Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10 – F. : +32 (0)2 234 65 11
Email : ccbe@ccbe.eu – www.ccbe.eu

CCBE Statement on mass electronic surveillance by government bodies (including of European lawyers' data)

14/10/2013

Background

The Council of Bars and Law Societies of Europe (CCBE) is the representative organisation of over 1 million European lawyers through its member bars and law societies from 32 full member countries, and 11 further associate and observer countries.

On 1st July, 2013, the CCBE issued a statement (please see also attached as an annex to this statement) on governmental practices involving mass data mining for purpose of surveillance, in which the CCBE expressed its deep concern that a core value of the profession, professional secrecy, known in some countries as legal professional privilege, is at serious risk, and erosion of this aspect of confidentiality will erode trust in the rule of law.

The CCBE statement was based on reports of mass violation of the human rights to private life and personal data, being carried out on a systematic scale by governmental agencies of leading Western powers, including Member States of the European Union. Such allegations indicate clear violations of the Charter of Fundamental Rights of the European Union by certain EU government bodies, mainly article 7[1] and 8[2], and also, due to the lack of any mechanisms for appropriate judicial review, article 47[3]. With regard to the alleged indiscriminate access to, and mass scale surveillance, of most communications between non-US nationals, such access also covered communications between lawyers and their clients. We are of the opinion that this kind of mass surveillance goes beyond risking specific human rights between private persons, and is a threat to the rule of law as recognised in modern democracies.

As of today, no reports have been published by the European Union or its Member States satisfyingly addressing the abovementioned allegations. Without any firm basis for facts on this issue, there is no way to know whether there was any breach of fundamental rights, like Article 8 paragraph 2 of the Charter of Fundamental Rights of the European Union, or Article 12 of the Data Protection Directive (95/46/EC), which also makes any attempt at enforcing such rights impossible. It is the right of each EU citizen to have access to data concerning them, and this also clearly includes the right to know whether they have suffered illicit intrusion in their cyber-privacy by a

---

1 **Article 7 - Respect for private and family life**

Everyone has the right to respect for his or her private and family life, home and communications.

2 **Article 8 - 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.

3 **Article 47 - Right to an effective remedy and to a fair trial**

Everyone whose rights and freedoms guaranteed by the law of the Union are violated has the right to an effective remedy before a tribunal in compliance with the conditions laid down in this Article.

Everyone is entitled to a fair and public hearing within a reasonable time by an independent and impartial tribunal previously established by law. Everyone shall have the possibility of being advised, defended and represented.

Legal aid shall be made available to those who lack sufficient resources in so far as such aid is necessary to ensure effective access to justice.

nation state. It is also a problem that bilateral negotiations with the United States of America on this subject have not been at all transparent to date.

Based on further press reports and the recent hearings in the European Parliament's LIBE Committee, the CCBE is of the opinion that the greatest threats to clients' trust in professional secrecy can be traced back to two sources: a) lack of trust in state bodies with secret investigatory powers (there are concerns that they will use these powers outside the limits of their democratic mandate); and b) an objective lack of technical means at the disposal of law firms to secure effectively professional secrecy.

In all Member States of the EU, professional secrecy of lawyers is strongly protected, although the limits and means of legal protection are different. Both the case law of the European Court of Justice and the European Court of Human Rights acknowledge this right. However, based on certain, recently revealed information regarding the practice of leading state surveillance agencies, concern has arisen that the protection offered by legal measures of EU member states for professional secrecy might not be working in practice.

No trust without confidentiality – repercussions for the Digital Agenda for Europe

The lawyer's role, whether retained by an individual, a corporation or the state, is as the client's trusted adviser and representative, as a professional respected by third parties, and as an indispensable participant in the fair administration of justice and democracy. It is of the essence of a lawyer's function that the lawyer should be told by his or her client about matters which the client would not tell to others – the most intimate personal details or the most valuable commercial secrets – and that the lawyer should be the recipient of other information on a basis of confidence. Without the certainty of confidentiality, there can be no trust. Therefore, if the right of EU citizens and businesses to be protected against any divulging of communications with their lawyers is denied, they may be denied access to legal advice and to justice.

