Report on European Lawyers Day

On 24 October, Hugo Roebroeck and Dawn Turek interviewed Ben Wizner, Legal Advisor to Edward Snowden and Director of the American Civil Liberties Union (ACLU) Speech, Privacy & Technology Project, about the impact of mass governmental surveillance on lawyer-client confidentiality for European Lawyers Day. It is intended that the 13-minute video will be available to use by all of our members for European Lawyers Day. The video is in English, with French subtitles. Attached as Annex I and II are the French and English transcripts of the video.

ANNEX I

ENGLISH VIDEO TRANSCRIPT: BEN WIZNER

* *How do you work on a daily basis?*
* *Do you have reason to believe your work as a lawyer is under surveillance?*

WIZNER: You know, with Edward Snowden, obviously we are talking about a client who is of tremendous interest to Intelligence Agencies around the world, not just the United States. There are probably a not a set of precautions that can be taken that are strong enough to guarantee confidential communication between us. On the other hand, you know, many lawyers will have the experience where their clients are actually the experts on a subject.

In this case, Edward Snowden is one of the world’s leading security technologists. He certainly knows, much more than I do, about encryption and about the ways in which government attack it. So, in one sense this is almost impossible, in another sense, from an ethical point of view, it’s very easy. It’s impossible to be sure that an adversary, like NSA with an 80 billion dollars a year budget and many other spy agencies around the world, have not found the way into our communications. But all I can do is follow his guidance about the safest and the most secure way for us to communicate.

We have spoken publically about this so I won’t be revealing that we use a program called ‘Tails’ that allows us to chat over encrypted channels - -we have to be online at the same time in order to do that. It’s not the most efficient way to communicate - surveillance does in effect put a tax on lawyers’ time and resources in order to do this. And there will always have to be topics that we can’t discuss even in those most protected channels. Some that we discuss only face-to-face and then there are other topics that we won’t discuss face-to-face because of the surveillance environment that might exist there. So, the short answer is, that this is one of those instances, where the most ethical thing to do as lawyer it is exactly what the client tells me to do. And, I will say, the rest of my communications don’t fall into an easy pattern.

You know, we have slowly but surely begun to install PGP encryption on all of the ACLU’s computers to at least have that available as an option. But I would say that about 25 percent of the emails that I send and receive during a day use PGP. And the rest of the, you know, hundreds of e-mails that make up a lawyer’s day, where you know, in the past we may have just picked up the phone and made a quick phone call, but now we just use e-mails, we don’t, you know, encrypt and decrypt each one of those, because of the very long passwords that are involved. It will just be too cumbersome and too much of a burden.

And finally, I would say this: that, you know, I work for an organization called the ACLU, it has existed in the United States for almost a hundred years. It is perhaps the most influential NGO of this kind in the United States. It will be extremely risky for the government to target the communications of ACLU lawyers. It would have to be a very compartmentalized program, where only a very small number of people knew about it, because if that kind of thing reached the press, it would be a devastating story for the government and would do as much to erode its credibility as all the Snowden stories that we have seen to date. So, I don’t believe that the government would undertake that kind of legal and political risk. That doesn’t mean that they aren’t getting these communications through targeting of our clients and we will get to that in a moment. But, you know, I don’t believe that practicing the kind of law that I do in the United States is equivalent to practicing it in a place like Russia or a place like China.

* *Have you changed your professional and personal habits since taking this case?*

WIZNER: Well, I can’t imagine that the answer is no. I am aware, much more often, about the ways in which we are tracked. But I think many people have experienced that awareness since reading Snowden’s disclosures. They realized that that smartphone in their pocket is a little police officer that they carry around and that the search terms that they enter somewhere might be getting stored in some database. I think we all now have this feeling that there are huge data centers that are recording all of this. There might not be an individual reading it today, but someone may come under suspicion tomorrow and all of could be sitting in front of an agent. I think we all have that kind of awareness but I don’t look over my shoulder if that’s the question. I don’t fear for safety I have never been harassed at an international border or questioned by anybody. I feel like I have a lot of room to do the work that I am doing

* *Has this case changed your perspective on the right to lawyer-client confidentiality?*

WIZNER: I am not sure. I think, you know, as I said before, I think this is an exceptional case where, you know, in general all the risk belongs to the client. But in this case, the risk and the expertise both belong to the client. So no, I mean I think that confidentiality is something that we have always taken extremely seriously. It is about as close to sacred as an obligation that a lawyer can have, so I don’t know that it has, you know, changed my view so much about it, but I certainly think about it a lot.

* *Are you confident in your abilities to evade illegal surveillance?*

WIZNER: No, no one evades mass surveillance, let’s be clear about that. You know, by its nature, mass surveillance is passive, it’s not targeted. It sweeps up, indiscriminately, huge troves of information. If the British government is, through its TEMPORA program, is sitting on the back bone of the internet, no one is evading it if our communications are going through those channels. Now, you can do a better or worse job in protecting the content of your communication, depending on what tools you use, but no, we are all swept up somehow and even if it is not an NSA program.

