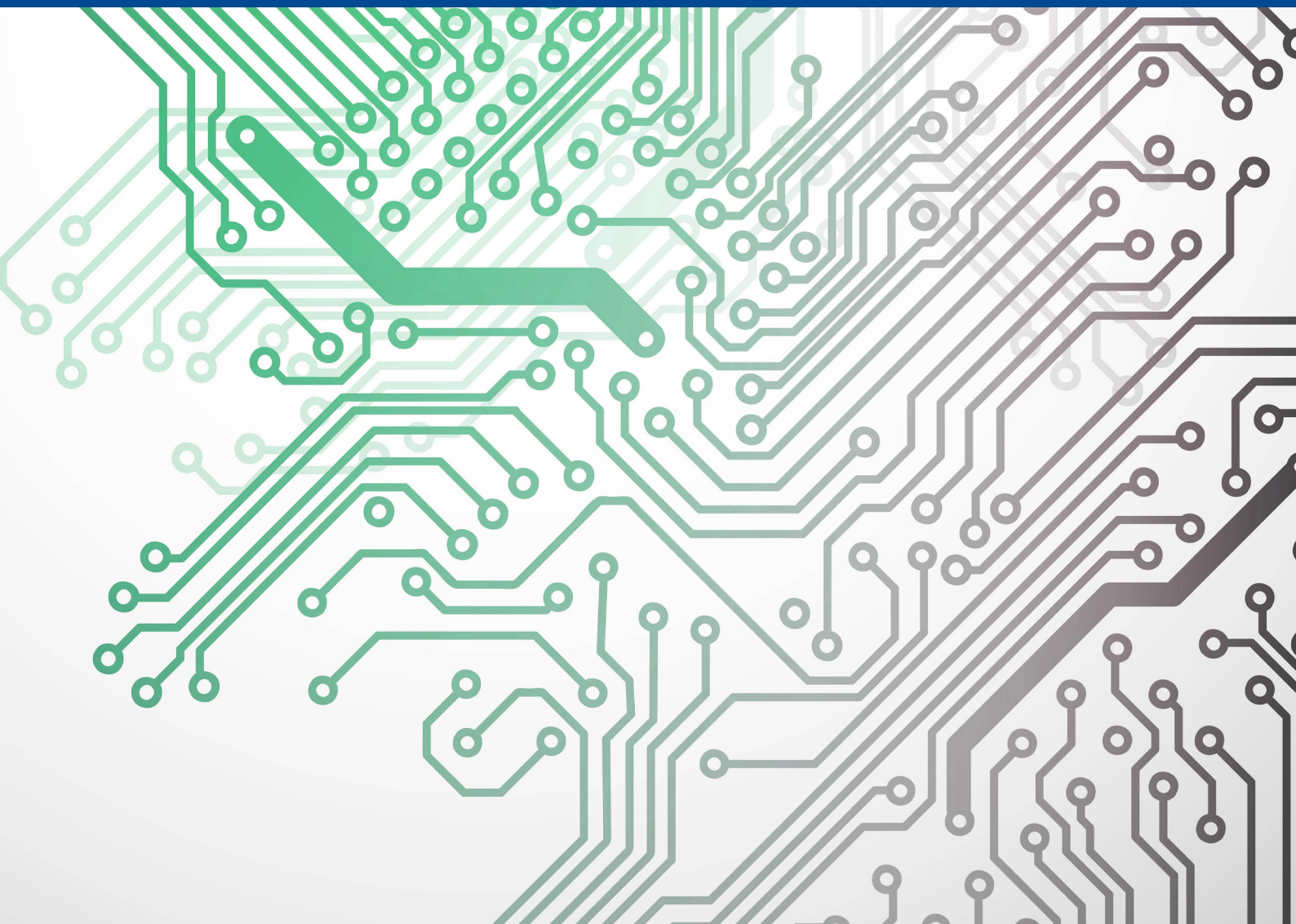
EUROPEAN LAWYERS
EUROPEAN BARS
CCBE
BARREAUX EUROPÉENS
AVOCATS EUROPÉENS

CCBE GUIDANCE

on Improving the IT Security of Lawyers Against Unlawful Surveillance



CONTACT:

Council of Bars and Law Societies of Europe
Conseil des barreaux européens
Rue Joseph II, 40/8
1000 Brussels
T +32 (0)2 234 65 10

Follow us on
www.ccbe.eu
ccbe@ccbe.eu

Cover illustration / *illustration de la couverture*:
© Rzoog - Fotolia.com

TABLE OF CONTENTS

INTRODUCTION

1

The requirement for lawyers to keep confidential their communications with, information received from, and advice given to their clients (whether expressed in terms of an obligation of professional secrecy or legal professional privilege), is an essential component of the rule of law in a free and democratic society. Yet it is a value which is coming under increasing threat, whether by means of unlawful interference by third parties or, in some cases, inadequately regulated governmental surveillance.

In relation, particularly, to governmental surveillance, in May 2016, the CCBE issued its Recommendations on the protection of client confidentiality within the context of surveillance activities in order to inform legislators and policy makers about standards that require to be implemented and maintained in order to ensure that the principles of professional secrecy and legal professional privilege are not undermined by practices undertaken by the state involving the interception of communications and access to lawyers' data for the purpose of surveillance and/or law enforcement.[1]

It is, however, recognised that there is a danger that, in some jurisdictions, regulatory controls on governmental surveillance may not be fully adequate, and, everywhere, there is the danger of unauthorised or unlawful interception by third party actors. Therefore, the present Guidance is intended to provide some practical guidance to European Bars and Law Societies as to measures which might be taken by individual lawyers and law firms to ensure the adequate protection of material falling under legal professional privilege, professional secrecy and relevant data protection obligations.

