Data Security:
Analysis of Global and Russian Trends

Marco Research S.A.M.

2016

Data Security: Analysis of Global and Russian Trends

2016

Marco Research S.A.M.

Roc Azur Bloc A
29 Boulevard d'Italie
Monte-Carlo
Monaco
Tel.: +377 977 73147
Fax: +377 977 73148

All of the information included in this document is for informational purposes only, and may not reflect the most current legal developments, judgments, or settlements. This information is not offered as legal or any other advice on any particular matter.

Marco Research S.A.M. and the contributing authors expressly disclaim all liability to any person in respect of anything, and in respect of the consequences of anything, done or not done wholly or partly in reliance upon the whole or any part of the contents of this brochure. No client or other reader should act or refrain from acting on the basis of any matter contained in this document without first seeking the appropriate legal or other professional advice on the particular facts and circumstances.

Table of Contents

Main conclusions

"Big Brother is Watching You": in 1949, the dystopian novel Nineteen Eighty Four introduced this phrase to popular culture. Today it lives the life of its own and means that intelligence agencies carry out - or at least are capable of carrying out - a total control over the general public.

The extent to which the George Orwell's realm is already our reality is the subject of heated debate. However, there is no doubt that the governments' aim is to have access to all devices and means of communication. In January 2015, British Prime Minister David Cameron stated that there should be no "means of communication" which "we cannot read". Two days later, US president Barack Obama sided with David Cameron.

Russia is no exception. The law "On Personal Data" and number of other legislative initiatives as well as the recent establishment by the National Anti-terrorist Committee of the Working Group On Access To Encrypted Traffic indicates that the Kremlin is not satisfied with the current state of affairs and, in the nearest future, it will have control of all communications on the Russian territory.

Despite the fact that governments' actions are controversial from the legal standpoint, we have to see reality as it is. And the reality is that the power of the intelligence agencies are extremely extensive. These include not only spying on a particular person using his/her own computer, communication channels and mobile devices but using technical devices belonging to other people, usually without their knowledge.

The recent compromise of the Panama Papers – a leak of 11 million confidential documents from the Panamanian law firm and offshore service provider Mossack Fonseca – identified this sector as a treasure trove for information and data not only for criminals but also for governments - akin to the wake-up call Snowden provided back in 2013. The lack of awareness and visibility of digital interactions and data may lead to greater public and legal scrutiny.

These latest developments must again reinforce cyber security and data privacy as a question of boardroom importance. Clients are advised to handle digital assets with the same care as traditional assets. Each day, clients and their offices receive, relay, and manage voluminous private information, including financial information, account numbers, health and even estate planning documents. In this regard, our recommendation is to review the procedures for handling and hosting confidential information and, in particular, to consider proper location and jurisdictions for servers, the use of end-to-end encryption and to ensure data security and privacy when evaluating and contracting third parties.

Global trends

Initially, secure communication methods were developed under the state control for military and intelligence purposes. However, with time it became impossible to keep the cryptographic systems only for the military.

Banks and financial institutions need encryption to facilitate money transfers and transactions with financial instruments. The advent of personal computers and, later, e-commerce led to the development of cryptographic instruments outside of the government bodies.

When in 1991 Philip Zimmermann created PGP cryptosystem, the governments found themselves in a position when they might be unable to read communications of their citizens. Criminal investigation was opened against Philip Zimmerman and lasted for three years.

Over the years a wide campaign, led by the Electronic Frontier Foundation and the Foundation for Information Policy Research, unfolded with the aim to combat governments' attempts to restrict public access to the cryptographic methods. This movement is known as "cryptographic wars".

At some point it seemed that the public has won. In the USA in 2000, Al Gore, the most outspoken advocate for restrictions on access to cryptographic instruments, lost presidential elections. In the UK, the Export Control Act 2002 was changed to ease the export of software with cryptographic protection. In May 2005, Chapter I of the Electronic Communications Act 2000, that allowed Home Office regulate encryption services, was repealed.

However, in 2013 former CIA and NSA employee Edward Snowden leaked classified documents which show that the USA, in collaboration with Australia and New Zealand, carry out total interception of information on domestic and international communication channels. Similar programs were also discovered in France and the UK.