You know, when I drive my car, smalls cameras that are placed in lots of places are snapping pictures of licenses plates as they go through with GPS coordinates. That information is been fed into databases that are joined into regional databases. So now, someone in the United States can know where I was by knowing where my license plate was. So many other databases like that are just being created, not by spy agencies making the decision, but by how cheap and pervasive data collection and storage has become. So, evading mass surveillance, you know, under those terms, is really not an individual possibility or responsibility. But what we need to do, as a society, is make mass surveillance more expensive, more difficult, more cumbersome to create the incentive for the government to do targeted surveillance rather than mass surveillance.

* *What advice do you have for lawyers in the wake of last year’s revelations?*
* *What recommendations do you have regarding the use of surveillance tools against lawyers?*

WIZNER: Well, I think all lawyers should be thinking about who their clients are. Do their clients have intellectual property that might be valuable to a foreign government or to a criminal hacker? Do their clients have confidential information that if disclosed would be ruinous or embarrassing. You can go down a list of categories like that and I think that almost all of us have clients, you know, who have information that will be of serious interest to someone else. And if that’s the case, lawyers need to wake up to this new threat model that we’ve seen.

You know, today it is the NSA, but the NSA should not be the only entity that we have in mind. Because these tools are proliferating, they are getting cheaper, they are getting more widespread and so you know, virtually, every government will have the capabilities that the NSA has shown. And not just governments, we are going to see criminal hackers whose are starting to use the same kind of tools. So yeah, in our view lawyers have an obligation to take whatever steps they are capable of to ensure that the data they are storing is encrypted.

Encryption still works. It is an important thing for people to understand, even after all of these disclosures. If you use the right encryption, it is virtually unbreakable. That does not mean that your encrypted communications can’t be intercepted. If I send you an encrypted email you need to decrypt it in order to read it. So someone who has hacked into your computer, into your end point, will be able to read the email. But if you are storing encrypted information and you have done it properly, it is really quite safe and even an intruder who can get in there could use all the computing power in the world and would not be able to decrypt it. And this isn’t hard to do. If lawyers don’t have the resources to do them themselves then, you know, I think Bar Associations need to be making that available to lawyers.

* *Do you think the annulment of the data retention directive by the European Court of Justice is a positive sign?*

WIZNER: Absolutely, here again, Europe is ahead of the United States. In the US, the NSA had been collecting and storing all of this telephone metadata itself for up to five years. One of the potential compromises that is being discussed would be something that looks like the European Data Directive that was just struck down by the Court, which is to push the information out of the NSA and have the companies themselves hold it for that period of time. That is obviously insufficient as far as we are concerned, although I should say, a small step in the right direction. It is less dangerous to liberty if the data is spread out among private companies and the NSA or the FBI need to go to a court to get permission to get it, rather than having it themselves at their disposal so they can run whatever analysis they want to on a daily basis.

Our view is that these data retention programs essentially arose because of capability, not because of debate. For the first time it became possible, financially and technologically possible, to record and store all of this information with very minimal cost. It used to be extremely expensive to do that. Governments around the world and corporations did it because they could. And now we are having this debate – you’re having it in Europe, we are having it in the United States. What are the trade-offs?

Certainly, there are benefits to law enforcement from having retained data, but that’s only part of the discussion, not all of it. The US Constitution was written to make the job of law enforcement more difficult, not easier, to put some protections between the State and individuals. I also think there is a lot more empirical information now that shows that storing information for five years is not necessary, that almost all of the requests from law enforcement come in the first six months, not in the third, fourth or fifth year. So, we need to understand that the benign or benevolent purposes to which this data is being put now, could become very dark purposes in a different political environment when it is much harder to turn back. Now is the time for us to be debating the proper balance.

ANNEX II

Transcription de la vidéo en français : BEN Wizner

* *Comment se déroule une journée de travail pour vous ?*
* *Avez-vous des raisons de croire que vos activités d’avocat sont sous surveillance ?*

WIZNER : Edward Snowden, voilà un client qui présente un intérêt considérable pour les agences de renseignement à travers le monde, et pas seulement aux États-Unis. Il n’existe certainement aucune précaution assez suffisante pour garantir la confidentialité de nos communications. D’ailleurs, de nombreux avocats ont l’expérience des domaines dans lesquels leurs clients sont les experts.

