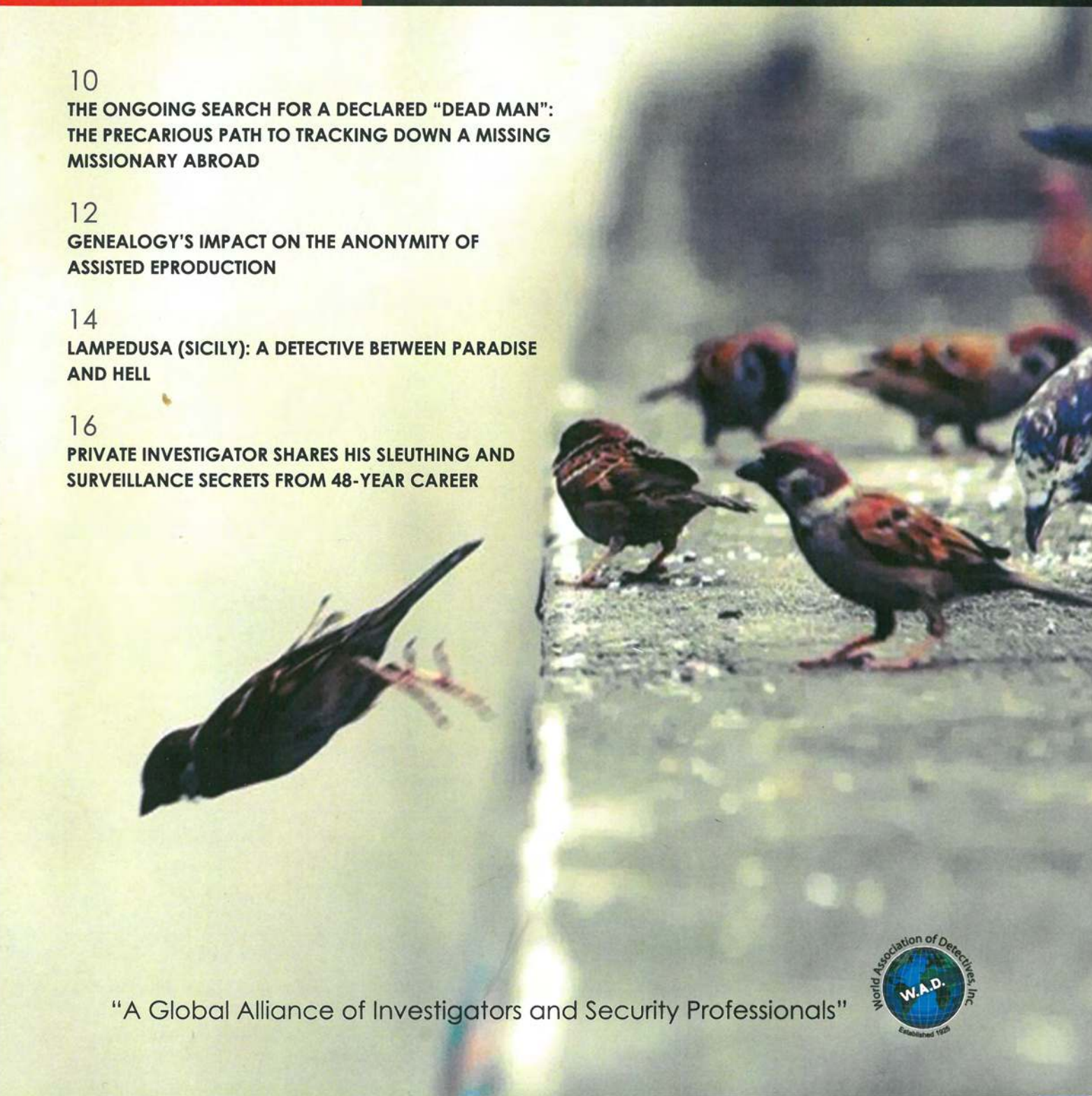
Volume 69, Issue 22 | January – April, 2018

W.A.D beyond GLOBAL

A Quarterly Journal for Investigators and Security Professionals



"A Global Alliance of Investigators and Security Professionals"

THE INTERNET OF THINGS, THE INDUSTRIAL INTERNET OF THINGS AND THE GDPR/2016 (GENERAL DATA PROTECTION REGULATION -EU)

By Laura Giuliani

Are we quite sure we aren't being spied upon in the office, at home or when we're driving our car?
Current hi-tech platforms such as the so-called Internet of Things (IoT) and/or the Industrial Internet of Things (IIoT) are increasingly playing a pivotal role both in sensitive data abuse and in cyberattacks.