The Guidance is addressed to the CCBE's member bars and law societies, who are invited to consider whether to incorporate the advice given here (so far as relevant to the circumstances of their respective jurisdictions) in guidance to their respective members.

This Guidance is divided into two parts: the first, a high-level overview of how lawyers might approach IT security issues, and the second, more specific guidance concerning the kind of technical measures which might be taken by lawyers to protect themselves against unlawful surveillance or other interference with their IT systems.

1 http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/SURVEILLANCE/SVL_Position_papers/EN_SVL_20160428_CCBE_recommendations_on_the_protection_of_client_confidentiality_within_the_context_of_surveillance_activities.pdf

OVERVIEW
HOW TO IMPROVE THE LEVEL OF IT SECURITY OF LAWYERS

2

1. Ensuring confidentiality as a core principle of the legal profession

The "Charter of Core Principles of the European Legal Profession"[2] states that it is the duty of the lawyer to keep clients' matters confidential and to respect professional secrecy. Observing confidentiality is both an obligation of the lawyer, and a fundamental human right of the client, to be respected by everyone.

The extent to which individual states have adopted regulatory frameworks which guarantee that principle is variable, and in a number of jurisdictions, governmental surveillance may pose a potential threat to that principle.

In its 2014 "Threat Landscape" report, the European Union Agency for Network and Information Security ("ENISA") emphasised that *"privacy violations, revealed through media reports on surveillance practices have weakened the trust of users in the internet"*.[3] Furthermore, the European Parliament resolution of 12 March 2014 on the *US NSA surveillance programme, surveillance bodies in various Member States and their impact on EU citizens' fundamental rights and on transatlantic cooperation in Justice and Home Affairs* contains in its conclusions that it is *"crucial that the professional confidentiality privilege of lawyers […] is safeguarded against mass surveillance activities"* and *"any uncertainty about the confidentiality of communications between lawyers and their clients could negatively impact on EU citizens' right of access to legal advice and access to justice and the right to a fair trial."*[4]

For the same reasons, the CCBE has repeatedly given voice to its deep concern since 2013 that such practices undermine not only the core value of the legal profession, but also the trust in the rule of law, culminating in the publication of its May 2016 *Recommendations on the protection of client confidentiality within the context of surveillance activities*. Notwithstanding the presence of the risk of both governmental surveillance and unlawful third-party access to IT systems and data, it is impracticable for lawyers to conduct their practices without resort to IT systems, including access to emails and the internet more generally. Indeed, as the use of the internet and the adoption of cloud computing solutions by clients continues to grow, lawyers may find themselves under considerable client pressure to use such systems themselves.

The Code of Conduct for European Lawyers sets out obligations for lawyers to respect the confidentiality of information, and at the same time requires that lawyers should maintain and develop their professional knowledge and skills.[5]

It follows from these requirements that there is an increasing imperative on lawyers to acquire those skills which may be necessary to ensure the protection of confidential client information in the virtual environment.

It is therefore the purpose of this Guidance to address what bars and law societies can do in improving the IT security of lawyers by way of informing their members (including, in particular, sole practitioners and small law firms, who may not have access to the same technical expertise as is available to larger firms) of some of the available options which may be open to them. The Guidance, however, is not intended to cover the technical use of specific tools, or to make detailed recommendations as to the particular IT infrastructure or products in which bars, law societies and lawyers should invest.

2 http://www.ccbe.eu/fileadmin/speciality_distribution/public/documents/DEONTOLOGY/DEON_CoC/EN_DEON_CoC.pdf
3 https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014
4 http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2014-0230
5 See Code of Conduct for European Lawyers 2.3.2, 2.3.4 and 5.8.

2. Knowing the basics of IT Security

Investment in IT security systems, protection tools and encryption tools may be necessary for lawyers, but it is not, of itself sufficient, without a good working knowledge by the lawyer of the environment in which such tools are to sit. For example, it is pointless to use tools of encryption if the attacker has gained control over an endpoint where there takes place decryption and the storing of information in an unencrypted form.

Therefore, a certain level of minimum knowledge of IT security is an important basic skill for any lawyer working with or relying upon IT systems. Even if the lawyer chooses to delegate or sub-contract to technical experts the taking of specific measures to ensure IT security in general or confidentiality in particular, there is still a minimum level of knowledge and competence that requires to be incorporated into the way law practices are managed. If not, the lawyers in the practice will be personally responsible for lack of IT security controls, as they would also be in respect of the lack of internal controls for managing clients' funds or documents.

Therefore, before considering technical measures, it is necessary to stress the need to ensure a common minimum knowledge level of IT security for all lawyers.

3. Building on common experience

The obligations imposed upon lawyers with regard to IT security by the law of the European Union are in general terms and tend to be seated in the specific context of data protection, for example the requirements of Article 17 of the data protection directive of 95/46/EC. Neither the new General Data Protection Regulation, nor the draft Network and Information Security Directive is expected to change this legislative approach in the near future. Accordingly, the technical achievement of the legally mandated standards of data protection is not to be found in formal legal requirements, but requires to be found elsewhere, such as in recognised industry practice and formal standards.

However, it is not the purpose of the present Guidance to get bogged down in the detail of specific IT solutions. It is recognised that, because of the wide variety of IT systems and tools in use, it would be pointless to discuss technical details in this document.

Rather, this document starts from the wider proposition that a useful starting point is the general approach to IT security that other professions and sectors have already taken, which is to apply, as appropriate, the recognised standards already used in IT security. As well as being sensible in its own right, it has the incidental advantage that the ability of a lawyer to demonstrate that he is following standards that are already applied in other sectors tends to lead to an increase in the confidence of clients that the confidentiality of their client data and communications is protected.