Edward Snowden est l’un des spécialistes de sécurité les plus éminents au monde. Il connaît certainement bien mieux que moi le cryptage et les méthodes du gouvernement pour s’y attaquer. C’est une prouesse technique alors que, du point de vue déontologique, la question est très simple. Il est impossible de savoir si un adversaire tel que la NSA, avec un budget de 80 milliards de dollars à l’année et de nombreuses autres agences d’espionnage dans le monde, a pu ou non se frayer un chemin dans nos communications. Mais je ne peux que suivre ses conseils sur les modes de communications les plus sécurisés.

Nous en avons parlé en public, ce n’est pas un secret, nous utilisons un programme appelé « Tails » pour dialoguer de manière cryptée. Il est nécessaire d’être en ligne pour l’utiliser. Ce n’est pas le moyen de communication le plus efficace. La surveillance pèse sur le temps et les ressources des avocats. Il y aura toujours des sujets impossibles à aborder, même en utilisant les moyens les mieux protégés. Certains sujets s’abordent face à face et d’autres pas, simplement à cause de la surveillance possible. Dans ce cas, je pense que la déontologie de l’avocat est d’agir exactement selon les souhaits du client. Le reste de mes communications ne suivent pas de modèle précis.

Nous avons installé le cryptage PGP sur tous les ordinateurs de l’ACLU. Il peut au minimum être utilisé de manière optionnelle. Environ 25 % des courriels que j’écris ou je lis en une journée sont cryptés en PGP. Quant aux centaines de courriels quotidiens d’un avocat, ceux qui remplacent nos anciens coups de téléphone, nous ne les cryptons et décryptons pas un par un. Les mots de passe sont trop longs. C’est trop de travail et trop de temps perdu.

Je tiens aussi à dire une chose. Je travaille pour l’ACLU (L’Union américaine pour les libertés civiles), qui existe aux États-Unis depuis environ cent ans. C’est sûrement l’ONG la plus influente de ce genre aux États-Unis. Il sera extrêmement risqué pour le gouvernement de cibler les communications des avocats de l’ACLU. Le programme devrait être très cloisonné. Seules quelques personnes devraient être au courant. Si la presse l’apprenait, le gouvernement serait compromis. Il perdrait toute sa crédibilité comme toutes les affaires de type Snowden que nous avons vues jusqu’à présent. Je ne crois pas que le gouvernement prendrait un tel risque juridique et politique. Cela ne veut pas dire que le gouvernement ne surveille pas ces communications en ciblant nos clients. Je vais en parler dans un instant. Je ne crois pas qu’exercer le droit comme je le fais aux États-Unis revienne au même que de le faire dans un pays comme la Russie ou la Chine.

* *Avez-vous changé vos habitudes professionnelles et personnelles depuis que vous êtes chargé de cette affaire ?*

WIZNER : Je ne peux pas vraiment dire que non. Je suis conscient, bien plus souvent, de la manière dont nous sommes suivis. Mais je crois que beaucoup de gens en sont conscients depuis les révélations d’Edward Snowden. Ils savent que leur smartphone est un mini-policier qu’ils emportent partout avec eux et que les termes de recherche qu’ils saisissent peuvent très bien finir dans des bases de données. Je pense que nous avons maintenant tous l’impression que d’énormes centres de données enregistrent toutes ces informations. Personne ne les lit probablement aujourd’hui, mais si la suspicion l’emportait, n’importe qui pourrait finir assis en face d’un policier. Je pense que nous avons tous ce genre de prise de conscience, mais si vous voulez savoir, je ne crains pas pour ma sécurité. Je n’ai jamais été harcelé à une frontière internationale ni interrogé par personne. Je sens que j’ai toute la liberté de faire mon travail.

* *Cette affaire a-t-elle changé votre point de vue sur le droit à la confidentialité des communications entre l’avocat et son client ?*

WIZNER : Je ne suis pas sûr. Comme je l’ai dit, je pense que ce cas est exceptionnel. Normalement, tous les risques reviennent au client. Ici, le risque et l’expertise reviennent au client. Donc non, je pense que nous avons toujours pris le secret professionnel très au sérieux. C’est une obligation proche du sacré pour l’avocat, donc je ne crois pas que cette affaire ait vraiment changé mon point de vue à ce sujet, mais j’y pense beaucoup.

* *Avez-vous confiance en vos capacités à échapper à la surveillance illégale ?*

WIZNER : Non, soyons clairs : personne ne se soustrait à la surveillance de masse. De par sa nature, la surveillance de masse est passive, elle n’est pas ciblée. Elle balaie, sans discernement, d’énormes sources d’information. Si le gouvernement britannique, à travers son programme TEMPORA, piétine les fondements d’Internet, personne n’est à l’abri si les communications passent par ces canaux. On peut faire le meilleur comme le pire en protégeant le contenu de ses communications en fonction des outils que l’on utilise mais tout le monde est concerné, même sans qu’il s’agisse d’un programme de la NSA.

