text.pdf.

106 “How the REAL–ID Act is Creating a National ID Database,” The Identity Project, February 11, 2016. Accessed May 31, 2017: https://papersplease.org/wp/2016/02/11/how-the-real-id-act-is-creating-a-national-id-database/.

107 Ibid.

108 “Minimum Standards for Driver’s Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes; Final Rule,” 6 C.F.R. § 37, Department of Homeland Security, 2008, p. 5288. Accessed January 3, 2018: http://www.cchfreedom.org/files/files/Real%20ID%20Rule%202008.pdf.

109 “MorphoTrust USA, Manufacturer of 80 Percent of the Country’s Driver Licenses, Announces All Factories Now ISO Certified” (press release), MorphoTrust, May 17, 2016. Accessed December 29, 2017: https://www.morpho.com/en/media/morphotrust-usa-manufacturer-80-percent-countrys-driver-licenses-announces-all-factories-now-iso-certified-20160517.

110 “H.R. 4760 – Securing America’s Future Act of 2018,” Rep. Bob Goodlatte, January 10, 2018, 90. Accessed January 29, 2018: https://www.congress.gov/bill/115th-congress/house-bill/4760.

111 “H.R. 4760 – Securing America’s Future Act of 2018,” Rep. Bob Goodlatte, January 10, 2018. Accessed January 29, 2018: https://www.congress.gov/bill/115th-congress/house-bill/4760.

112 “Congress Quietly Pushing Bill to Require National Biometric ID for ‘All Americans,’” Matt Agorist, *The Liberty Beacon*, January 23, 2018. Accessed January 29, 2018: https://constitution.com/congressional-bill-force-americans-carry-biometric-id-card/.

113 “H.R. 4760 – Securing America’s Future Act of 2018,” Rep. Bob Goodlatte, January 10, 2018, 356 - 367. Accessed January 29, 2018: https://www.congress.gov/bill/115th-congress/house-bill/4760.

114 Ibid., 366.

115 “Positive Patient Identification Begins at Step One,” Health Management Technology, July 24, 2012. Accessed January 22, 2018: https://www.healthmgttech.com/positive-patient-identification-begins-at-step-one.php.

116 “Evaluation of the State HIE Cooperative Agreement Program: Final Report,” NORC, March 2016. Accessed January 22, 2018: https://www.healthit.gov/sites/default/files/reports/finalsummativereportmarch_2016.pdf.

117 “What is the eHealth Exchange?” HealthIT.gov, November 17, 2015. Accessed December 29, 2017: https://www.healthit.gov/providers-professionals/faqs/what-ehealth-exchange.

118 “Red Flags Health Care Clinics Policy,” Nova Southeastern University, n.d. Accessed December 29, 2017: http://www.nova.edu/risk/policies/redflags_healthcare.html.

119 “President Obama Signs Red Flag Program Clarification Act,” Privacy & Information Security Law Blog, Hunton & Williams, December 20, 2010. Accessed December 29, 2017: https://www.huntonprivacyblog.com/2010/12/20/president-obama-signs-red-flag-program-clarification-act/.

120 “Court’s Ruling Ends AMA Lawsuit Over Red Flags Rule,” Molly Merrill, *Healthcare Finance*, March 8, 2011. Accessed December 29, 2017: http://www.healthcarefinancenews.com/news/courts-ruling-ends-ama-lawsuit-over-red-flags-rule.

121 Conversation between a clinic and CCHF president, Twila Brase.

122 “Letter: Real ID Law an Abuse of Senior Citizens,” Debbie Schaeffer, *Carroll County Times*, January 19, 2018. Accessed January 19, 2018: http://www.carrollcountytimes.com/cc-op-letters-schaeffer-20180118-story.html.

123 “National Patient ID,” Twila Brase, Citizens’ Council for Health Freedom, July 2012. Accessed December 29, 2017: http://www.cchfreedom.org/files/files/Final_UPI_Report-Use(1).pdf.

124 “National Patient Identifier Gains Congressional Support,” Kate Monica, *EHR Intelligence,* May 11, 2017. Accessed December 29, 2017: https://ehrintelligence.com/news/national-patient-identifier-gains-congressional-support.

125 “Overview of Newborn Screening,” Newborn Screening Laboratory Bulletin, Centers for Disease Control and Prevention, February 21, 2014. Accessed January 11, 2018: https://www.cdc.gov/nbslabbulletin/bulletin.html.

126 “After Newborn Genetic Testing of Baby is Done: State by State Government Newborn Blood & Baby DNA Retention Practices” (2002-2016), Citizens’ Council for Health Freedom, 2016. Accessed December 29, 2017: http://www.cchfreedom.org/files/files/2016%20Newborn%20Retention%20All%2050%20States.pdf; see also www.itsmydna.org.

127 “Google Faces Off With Privacy Laws,” Jack Nicas, The Wall Street Journal, January 18, 2018. Accessed January 24, 2018: https://www.wsj.com/articles/why-google-wont-search-for-art-look-alike-in-some-states-1516194001.

128 “Mandatory National IDs and Biometric Databases,” Electronic Frontier Foundation, n.d. Accessed December 29, 2017: https://www.eff.org/issues/national-ids.

129 “Aadhaar: A Unique ID Number for All,” Safran Identity & Security, 2016. Accessed November 28, 2016: http://www.morpho.com/en/media/20151123_aadhaar-unique-id-number-all.