Whether these activities violate the law, particularly the Fourth Amendment to the US Constitution, is an interesting but largely rhetorical question. A number of cases, in particular, *Hepting v AT&T*, *Jewel v NSA*, *Clapper v Amnesty International*, *Al-Haramain Islamic Foundation v Barack Obama* and *Center for Constitutional Rights v Barack Obama* did not, apparently, change the policy. On the contrary, the US government granted immunity from prosecution to Internet service providers participating in the domestic surveillance. Moreover, this immunity has retroactive effect.

The reality is that the intelligence agencies conduct a number of secret programs aimed at wiretapping and interception of electronic communications of billions of people. Information is collected directly from central servers and internet backbones located in different countries around the world.

NSA can access confidential data from smartphones running popular operating systems Android, iOS and BlackBerry and can obtain information about the location of the devices, content of the electronic notebooks, SMS-messages, files and other data.

Major Internet companies, including Google, Facebook, Skype, Yahoo !, Apple, Microsoft, AOL and Paltalk share data with NSA. Microsoft provided NSA with backdoor entrance to some of its programs, including Outlook and Windows from Vista SP1 and onwards.

Panama Papers

However, as the "Panama Papers"- the recent leak of 11.5 million documents, totalling 2.6 terabytes of data from the law firm Mossack Fonseca - show, one does not only have to fear governments utilizing backdoors and super computers for decryption, but counterparties, agents and service providers showing an astonishing disregard for secuity.

Namely, until late April 2016 Mossack Fonseca's email transport was not encrypted – this corresponds to sending a plain-text post-card with your most private information for everyone to read and intercept.

> "[…] Specifically, we have added a web application firewall. [Now] we have also activated a transport layer security protocol that will ensure we have secure email encryption available."
>
> Client Announcement send by Mossack Fonseca on Friday 04/15/2016

Amongst other lapses, Mossack Fonseca has failed to update its Outlook Web Access login since 2009 and not updated its client login portal since 2013.

If there ever was an organization that warranted exceptional network security tools and data security measures, a company trusted with management of over 214,000 offshore shell companies certainly would be it. Organisations will need to start factoring cybersecurity capabilities into their vendor evaluation.

The situation in Russia

Russia is a member of the Wassenaar Arrangement, an international convention seeking to restrict distribution of conventional arms and dual-use goods and technologies. Encryption methods come under the scope of the arrangement.

Commercial activities with cryptographic technologies are subject to strict state control, in fact stricter than is required by the Wassenaar Arrangement.

In particular, Government Resolution of 16 April 2012 №313 "On Licensing Of The Development, Production, Distribution Of Encryption (Cryptographic) Methods" bans any data protection activity unless authorised by the state.

Order of the Russian Federal Security Service of 9 February 2005 N66 "On Approval Of The Design, Manufacture, Sale And Maintenance Of Encryption (Cryptographic) Instruments" states that control over data encryption activities is carried out by the Federal Security Service.

In accordance with the Federal Law "On Personal Data", from 1 September 2015 personal data of Russian individuals must be processed and stored on the Russian territory.

On 19 April 2016, the National Anti-Terrorist Committee of Russia set up Working Group On Access To Encrypted Traffic. The group includes representatives from all law enforcement agencies, the Ministry of Economic Development, the Ministry of Communications and the Russian Association of Electronic Communications.

Our understanding of these events is that the Russian government seeks to collect full information about its citizens and take all communications under control.

Final thoughts

The legislation of most developed countries, including Russia, does not allow the use of evidence obtained in violation of law. Such evidence, generally speaking, is inadmissible and, therefore, cannot be used in legal proceedings.

However, in practice this is not always the case. Moreover, the Panama scandal indicates that governments may be tempted to use stolen documents in, inter alia, criminal proceedings.

We believe that the intelligence agencies of developed countries will get what they want and very soon establish full control over the vast majority of communications. This means that it is time to take a closer look at how confidential and sensitive information is used and stored and factor cybersecurity capabilities into counterparties and agents' evaluation.