Furthermore, it a) helps lawyers to compare their own level of IT security with that of other professions and sectors; and b) facilitates reuse of experiences, policies and applicable technical details (controls) already used in other sectors.

Accordingly, bars and law societies should assist lawyers in acquiring a good understanding of the usefulness of relevant IT security standards, without necessarily obliging all law practices to be certified against these standards. Indeed, since IT security standards are formulated at such a generic level that only experienced IT security specialists can apply them directly (and in many instances IT staff employed by law practices may lack the appropriate expertise) the purpose of raising awareness of the standards amongst lawyers is not to require lawyers to be certified against those standards, but rather to provide an insight into the sort of systematic and

structured approach which might be taken.

Further, based on the minimum requirements set out in part II of this guidance, bars and law societies are recommended to:

- examine in reasonable detail the state of play of the IT security readiness of lawyers within their jurisdiction;
- where appropriate, issue recommendations to their members which translate, convey and if necessary, localise requirements set out in this Guidance and the relevant IT security standards;
- publicise the relevant standards and explain them to their members;
- make sure that any recommendations or guidelines which they may issue are in compliance with the relevant IT security standards;
- seek to ensure the compliance of their members with such recommendations or guidelines.

Some bars have already addressed one or more of the issues set out above,[6] organised specific training, or published books on this subject.[7] Materials such as this provide a practical starting point or benchmark for other bars and law societies in Europe.

It is underlined that steps taken in this field are not only beneficial to individual lawyers, but more importantly, to their clients. Therefore, bars and law societies should consider when they publish such guidelines to their members, whether also to inform the general public and clients of the guidelines or recommendations by promoting the existence of such guidelines, bars and law societies can make clients aware of the fact that lawyers continue to take the protection of confidential client information seriously, regardless of the channel used for communication.

6 E.g. Conseil National des Barreaux, http://cnb.avocat.fr/Securite-de-l-information-au-sein-des-cabinets-deux-guides-mis-a-disposition-de-la-Profession_a1191.html, practice notes from the Law Society of England and Wales e.g. at http://www.lawsociety.org.uk/support-services/advice/practice-notes/information-security/, or the Hungarian Bar Association at http://www.magyarugyvedikamara.hu/common/file-servlet/document/898/default/doc_url/160113_Utmutato_IT_biztonsaghoz_kamarai1096398_1.pdf

7 E.g. Cyber Security Toolkit by Peter Wright, published by the Law Society Publishing, or The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms and Business Professionals.

TECHNICAL MEASURES AGAINST UNLAWFUL SURVEILLANCE

3

1. An overview of applicable IT security standards

There are numerous different global IT security standards. Some of these standards are well-known, but do not provide a suitable framework to govern the manner in which individual professions, such as lawyers, might effectively be enabled to ensure a high level of IT security. For example, the well-known Common Criteria (CC) standard is about defining protection profiles for specific categories of use, e.g. for the encryption of USB flash drives, for ATMs or for electronic signature creation applications etc. and beyond protection profiles, about evaluating whether certain specific products and systems ("security targets") comply with such profiles or not. Therefore, this is more about ensuring that a specific product or system complies with specific, predefined requirements, such as generic commercial IT security. For that reason, this standard, though of some interest to lawyers with regard to general security related equipment and products (USB flash drives, smartcards, firewalls etc.) which the lawyer may be using, it will be appreciated that it does not provide an appropriate benchmark for the issues dealt with in the present Guidance.

Another widely used global standard is COBIT (Control Objectives for Information and Related Technology). This standard currently has a very wide scope, and defines itself as a framework for the governance and management of enterprise IT, including the management of IT security. Considering its scope, this standard seems only relevant for organisations which have a complex IT infrastructure, and which are in a position to adopt it as a holistic approach to IT, and to translate business requirements into IT requirements, or so as to ensure the retention of managerial control over IT functions. This standard clearly has a rather different focus than the problem the majority of lawyers and small practices currently face.

Thus, it will be seen that, out of the small number of global IT security standard families, only two are applicable to managing the IT security risks of lawyers, namely:

(a) FIPS 800-53 and FIPS Cybersecurity Framework (and related standards) by NIST[8]

(b) The ISO 27000 based standards.

It is the purpose of Part II of this Guidance to make more detailed recommendations drawing on these standards. In particular, section 7 provides a more detailed example of treating one specific aspect of risks, namely, the confidentiality of client-lawyer communications.

a) The NIST Standards

The standards issued by the National Institute of Standards and Technologies of the United States of America (NIST) are more accessible and can be used as a starting point for future discussions of IT security frameworks for lawyers. The standard, *NIST Special Publication 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)* covers generic security controls for federal IT systems. It is a very detailed, well-known and much used standard, but perhaps it has too much detail for the size of an average European law firm. Also, evaluating conformance to this standard can also be a difficult exercise for such practices in the European context. Another, more generic and concise US framework is the *FIPS[9] Cybersecurity Framework (and related standards)[10]* (also issued by NIST), which is more suitable for use by smaller organisations, such as the typical law firm. There is the additional advantage that there has already been published practical draft guidance for small firms.[11]

8 FIPS Cybersecurity Framework. FIPS 800-53: NIST Special Publication 800-53 Revision 4, April 2013, Security and Privacy Controls for Federal Information Systems and Organizations.
9 FIPS is an abbreviation for „Federal Information Processing Standards".
10 http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf
11 NIST Small Business Information Security: The Fundamentals, http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf.

b) The ISO Standards

Last, but not least, there is an ISO equivalent for the implementation of IT security management standards, the ISO 27000-based standards, which includes standards against which organisations can receive certifications like for ISO 9001. Also, sufficiently detailed technical guidelines have been published, such as ISO 27002, and a number of guidelines for smaller companies.[12]

The standard families indicated above have the same philosophy behind them, but there are slight differences in the levels of detail, their intended audience and the way conformance with these standards is proven.