Taking stock of the technical tools at the disposal of law firms, including the largest firms, the CCBE realises that lawyers are currently using systems for electronic communications and for cloud services that are not secure, because we now know they were designed with backdoors that government agencies can open. However, as we have recently learned, even the largest of these government agencies has trouble sometimes controlling the secret information to which they have access. It is evident that the more backdoors there are, the less secure the online infrastructure will be.

If lawyers are using such insecure electronic communications or cloud services, they are *de facto* infringing their obligations as data controllers and in breach of their deontological rules. This problem of having to use insecure communications is not merely a problem of training or culture, but more a problem of all European undertakings, except for the largest ones or those in the defence industry.

As a consequence of these circumstances, lawyers are forced into a situation where they have to choose between the following options:

a) to continue using electronic communications and cloud services that the general public uses, knowing that they are in breach of their obligation towards clients to keep their information confidential, and after calling attention to the risks, simply ask for the clients' informed consent for such hazards; or

b) to use electronic communications services made possible by new investments in building an "EU-only", totally separate internet with strict gateways enforcing all strict policies etc., and thus, rebuilding trust at the EU-level – while also accepting the inefficiency of such solutions, for instance the costs of rebuilding; or

c) not to use email, electronic communications services or cloud services for communications with clients, exchanging data only by way of physical data carriers like flash drives, or relying on typewriters and postal and express delivery services.

It may be clear that none of the above alternatives is realistic in practice and that this situation is completely unacceptable in a democratic society based on the rule of law.

This, in turn, will also have repercussions for the future of the Digital Agenda for Europe, the main objective of which is to help Europe's citizens and businesses to get the most out of digital technologies. However, as indicated in the Digital Agenda for Europe, "Europeans will not embrace

technology they do not trust - the digital age is neither "big brother" nor "cyber wild west"[4]". As shown above, this is a significant fact in the case of lawyers. As long as professional secrecy between lawyers and clients cannot be guaranteed, the effective provision of legal services will be seriously undermined. Given the important relationship between legal services and economic performance – stemming from the roles that legal services play in facilitating and sustaining markets – this situation will impact negatively on the European economy.[5]

Rebuilding trust

Based on recently revealed information regarding the practice of certain state surveillance agencies, concern has arisen that the protection offered by legal measures of EU states for professional secrecy might not have worked in practice, and there might have been cases where EU Member States have enabled electronic surveillance carried out against their own nationals, in violation of their own national rules.

Furthermore, if in an EU Member State a court order is required by law to access confidential information held by lawyers in another country, that condition cannot be fulfilled if the issuing court is by definition established in a foreign country, without any possible supervision by a judge in the country where the lawyer resides. Similarly, national security grounds of another State, whether EU or not, will not necessarily be justified as national security grounds in one's own member state, and national security agencies of an EU Member State should not cooperate in such surveillance without respecting the national rules on professional secrecy.

Recognising the necessity for government bodies in law enforcement and national security to conduct electronic surveillance of citizens in certain limited circumstances, the loss of confidence that has occurred can only now be addressed by political means: for instance, by carefully analysing what areas of secret surveillance work should not be made public, and, as a corollary, where civil participation (including through representatives of the legal profession) could be useful to regain and maintain the trust of the public.

Recommendations

1. Referring to the CCBE's position (adopted 7/9/2012) on the proposed data protection reform package, the CCBE believes that law enforcement authorities' obligations regarding the protection of personal data and any other data subject to professional secrecy should be at least as high as the protection expected from data controlling entities in the private sphere. This reinforces the need to have a single, comprehensive data protection regime.
2. Furthermore, steps must be taken at the EU level to establish the minimum level of legal protection afforded to professional secrecy from government electronic surveillance, including the use of electronic communications services or other cloud service for lawyer-client communications. Lawyer-client use of these facilities should be protected in the same way regardless of whether they are stored in a data centre, or in a computer at the lawyer's office or on his person. Content that contains a professional secret, and that is processed by an electronic communication service or a cloud service provider (including an email service provider), should not be accessible to government agencies. Electronic communications services and cloud service providers should be required to offer lawyers an option for indicating such information – of course, only after careful verification as to whether that user is indeed a lawyer as claimed.
3. EU minimum standards for electronic surveillance should be established, including the need to place reasonable limits upon the invocation of national security as grounds to restrict the right to privacy. Such regulatory work should be based on reports and suggestions already made at regional and international level on this subject, for example the report by Frank La Rue, Special Rapporteur of the Human Rights Council of the United Nations (see under this

[4] Communication from the Commission, A Digitial Agenda for Europe, page 16, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:EN:PDF.