Par exemple, des petites caméras placées à divers endroits prennent des photos des plaques d’immatriculation des voitures en prenant en compte les coordonnées GPS. Ces informations sont enregistrées dans des bases de données régionales. Quelqu’un aux États-Unis peut savoir où je me trouvais à l’aide de ma plaque d’immatriculation. De nombreuses autres bases de données du même genre sont en cours de création. Ce n’est pas parce que les agences d’espionnage l’ont décidé, mais parce que la collecte et la conservation de données ne coûte presque rien et est devenue omniprésente. Dans ces conditions, fuir la surveillance de masse n’est pas une possibilité ni une responsabilité individuelle. Ce que nous, la société, devons faire, c’est rendre la surveillance de masse plus chère, plus difficile, plus compliquée pour inciter le gouvernement de préférer la surveillance ciblée à la surveillance de masse.

* *Quels conseils donneriez-vous aux avocats à la suite des révélations de l’année dernière ?*
* *Quelles sont vos recommandations en ce qui concerne l’utilisation des outils de surveillance contre les avocats ?*

WIZNER : Je pense que tous les avocats devraient bien penser à qui sont leurs clients. Leur propriété intellectuelle pourrait-elle servir à un gouvernement étranger ou à un pirate ? Disposent-ils d’informations confidentielles dont la divulgation serait désastreuse ou embarrassante ? Dans ce genre de catégorie, je pense que la quasi-totalité d’entre nous a des clients dont les informations qui présentent un intérêt particulier pour quelqu’un d’autre. Si c’est le cas, les avocats doivent prendre conscience de ce nouveau type de menace que nous connaissons.

Aujourd’hui, c’est la NSA, mais il faut penser aux autres entités. Les outils se multiplient, ils sont moins en moins chers, de plus répandus. Les gouvernements auront pratiquement tous les moyens de la NSA. Et pas seulement les gouvernements : les pirates informatiques commencent à utiliser le même genre d’outils. Donc oui, à notre avis, les avocats ont l’obligation de prendre toutes les mesures possibles pour que les données qu’ils conservent soient cryptées.

Le cryptage fonctionne encore. Il est primordial de le savoir, malgré toutes les divulgations dont nous parlons. Un cryptage correct est quasiment infaillible. Les communications cryptées pourront quand même être interceptées. Si j’envoie un courriel crypté il faudra le décrypter pour le lire. Quelqu’un qui pirate un ordinateur pourra lire les courriels. Mais si les informations cryptées le sont correctement, elles sont en sécurité. Même un intrus disposant de toute la puissance informatique disponible à ce jour ne serait pas capable de le décrypter. Et ce cryptage n’est pas très compliqué à réaliser. Si les avocats ne disposent pas des ressources nécessaires pour le faire eux-mêmes, je crois qu’il est du devoir des barreaux de le mettre à la disposition des avocats.

* *L’annulation de la directive sur la conservation des données par la Cour européenne de justice est-elle un signal positif ?*

WIZNER : Absolument. Ici encore, l’Europe est en avance sur les États-Unis. Aux États-Unis, la NSA a recueilli et conservé toutes les métadonnées des téléphones elle-même pendant un maximum de cinq ans. L’un des compromis en cours de discussion ressemble à la directive européenne sur les données que la Cour vient d’annuler. Il s’agit de confisquer les données à la NSA et les confier aux entreprises elles-mêmes pendant cette période. C’est clairement insuffisant pour nous, mais c’est déjà un progrès. Les libertés sont moins menacées si les données sont réparties dans des entreprises privées et que le FBI ou la NSA doivent demander à un tribunal la permission d’y accéder. S’ils les ont à leur disposition, ils peuvent les analyser à tout instant comme ils le veulent.

Nous pensons que ces programmes de conservation des données sont nés en raison des possibilités techniques et non des débats. Il est devenu possible, financièrement et techniquement, d’enregistrer et de stocker toutes ces données à un coût très réduit. Avant, c’était très cher. Les gouvernements et les sociétés du monde entier l’ont fait parce qu’ils le pouvaient. Le débat est né, vous l’avez en Europe, nous l’avons aux États-Unis. Quels sont les compromis ?

Certes, l’application de la loi bénéficie du fait que les données sont conservées, mais c’est seulement une partie du débat. La Constitution des États-Unis a été conçue pour rendre l’application de la loi plus difficile afin d’établir des barrières protections entre l’État et les citoyens. Et de nombreuses informations empiriques nous montrent à présent que conserver des informations pendant cinq ans est inutile. La plupart des demandes d’application de la loi surviennent dans les six premiers mois, pas dans la troisième, quatrième ou cinquième année. Les bonnes raisons de conserver ces données à l’heure actuelle pourraient devenir très mauvaises dans un autre contexte politique où il sera beaucoup plus dur de revenir en arrière. Il est maintenant temps de débattre du bon équilibre à trouver.