Of course, the number of IT security standards is a lot higher than the ones presented above, and their scope covers a wider area than has been highlighted above. However, most of these IT security standards fit into one or more of the above frameworks as covering a special aspect of the more generic IT framework.

2. Essential minimum steps for an effective security management system

In order to develop a basic information security system, a law firm or sole practitioner should start – taking into account the area of law in which the firm practices, its usual clientele, and the skills of its staff – with the following steps:

- Identify its key information assets, especially client information and documents, key services, and registries that are critical to its operation.
- Based on the identification of such key assets, the law firm should also identify those security failures that would have the most severe impact on the business of the law practice (taking also into account the probability of such security failures occurring, and, if they did what would be the consequences of such security failures), and identify what kind of options it has for the minimisation of such risks.

The advantage of basing the assessment on IT security standards becomes apparent when addressing possible ways of treating risks, how to approach the possible treatments, and what categories of treatment to start with. Such options should cover, at a minimum, the following aspects:

- controlling access to key information assets (including identification of users of IT systems and granting them only necessary access rights),
- defining physical security areas with controls,
- secure disposal and removal of equipment (including mobile devices and non-mobile data carriers) and off-premises security of equipment,
- network security (especially use of shared infrastructures like wireless and wired networks),
- operational procedures to ensure protection against malicious code,
- management of passwords, back-up, reporting of security incidents etc.[13]

Measures set out in section 7 below provide a more detailed example of treating one specific aspect of risks i.e., the confidentiality of client-lawyer communications.

12 See e.g. "ISO/IEC 27001 for Small Businesses: Practical Advice" by Edward Humphreys, published by ISO in 2010.

13 Treatment of such risks include the list of "Guide de sécurité de l'information pour les avocats", or the document of NIST Small Business Information Security: The Fundamentals at http://csrc.nist.gov/publications/drafts/nistir7621-r1/nistir_7621_r1_draft.pdf, and of course, the longer lists in ISO 27002 and NIST FIPS 800-53.

3. IT security controls in relation to mobile devices (see control 6.2.1 under ISO 27001)

One particular aspect of the risk analysis called for above is the special risk attendant on the use of mobile devices.

Mobile devices, like laptops, tablets and mobile phones are exposed to various risks, all related to the loss of control over the asset itself. These tools are used outside of the well-controlled office environment. Therefore, there is an increased risk of losing, damaging or compromising the device or the information on the device. If a malicious person gets hold of one of any of these devices, he will be able to launch a very wide range of security attacks.

Mobile devices require more security controls than devices kept in the office. It is not absolutely necessary to encrypt mass storage in a desktop environment, but for a laptop it is certainly required. In the absence of appropriate and effective protective measures, the data medium of the mobile device can easily be obtained through the use of basic tools, regardless the strength of our user password. Therefore, although a secure password can protect resources accessible through a network, data on removable media can effectively be protected only if it is also encrypted. This applies also to all mobile devices including mobile phones, USB flash drives and of course, laptops. Access-controlled encryption is widely available for all such devices and is easily affordable.

Furthermore, given the risk of theft of the device, additional physical protection measures may require to be implemented, for example, the use of a pocket-sized lock which may be used to protect laptops from being snatched (grab-and-run thefts), and such elementary precautions as the packing of mobile devices in hand luggage rather than in checked baggage.

Besides the physical protection of such devices, lawyers should be careful of what network resources are used for connecting to their remote services or storage locations. Smart phones and tablets may pose a particular risk as there may be a tendency by users to implement fewer security controls than are applied to the use of laptops, even though the risks are similar. It should be noted that it is possible to install antivirus software, firewalls and protection against harmful websites on mobile devices (and, as mentioned above, also to encrypt the data on them). However, such software is not usually included when a mobile device is bought, and therefore the acquisition of such software requires to be budgeted for, licensed, installed and configured by the user.

4. IT security controls to protect against malware (control 12.2.1 under ISO 27001)

Malware takes many forms: viruses, worms, Trojans, backdoors, rootkits, but the exact categorisation of a piece of malware is not relevant for the purpose of the present Guidance.[14]

Malware can seriously harm or destroy computer resources, provide unauthorised access to stored data (for any malicious purpose) or for instance send to clients embarrassing messages apparently originating from the law firm.

These codes can infect computers in numerous ways, called attack vectors. An infection can still occur through the usage of infected removable media (e.g. USB flash drive), but typically these harmful codes are nowadays coming from a greater distance, constantly looking to find their

14 For more background information see point 2 of this guide: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

newest “victim”. They can infect resources by using previously gathered email addresses[15] or other computer connections (network services). Quite often attackers lure unsuspecting users to seemingly exciting or useful websites. Of course these harmful codes can be led by active reconnaissance as well, for example by attempting to scan network addresses.

After having acquired such addresses, the attacker, based on trial and error, can quite effectively find a random IT vulnerability on the targeted device, which vulnerability will then allow unauthorised code to be run on the device.[16] Unfortunately, there is no such a thing as a virus free platform for consumers and similar grade business users.[17]

The most important line of defence for a law practice is using a proper anti-malware software. In order to make the right decision on which anti-malware to buy, not only the price that can be afforded needs to be considered, but also the results published by independent European test laboratories on how effective the defence of a certain malware program has proven to be.[18] It seems trivial, but in case of anti-malware it is still surprising to see that it is not always the most promoted and easy-to-use software which will provide the best protection.