Behind these acronyms — IoT, IIoT – lie a host of chip-enabled devices that can be linked to standard servers, Pcs and smart devices (tablets and smartphone) for various applications; such as domotics, industrial components, smart sensors, other mobile devices, etc.

The threat of illicit data mining from such devices is compounded by their own characteristics: they are ubiquitous, their usage tends to revolve around sensitive areas (home, office, plant), and at sensitive times; their easy availability through the WEB, and the aboundance of computing power in general, are unavoidable facts. In brief, the Internet's capability of data gathering via remote devices has a dark potential, which is being exploited to ever more alarming effect.

But if the objects that surround us, and possibly their makers, so often become the perpetrators, our own carelessness may well be their best accomplice. Only rarely do we concern ourselves with the privacy policies of our items of everyday use; as a consequence, more and more, our "smart" tvs, vacuum cleaners, toys such as dolls might become uncanny, hidden spies of our private and professional lives. Their activities may well include the mapping of our homes and offices; or they might record us, listen in, take pictures, transmit our data to a cloud; they can also become powerful, if possibly illegitimate, business or marketing tools.

Take the famous German doll CAYLA, which hides a potential for crime beneath its silky voice and reassuring air. According to Germany's Federal agency for telecom networks it might also be used as a bug. Cayla has a built-in Bluetooth-enabled mic which can connect with any smart device in a 10-metre range, and might be used for listening in, wiretape and even communication device. According to the agency, which has banned its sale, hackers might easily tweak the doll for such purposes.

Also, beware of the spying Barbie doll. In the US, the Campaign for a Commercial-Free Childhood (CCFC), an association that fights for kid's rights, has launched an online petition against the «eavesdropping Hello Barbie» Mattel, the manufacturer of the world's most popular toy, had started marketing this hi-tech, AI-based version, tweaked for maximum kid interaction. A mic embedded in the doll's necklace captures kids' questions, which are then forwarded via WiFi to the servers at ToyTalk, a Californian AI company, which has the recording converted to text data and analyzed to come up with the best answer from a database of over 8k prerecorded soundbites.

Then, there's Roomba, a spy that maps out interiors even as it is ostensibly cleaning them up; iRobot's brand new vacuum cleaner, which can now be controlled via Amazon's Alexa digital PA system, has been gathering data about its areas of deployment for years, in order to enhance its autonomy of movement. Equipped with proximity sensors and a camera, it can perform 3D mappings of its surroundings.

All of which, as can easily be imagined, has a great potential for infringement of privacy: this kind of comes with the territory, you could say, wherever the IoT and its services, as innovative as they are hungry for personal (not to say sensitive) data, are concerned.

Rightly taking such critical issues into account, for the very first time Europe's regulators have now set protection guidelines. Based on a principle of prevention, the General Data Protection Regulation (REG. UE/2016/675) set to become binding as 2018, it requires companies and professional firms to protect the privacy of EU citizen.

In order to avoid any interference in private lives, as well as to regulate the all to great power of the big digital companies, the new European rulebook has been introduced on May 24, 2016, and is set to become enforceable (with heavy sanctions) this year, as of May 25. The EU directive (GDPR – n° 679/2016, substituting the previous Data Protection Directive 95/46/EC) concerns all businesses operating within the digital marketplace handling data of EU citizen. It puts responsibility on those collecting data under the principles of privacy by design and privacy by default. This means that businesses gathering consumer data will be required to proactively implement protection measures for their products and services, or face severe sanctions.

The Regulation guidelines are 1) very detailed and 2) uniformly apply to the European Union, 3) but may also be applied to non-EU businesses (GDPR regarding gathering of data by EU residents by any operator), 4) are effective immediately, as they do not require national governments to pass any legislation and are directly binding; 5) it sets standard requirements that are non-negotiable and 6) sets "Breach notification" rules, so that any operator suffering a data breach which might "put the rights and liberty of individuals at risk" is required to notify this to authorities within 72 hours of becoming aware of it.

The protection of personal data is itself based on the fundamental, unalienable right to privacy of any individual under art. 8 of the Charter of the Fundamental Rights of the European Union (2000/C 364/01) (the so called Charter of Nice), which states:

Protection of personal data

1. ***Everyone has the right to the protection of personal data concerning him or her.***

2. ***Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.***

3. ***Compliance with these rules shall be subject to control by an independent authority.***

Furthermore, the regulation aims to contain the devastating, uncontrolled impact of new technologies, transcending national boundaries; as a consequence, personal data treatment assumes a transnational character.

All of which represents a big leap forward in the fight against unlegitimate use of personal data, and if correctly enforced it should afford us some degree of comfort and confidence in using those devices which are really meant to make daily life – at home, at play or in the office – easier.