[5] See Professor George Yarrow and Dr Christopher Decker, Regulatory Policy Institute, Assessing the economic significance of the professional legal services sector in the European Union, August 2012. On page 3 it is pointed out that " A particularly important relationship between legal services and economic performance stems from the roles that legal services play in facilitating and sustaining markets. The core activity of the professional legal services sector tends to expand market activity throughout the economy, and it is therefore closely linked to economic performance and growth.

link) or the draft report by a Committee of the Council of Europe Parliamentary Assembly, "Compilation of good practices on legal and institutional frameworks and measures that ensure respect for human rights by intelligence agencies while countering terrorism, including on their oversight" (see under this link).

4. The EU should work towards reinforcing the right to privacy at international level, e.g. based on optional protocols to Article 17 of the International Covenant on Civil and Political Rights, and by strengthening the level of protection guaranteed in practice by the safe harbour principles. As regards European countries outside the European Economic Area, within the framework of the on-going modernisation process of the convention, the EU should support adoption of more specific and detailed exceptions under Article 9 of Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data.

5. Beyond all the necessary protection measures that can be achieved by political and legislative means, technical measures have to be taken as well to rebuild the trust in electronic communications and cloud services. Technical measures aimed at making Internet and cloud computing more secure and government access more subject to legal scrutiny, also have to take into account the specific requirements that have to be met in relation to information that is subject to professional secrecy obligations and legal professional privilege rules, like that between a lawyer and client. In other words, electronic communications and cloud services infrastructures have to be built where even technical functionalities guarantee that backdoors are not abused by governments or by third parties.

Conclusion

The CCBE, therefore, urges the EU institutions to create the necessary legal and technological framework in order to remedy the current situation as regards electronic mass surveillance and to safeguard professional secrecy, which is a right of all EU citizens and one of the core values of the legal profession.

ANNEX: CCBE Statement on governmental practices involving mass data mining for the purpose of surveillance – 1 July 2013

Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10 – F. : +32 (0)2 234 65 11
Email : ccbe@ccbe.eu – www.ccbe.eu

CCBE Statement on governmental practices involving mass data mining for the purpose of surveillance

01/07/2013

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 32 member countries and 11 further associate and observer countries, and through them more than 1 million European lawyers.

The CCBE has noted with great concern the recent revelations of governmental practices involving mass data mining for the purpose of surveillance.

The CCBE has repeatedly stressed the importance of professional secrecy (known in some countries as legal professional privilege) and would point out that the European Court of Justice itself expressly stated in its decision in the AM&S case (case C-155/79): "that confidentiality serves the requirements, the importance of which is recognized in all of the member states, that any person must be able, without constraint, to consult a lawyer whose profession entails the giving of independent legal advice to all those in need of it", and added that "the principle of the protection against disclosure afforded to written communications between lawyer and client is based principally on a recognition of the very nature of the legal profession, inasmuch as it contributes towards the maintenance of the rule of law and that the rights of the defence must be respected".

This core value of the legal profession is, however, under attack from organisations with highly sophisticated technical capabilities and financial means, including state bodies having secret investigatory powers.

Lawyers have no choice but to use modern technology when communicating with clients, courts, lawyer colleagues and others. Yet it now appears that such technology is not safe to use.

The erosion of the confidentiality of lawyer-client communications also erodes the trust of a citizen in the rule of law.

Therefore, the CCBE calls upon the EU institutions to take steps to protect and enhance the confidentiality of lawyer-client communications when modern technology is used. Such steps could include work in the area of technical standardisation (e.g. the possibility of setting up a lawyer account that is subject to greater protection against data mining) or in the area of instruments of international law.