Anti-malware software should be installed not only on desktop and other fixed equipment but also on mobile devices such as tablets and smartphones if client data or other important legal information is stored on such devices.[19]

Antivirus software cannot grant protection against all attacks. According to the above mentioned laboratories, detection rates over 99 % can be achieved by defending against malware already identified and analysed by anti-virus software companies. However, a significant period may elapse between the appearance of a piece of malware and its registration in antivirus software, and a general strategy of targeted attacks (hacks) is to exploit a vulnerability which has not yet been addresses by an anti-virus software update or not yet been fixed on the targeted computer. Such vulnerabilities are known as zero-day vulnerabilities.

If the infection has already happened and the anti-malware software is unable to rectify the infection, lawyers are advised to ask for professional help before restoring the former data from backups, otherwise the malware may still be active and corrupt restored data as well. It is also necessary that law firms should require their users to report any such incidents.

Protection against malware leads to the delicate question of when to update software. Software manufacturers often provide updates to fix the latest vulnerabilities which have been discovered. So the prompt installation of all updates and repair packs will significantly reduce exposure not just to malicious codes, but also to targeted IT attacks. However, installing updates brings the danger that, rather than remedying the software in question the installing breaks software that previously was working without any problem. For this reason, larger firms, who have sufficient resources, should first test any updates in an appropriate test environment, rather than on a computer which is used for client business.

15 By sending harmfuls codes in attachements, or by directing people to a dangerous website address with included malware.
16 The software vulnerability that can be used for unauthorisized information gathering or for running unauthorised codes, is called an “exploit”.
17 The difference in the ratio of successful attacks quite often derives from the fact that malicious codes need to be programmed for a certain type of device, therefore less used systems will be less popular for malware attacks
18 https://www.av-test.org/en/antivirus/, http://www.av-comparatives.org/dynamic-tests/, https://www.virusbtn.com/vb100/latest_comparative/index
19 See under one of the reports about the Android devices: http://www.av-comparatives.org/wp-content/uploads/2015/09/avc_mob_2015_en.pdf

5. Controls regarding the secure disposal of media used by lawyers (8.3.2./10.7.2. under ISO 27001)

Since client data is amongst the most valuable assets of lawyers, such data must be protected, even after the data is no longer needed. Erasure or other destruction of such data has to be secure as well.

Both data storage devices (USB flash drives, external hard drives), and built-in media (e.g. SSD/ flash memories) store client data. This has to be kept in mind when these devices are made available for servicing, or when disposing or selling devices that are no longer needed. Lawyers have to keep in mind that such data are stored by not only computers, tablets and smart phones, but also photocopying equipment, scanners and fax machines.

Simply deleting stored data or formatting the device will not stop a determined person from restoring the data, so either special deletion mechanisms should be used when transferring media outside the organisation or such data carriers should not be sold or disposed of at all.

6. Overview of categories of surveillance activities and associated risks (see e.g. network controls and cryptographic controls under 13.1.1. and 10.1.1. controls of ISO 27001)

In order to get an overview of what tools might help lawyers in improving the state of IT security in relation to unlawful surveillance, there is outlined below a number of scenarios listing different categories of (1) surveillance activities, (2) surveillance risks and (3) situations where lawyers are exposed to such risks. The focus of the Scenarios is an analysis of measures to identify and protect against the risk of unlawful surveillance. Due to the existence of extraterritorial jurisdiction (which is not exceptional e.g. under criminal law or competition law), situations could arise where an act of surveillance to be carried out by authorities of one country is lawful in that country, but it is not lawful in all the countries affected by the surveillance (e.g. in the country of the other party to the communication).

Normally, these differences should be reconciled by the use of traditional methods of international cooperation between law enforcement and national security agencies, but clearly, this does not always happen. Even within the EU, member states may carry out operations in support of national security which may be against the interests of and/or the laws of the other member state concerned. In such cases, preparing protective measures against governmental surveillance might be justifiable as a legitimate, desirable and meaningful act, provided, of course, that it is technically possible. Even if a provider of an electronic communications service (**"ECS"**) is required by its domestic law to provide access to the communications carried out using its network or service, that does not necessarily mean that the surveillance measure will be lawful in all cases. Therefore, and for these reasons, such situations are also included in the following analysis.

1) Categories of surveillance activities

a) Surveillance activities based on the provision by service providers of access in advance to a specific infrastructure to bodies entitled to carry out surveillance activities under their national law.

b) Surveillance activities based on a specific legal process of surveillance, for example the obtaining of warrants or other external authorisations. A distinction might be drawn between access to content data and metadata, but it should be noted that data is increasingly being interpreted as metadata and more and more data can be collected from the metadata relating to communications, including lawyers' communications with clients. Therefore, from the perspective of confidentiality, the practical difference between metadata and content data is minimal, and in both there is represented the same level of threat to client-lawyer communication.

c) Surveillance activities applied in an untargeted and indiscriminate manner on an entire population or a substantial part thereof (Bulk" or "mass" surveillance). This is a form of surveillance which has only recently become technologically possible.

d) Targeted surveillance activities involving intelligence gathering on specific individuals or groups of individuals. For the purposes of the present Guidance, this is referred to as "targeted surveillance". However, the boundary between bulk or mass surveillance and targeted surveillance is ill-defined and subject to change, especially when under judicial scrutiny. For example, when a tribunal says that "*indiscriminate trawling for information by interception, whether mass or bulk or otherwise, would be unlawful*",[20] then the most important question will be what kind of "selectors" would make a surveillance lawful. It is suggested that the surveillance in question would be targeted surveillance only when at least one subject of the surveillance is identified in advance, before the surveillance starts.

