*****NEWS RELEASE*****

For Immediate Release
February 20, 2018

MEDIA CONTACT:
Hamilton Strategies, 610.584.1096, ext. 104, or Media@HamiltonStrategies.com

Citizens' Council for Health Freedom Exposes IDEMIA and the Push for National Biometric IDs in America

New Report Educates Americans on Corporation Facilitating Government Intrusion—and Possible Future Biometric National Patient IDs

ST. PAUL, Minn.—A stalwart advocate for patient privacy, ***Citizens' Council for Health Freedom (CCHF, www.cchfreedom.org)*** has released a new report exposing a global corporation that is working with state and federal government agencies to facilitate the collection of biometric data from Americans.

Perhaps the most concerning aspect is that Idemia, which calls itself "the global leader in trusted identities," produces driver's licenses for 42 states and is ready to transition state driver's licenses and IDs to the digital realm—to a cellphone, which would enable remote access and control. Several states have already made steps toward this end with trials on digital driver's licenses (DDLs).

"We learned about Idemia, then called MorphoTrust, after receiving an unexpected inquiry from a citizen during our efforts to stop REAL ID," said CCHF president and co-founder Twila Brase, the lead author of the report. "This corporation is huge and partially under French ownership. It provides biometric IDs for India and it's part of most Americans' lives, but they have no idea that Idemia exists. The possibility of mandated biometric IDs and current states' efforts in Iowa and elsewhere to create a digital driver's license that can be accessed and deactivated remotely by the government should concern everyone."

In the new report, titled "Exposing Idemia: The Push for National Biometric IDs in America," ***CCHF*** reveals the following key facts:

- 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 (i.e., "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.

In the report, Brase and co-author Matthew Flanders of ***CCHF*** note that Benjamin Franklin prioritized freedom: "Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety."

"Although Mr. Franklin could not have foreseen our technological world, including computers, the internet, smartphones and electronic health records," Brase said, "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."

National ID cards and the databases behind them comprise the cornerstone of government surveillance systems that create risks to privacy, autonomy and anonymity, ***CCHF*** reports. The requirement to produce identity cards on demand conditions citizens to participate in their own surveillance and social control.

"Freedom lost is not easily regained," Brase said. "The authors of the U.S. Constitution and its Bill of Rights understood the importance of privacy to freedom and security. Although some say biometric IDs would increase security, the loss of the individual right to be free would be the greatest insecurity of all. Idemia, the focus of our 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."

But Idemia is acquainted with most American citizens, whose private information flows through its equipment, databases and software products. 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.

"Our 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," Brase and Flanders write. "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."

Read more about the history of Idemia on pages 2 and 3 of the report.

"In the future, these data systems could include private medical information and the ultimate biometric, citizen DNA," Brase said. "Most Americans do not know that many state governments store, use and share the DNA of newborn citizens collected as part of state newborn genetic screening programs—without parent consent. 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.

Brase added, "We hope our report, 'Exposing Idemia,' will enable informed legislative decision-making and encourage active citizen engagement to protect individual privacy, personal security and patient autonomy."

CCHF's report also covers global reach of Idemia, digital IDs overseas, 24/7 biometric surveillance, digital databases, federal facial recognition programs at U.S. airports, pending lawsuits, the possibility of digital REAL ID and National Patient IDs, and one patient's REAL ID story. View the complete report here.

For more information about ***CCHF,*** visit www.cchfreedom.org, its Facebook page or its Twitter feed @CCHFreedom. Also view the **media page for *CCHF* here**. For more CCHF reports on health privacy and surveillance, visit the CCHF privacy page. For more about ***CCHF's***initiative to protect newborn DNA, visit www.itsmydna.org.

###

For information or to interview Twila Brase of *Citizens' Council for Health Freedom*, contact Deborah Hamilton, Media@HamiltonStrategies.com, 610.584.1096, ext. 102.