“Cloud and surveillance”

(These notes formed the basis of Neil Brown’s panel session at Broad Group’s “Cloud Law European Summit” on 25th November 2014. CC BY 2.0)

Ladies and gentleman, I am delighted to be here this morning.

My aim is to introduce you to some considerations on perhaps the other side of the privacy debate, and that is to talk briefly about the cloud and surveillance.

From inherently national to supra-national

And I start by taking you back in time.

Telecoms were inherently national — until relatively recently, most telephone systems were run by the government, by the state, as a monopoly. From the mid-1980s onwards, we saw gradual movement towards market liberalisation — allowing other companies to enter the market for the provision of communications services — and privatisation of the state telecoms companies.

And because telecoms were inherently national, laws were inherently national too. And because surveillance was intrinsically linked with communications, this meant that the law on surveillance was very nationalistic too.

What we have now, in terms of cloud services, and over the top communications services, is an almost complete abandonment of this nationalism.

Laws have not moved on

But whilst services have moved on, and what you are delivering, or what you are buying, are largely supra-national in nature, laws around surveillance have, broadly speaking, not moved on.

Surveillance law is still very much national in nature — we have not seen, for example, the same kind of European harmonisation as we have with the broader regulatory regime.

UK law today

The basis of surveillance law in the UK today is under the Regulation of Investigatory Powers Act 2000, which is generally known as RIPA, with a power to order certain providers to store data for subsequent access by law enforcement in the rather more recent Data Retention and Investigatory Powers Act 2014, DRIPA.

And from the perspective of cloud service providers, there are probably three aspects of this regime which are of most relevance.

- First, there is law around interception, which is the real-time access to the content of communications. Who is sending what to and from which cloud services?

- Second, there is a framework which can require the mandatory retention of certain data for subsequent access by law enforcement, and rules governing when police can demand that certain data are provided to them. You may have seen in the press yesterday or over the weekend about plans to expand this retention regime, to force providers to retain more data relating to Internet connections. This still will not answer the question of what is being sent or retrieved, but will probably still answer the who, when, and to where questions.

- Third, there is a regime for forcing users or service providers to hand over passwords or encryption keys, to allow plain text access to seized material.

And while these are quite specific to electronic communications services, other, more traditional, mechanisms still apply — production orders, for example, or a general power of seizure, which includes an obligation to turn electronic data into a visible and legible form which can be taken away.

Points for cloud service providers

If you are providing a cloud service, of course, it is not just the laws of the UK which you will need to consider — do you have a solid understanding of the rules in each of the markets in which you have servers or presence or, potentially, even of the countries

in which you have customers? I did a small piece of work earlier this year, which identified approximately 40 pieces of legislation which could be used as a basis for demanding that a service provider hand over at least some data relating to a communication or a subscriber.

Do you have a system for ensuring that you are aware of updates to those laws?

What is your policy and a process for handling demands from law enforcement — is this something which you talk to your customers about? What would you do the number of demands increased?

Points for cloud service users

For those of you who are procuring cloud services, or just using them yourselves, do you a solid understanding of the locations in which your data might be stored? You may not know in exactly which locations your data are at any time — is that a concern for you, or are you happy with the risk if you at least know which countries it could be in?

Are you and you alone in control of the security of your data, or are you reliant on security provided by your cloud services provider? Do they control encryption, or do you?

If you are dealing with particularly sensitive — medically confidential, or legally privileged, material, for example — are you comfortable that not only your clients' data are adequately protected, but that you are protected in terms of your professional obligations?

Law reform

Lastly, I would question whether the laws we have today are suitable for the world in which we are operating. And it is my sense that a harmonised framework, even at purely a European level, would be beneficial. And I think that the key points of such a framework can be put into four points.

Point 1

Point one, is that there is a balance to be struck between the fundamental right of privacy on the one hand, and need to ensure the effective protection of citizens, prevention and detection of crime and preservation of national security, on the other. And we must be explicit and clear and transparent in what we are balancing, and how we reach any conclusion.

Point 2

Point two, is that a general refresh of laws is needed.

It is time to consider holistically what powers the government needs its agencies to have, and, where these entail intrusion into the right of privacy we each enjoy, to justify that intrusion. And it is important to do that looking at powers as a whole, not focussing on particular pieces in isolation.

Point 3

Point 3, is that, consistent with the broader approach to good regulation, any new framework must be technologically neutral. As we have discussed, the world has changed, especially technologically, since 2000, with the development of the kind of services which we discuss here today.

Laws should focus on harms, not technologies. We must be cognisant of the changes in technology, and, if the government can make a case requiring the interception of electronic communications, it should be immaterial how those are carried or provided. You should not be stuck based on the technologies you choose to deploy.

Point 4

Point 4, my final point, is that there is an absolute need for any regime to be based on core principles of necessity, proportionality and legitimacy, with strong controls of use of data coupled with audit and accountability.

Conclusion

To conclude, as more services move online, and as services move into the cloud, you can expect greater attention to be placed on your services by the government and by law enforcement agencies. Make sure that you, and your customers, are prepared for this.