2) Surveillance risks

From the viewpoint of a lawyer, the following different categories of risks should be identified.

a) Recording a conversation without either participant's knowledge (either with or without the help of some or all service providers participating in the technical conduct of the online or offline electronic communication, for example, with the help of the internet access provider, or a third party provider of email or other electronic message delivery systems).

b) Recording metadata related to the conversation (identifier or identity of parties, time, duration, length/size of messages, location of parties, IP or physical addresses of access etc.)

c) Accessing end user communication **devices** (smartphone, computer) and thus recording communications or related metadata at the end user side, or recording/ accessing logs and other metadata (conversation history etc.) stored on the end user device.

d) Accessing data by way of **recovery** from equipment which has been **disposed** of or from **data carriers**.

e) Accessing non-conversation data, e.g. stored documents, research or usage history.

20 Investigatory Powers Tribunal Libery et al. vs. GCHQ 160 (ii) at http://www.ipt-uk.com/docs/IPT_13_168-173_H.pdf.

3) Usage scenarios

The following list enumerates the main usage scenarios which present potential surveillance risks:

a) Lawyer communicating with a client or another lawyer (including by "normal" office telephone, VoIP or by OTT providers such as WhatsApp etc.);

b) Lawyer sending an email to a client or another lawyer;

c) Lawyer sending documents to a client or another lawyer using technology other than email;

d) Lawyer using e-government/e-court solutions for sending, receiving and storing communications (e.g. court submissions);

e) Lawyer storing/retrieving files, documents and records electronically (not sending to third parties);

f) Lawyer doing legal research;

g) Lawyer disposing of IT equipment posing security risks (phones, computers, and also faxes, scanners, printers and photocopiers using memory or hard disks);

The first part of the following analysis, will look at characteristics that are common to most of the above scenarios, and the second part will review special characteristics of relevant scenarios.

7. Ensuring the confidentiality of communications – specific surveillance risks and possible counter measures

Risk 1: Recording of conversations and related metadata

Depending on the technology and services used, a certain degree of protection of the conversation is usually present. However, communications often pass through different network segments with very different capabilities and different dangers. The local loops of traditional telephone calls are protected only at a physical level (e.g. in locked cabinets), which protection can easily be circumvented within buildings.

a) Recording by way of service providers

There is a certain required level of protection of conversations set out in services which are subject to well-defined standards for example, within the infrastructure provided by wireless technology (such as UMTS and LTE). At the same time, providers of such services may also be required to grant to governmental agencies access to otherwise protected conversations. In the EU, networks and services authorised under the 2002 regime of "electronic communications" are required to enable legal interception (see under Directive 2002/20/EC Annex A.11), and failure to do so enables most national authorities to stop the provision of the service or network. This includes landline and mobile telephone services and internet access.

However, services building upon already existing internet access are not regarded as "electronic communications" services. Thus, although email and instant messaging (chat), are regarded as electronic communications, services such as Skype, Viber or other similar services using "inapp" calls are not always considered as electronic communications services in all EU member states (in this paper, these are referred to as "OTT services").

Some law enforcement or national security agencies have succeeded in convincing some OTT service providers to cooperate with them, and provide them with practically the same level of access as with a traditional electronic communications service. However, if the OTT service provider has no technical presence at all in a country (for example, they have only a sales staff), it is very difficult for most agencies to put pressure on such providers if they do not want to cooperate. Accordingly, agencies require to turn to international channels of coordination and cooperation. Further, by law, an OTT service provider is not required to have a specific capability for enabling interception at its own cost. Therefore, where an OTT service provider does choose to co-operate, it might be more successful in transferring the costs of legal interception to the governmental agency requiring it.

Using OTT services having a physical presence only in other jurisdictions can serve as a kind of protection measure against targeted surveillance by local agencies, provided that cooperation is not very strong between the jurisdictions. At the same time, one has to keep in mind that the most popular OTT service providers are physically located in countries where – at least based on anecdotal evidence – the risk of bulk surveillance is the most prominent. It is also important to note that all OTT services can be recorded at the level of the internet access provider and a local mobile network operator or landline internet service provider can of course easily record emails for the purposes of legal interception.

Possible counter measures

The implementation of protective measures against surveillance may have an impact on the ease of use or effectiveness of the service. This may be a matter which would require to be borne in mind, though primacy ought to be given to the deontological obligation to seek to ensure confidentiality.

a) Encryption of communication as a protection

One solution could be the use of encryption for conversations. The methods of encryption are many and diverse, so one has to dig deeper to understand what is encrypted and what is not. For example, although even second generation mobile calls are encrypted between the end user device and the base station, this encryption is weak against even a dedicated private attacker with some resources. Even if a service provider markets its service as being encrypted, the provider may still have access to the keys of encryption, thereby rendering a given conversation secure only so long as the provider is not forced to cooperate with enforcement agencies.

Nevertheless, there are end user devices (e.g. telephones, PBX) providing end-to-end encryption between compatible devices, encrypting both traditional phone calls as well as OTT calls.[21] However, it is important to note that:

- not all of these solutions are without a “legal backdoor” for governmental agencies to access;
- for end-to-end encryption to work, both ends have to use compatible devices; and
- in certain countries, even within the EU, the importation or sale of such products may be restricted on national security grounds.[22]

End-to-end encryption can be provided by running special software on a smartphone or tablet.[23]WhatsApp and Viber have also made it possible (or even provided a default option) for the software used for accessing their services to incorporate end-to-end encryption of conversations.

21 http://www.cryptophone.de/en/products/mobile/, the Blackphone at https://www.silentcircle.com/products-and-solutions/devices/, http://www.bull.com/hoox etc.
22 E.g. importing and selling Cryptophone in Hungary is prohibited based on security grounds.
23 E.g. see other products of Cellcrypt, Chatsecure, Signal Private Messenger, Silent Circle, wickr etc.

Most of the software only solutions will not use traditional mobile numbers for call routing or messaging.

Also, when using a software only end-to-end encryption, the conversation can still be prone to attacks at the level of the operating system or software environment running on the device (e.g. Android) (see below in more detail under "Accessing devices").

As for risk of legal backdoors in devices or the risk of unreliable promises made by electronic communications services providers, it is very difficult for lawyers to do anything about this at an individual level, just as it is impossible to take measures against backdoors at the level of network equipment or an unreliable certification authorities publishing e.g. SSL certificates to an attacker.

b) Using non-registered telephones for communications or telephone where subscriber/ user data is outdated

As has been widely reported, during the terrorist attacks at Bataclan, France, the perpetrators, rather than using encryption, merely used throwaway phones for communication. Since in most member states, one can buy new SIM cards without providing identification of the user and there are prepaid phones where previous users are not forced to register the transfer of the subscription to a new user (indeed, in some member states there are no regulatory or other mechanisms which would make this possible), this option will be open to mitigate surveillance risks as well.

b) Recording metadata of conversations

The most important difference between recording of the metadata and recording of the conversation itself is that usually no warrant or other external approval is needed for a governmental agency to have access to such or all metadata of a communication (and therefore, also the "paper trail" of the surveillance will also be minimal.)

Possible counter measures

Most of the metadata of conversations created during the provision of a service can be recorded by the service provider, unless the provider specifically elects to exclude the recording of such data. It is technically not possible for a lawyer (or anyone else) to prevent the recording of such metadata. Even when using end-to-end encryption, if a lawyer calls a traditional telephone number, all important metadata will be recorded at the service provider, including the number called, the length of the call etc.

So if this is seen to be a problem, the lawyer would require to avoid using that method for communication, and use OTT services instead.

Risk 2: Accessing devices

As stated above, even end-to-end encryption may be useless if the attacker has access to the end user device itself.

Due to the large variety of different software which could be installed on a large number of possible devices, the greatest risks are software vulnerabilities, i.e. errors not fixed in some elements of the software environment used on the device concerned. An attacker could exploit these vulnerabilities to gain unauthorised access to functionalities of the device and thus take control of the device, including recording calls, or accessing logs containing important metadata.

Malware (viruses, worms etc.) present on a device can also grant the same unauthorised access to attackers. This malware could be installed accidentally, including through malicious websites accessed on the device.

Last, but not least, having physical access to a device may provide attackers with such capabilities.

Possible counter measures

Such risks can be decreased by using the basic IT security hygiene set out in the recommendations above and by restricting physical access to the device, or by changing devices at appropriate intervals. Enabling password based locks of devices and encryption of data contained on such devices prone to being lost, is a minimum precaution of some importance which should be undertaken by all lawyers regardless of whether they seek protection against surveillance or not. Of course, strong passwords should be used and changed frequently.

Risk 3: Data previously deleted

Lawyers and law firms frequently have to dispose of certain IT equipment that contain non-volatile memories or data carriers (data mediums), like telephones, laptops, computers. Modern scanners and photocopiers quite often have built-in memories or hard disks.

Unless such equipment is disposed of in a proper way, anyone having access to such data carriers can restore considerable parts of the data stored on the devices, even if the data had previously been deleted.

Possible counter measures

It is important that lawyers either ensure that all data on such data carriers are overwritten before disposal, or that data carriers are physically destroyed or that all data carriers are retained for security purposes (and not resold). Most office grade paper shredders are capable of the physical destruction of CDs and DVDs, but destruction of hard disks and SSDs may be relatively costly.

If data carriers are destroyed outside the premises of the lawyer by a third party, it is advisable to request a certification from the third party that the destruction was indeed carried out.

Risk 4: Accessing non-conversational (stored) data

Data unrelated to conversations, such as data stored at the law firm's premises or with a third party is at similar risk of surveillance as data which does relate to conversations. Usually, access to such data at the law firm's premises by a governmental agency is subject to extra regulatory safeguards (e.g. warrants). However, access to data retained by a third party for a lawyer is quite often not subject to the same regulatory safeguards as would apply to the premises of a law firm, and the service provider will not necessarily recognize the information as privileged.

Possible counter measures

Even if transit from the law firm to storage is protected by a method such as SSL encryption, use of storage services enabling so called "client side encryption" is advised.[24]

However, it is of utmost importance that in such cases the lawyer also arranges for safekeeping the password or other security mechanisms (i.e. tokens) used for accessing the encrypted data. People have become accustomed to being able to access to a resource even if they have lost their password by providing an alternative, reliable way of authentication. But that is not the case with encryption: should the lawyer loose such password, the service provider will have no technical means to provide access to the encrypted data, so the data encrypted will surely be lost.

24 E.g. SpiderOak, TresorIT.

8. Recommendations regarding certain communications technologies

a) Security of access networks

Although the use of wi-fi networks is widespread, care should be taken by a lawyer when using these for access. In general, wi-fi is not really suitable for professional uses involving handling confidential information, unless there is an extra security layer of end-to-end encryption similar to that employed when using VPNs.

Without such an extra encryption layer, a lawyer should not use a wi-fi without the most basic access control for sending client information. If such precautions are not taken, anyone (anonymous people, machines) in the vicinity can view and record the complete data traffic.

Furthermore, just because a network is protected by a password, that alone will not make it more secure than "open" wi-fi networks. If an unidentifiable attacker can also join the same network, because the password is shared (for example, with everyone within visibility range, or who may have used the network in the past), that attacker will have the same opportunity of viewing the data traffic of the lawyer as with a passwordless wi-fi network. Therefore, lawyers should refrain from using wi-fi without a VPN if it cannot be ascertained that the password for the wi-fi has been changed in the last one or two days.[25] Reliable and secure authentication of "guest users" is somewhat complicated and, no doubt due to that, very rare.

Using mobile internet is safer than using Wi-Fi, but the former is not always an option when abroad.

The safest solution is to establish a VPN network connection between the mobile device and the office, or another sensitive mobile IT resource.

This is also an important issue to remember when lawyers provide their clients with (free) Wi-Fi access at the lawyer's office – the law firm might unknowingly put its clients' data at unnecessary risk when doing so. The Wi-Fi connection offered to clients must not be the same as the one which is used in the office. The difference between the two networks should be explained to all members and employees of the firm and they should be asked never to use the client Wi-Fi access for office use. Moreover, lawyers should offer Wi-Fi access to their clients only if they can assure the appropriate protection and trustworthiness of the network.[26]

Sole practitioners and smaller law firms should keep in mind that if they use a wired network (e.g. Ethernet) provided by their landlord (e.g. in serviced office environments), they should verify with their landlord (or, preferably, with an IT expert) whether the LANs of each tenant are securely separated from each other. If other tenants are able to access the law firm's computers, these computers and the client files on it are at considerable risk, even if an everyday user may not be aware how such access might be obtained.

b) Email messages

Email messages used by law firms can be recorded in a number of ways, by either the provider of a local access network at the sender's or recipient's site, the sender's or recipient's internet access provider (if they are not the same as the provider of the local loop), by the provider who grants access to the emails, or the one who relays the emails to be sent to the recipient.

25 The attacker can intercept the communication between the Wi-Fi access point and the device in use when enering the shared and jointly used passwords. But it is not as easily done as in the case of an open Wi-Fi network. (WPA PSK).

26 Instead of using a Wi-Fi connection without or a single shared password, we can use a hotspot access generator system can be used, for example. http://www.zyxel.com/us/en/products_services/uag50.shtml.

From the viewpoint of governmental surveillance and the obligation of the service provider, the email providers are more like OTT providers, and are not a priori subject to sophisticated requirements of recording and retaining emails according to the needs of surveillance agencies – at least, not until they are approached by these agencies to provide these capabilities. Regardless, granting access to emails should always require an external approval (e.g. judicial warrant) for the surveillance agencies.

More and more often, the connection between the email service provider and the local client software is secured by SSL encryption. However, that will not necessarily mean that when the provider forwards the message to the recipient's provider or to interim providers, the message will stay encrypted. In future such encryption might become more commonplace, but given the large number of email service providers and their different configuration, it is very difficult to ensure end-to-end encryption of emails without sacrificing the capability to deliver the message everywhere.

From the viewpoint of legal assurances for client-lawyer communications, using an in-house email service managed by the law firm, should provide more legal protection. However, in practice, for the majority of law firms, operational and technical security and reliability would probably suffer more as a result of this "homemade" approach then what the extra additional legal assurance can provide. Untargeted bulk surveillance of emails is technically possible for the largest providers of email services.

For that reason, it is important that the capability to use end-to-end encryption of emails is already built into most of the email clients ("mail user agents"). Also, considering that a large number of European lawyers have access to X.509 certificates for electronic signature (and similar certificates for encryption), the security of emails could considerably be improved within the EU if there was an easy-to-use and reliable directory of the encryption certificates of lawyers.

If such encryption is not possible, because, for instance, it was desired to send an email to a client without any encryption certificate, it would be better to encrypt the most important client information in an attachment, and send a one-off password to the client using a different channel (e.g. SMS or phone, and not by email).

c) Electronic court and e-government procedures

More and more often, lawyers have to use electronic transmission facilities provided by court authorities in order to submit and receive documents. When using such solutions, there is a risk of unauthorised access from third parties or from foreign governments. Encrypted transmission of documents and encrypted storage is an important protection measure, but more often, these facilities can only be ensured by the state-side provider granting access to its system. In certain member states, the bars or law societies may provide the electronic transmission facilities, with the role of the state being limited to providing the gateway to such facilities. Though this has some advantages, such as keeping control of the system within the profession and providing lawyers with practical solutions tailored to their needs and ensuring that they are provided with full information on their usage and any harmful incidents which may have occurred, it also transfers cost and risk to the bars or law societies which provide the facilities. For this reason, this may not be a solution which would commend itself to all bars and law societies.

CONCLUSION

4

Absolute protection of IT systems against surveillance, lawful or otherwise, and against other forms of hacking cannot be achieved. IT systems will always be vulnerable, and, as this Guidance demonstrate, there is no such thing as a comprehensive system which will give total protection of data. There is a wide variety of security risks to which data held by lawyers and communications between lawyers and clients are being exposed on a daily basis.

Against that background, it is important for lawyers to be able to demonstrate, to their clients, and to the wider public the measures they have taken. An essential component of this is to approach any risk analysis on a structured and coherent basis.

Accordingly, this Guidance sets out a suggested framework on the basis of which Bars and Law Societies might seek to make recommendations to their members as to the sort of systematic and structured approach that might be taken to mitigate the risks. It may be that the suggestions set out in this Guidance could serve as a basis for individual Bars and Law Societies setting out more detailed recommendations or even mandatory requirements applicable to their members, in a manner similar to the regimes in place for the safeguarding of paper documents and face to face communications.

Following this Guidance should not, however, be regarded as a mere "tick-box" exercise. The threats to the security of IT systems are constantly evolving as, indeed, are the IT systems themselves. Even large organisations, which are much better resourced than the biggest law firms have been subjected to security breaches, in spite of their best endeavours to guard against them.

Therefore, the question is not whether IT security breaches can be prevented, but rather as to how lawyers can demonstrate that they have thought about and addressed the issues and taken such counter measures as may be appropriate.