Non-criminal issues and criminal issues in relation to Data Protection

2014, 359

From James MacGuill, Dundalk. The author is Chairman of the Criminal Law Committee of the Council of Bars and Law Societies of Europe (CCBE).

Dear colleagues, the kind words of introduction would have been shown to be very empty indeed if there had been any data leaking from University College Cork and my exam results were available to you dear colleagues.

I hope that those of you who have seen the printed paper do not take fright. I have no intention of delivering the whole of the very long paper that has been prepared. I am just going to make a number of key points.

The first point, which is important to us as lawyers in our own right but also as lawyers protecting the rights of citizens, is to look at the scale of criminal misconduct that is engaged in by governments throughout the world. I wish to single out the United States, naturally, and Australia. But I have seen that this week the United Kingdom has also disgraced itself in the manner in which it has taken personal data from the *Yahoo* website. We can talk about this shortly.

There are two measures in relation to Data Protection currently pending for consideration at European level, one dealing with non-criminal issues and one dealing with criminal issues. I propose briefly to compare the provisions between the two and to pose the sensible question as to why there should be a distinction between them at all. I also propose to express some of the concerns that the CCBE have raised about the almost casual and accidental way the professional secrecy or lawyer-client privilege could have been undermined in the proposal in its original form. Fortunately there is an ameliorating amendment proposed by the parliamentarians in the course of the current trialogue.

And then, finally, I conclude by making some suggestions as to how data protection law could generally be strengthened in the public interest. So, I do appreciate that it is a cruel and inhuman punishment to have to listen to about 15 minutes of me first thing in the morning when the Presidents are gathered but I will try and keep to the allotted time.

There is a famous American quotation to the effect that it has long been established that the loss of constitutional freedoms for even minimum periods of time unquestionably constitutes irreparable injury. I think that holds true not just in terms of the American situation but in terms of all our jurisdictions. We can never be overly vigilant in protecting the rights of our citizens, who are our clients, from the overreach of government, of big business, of insurers of the health sector in terms of the data that they harvest and the improper uses that they are prepared to put that data to. By way of an illustration, I think it is worthwhile looking at the American experience, following the disclosure by Mr. *Snowden* that there had been whole-scale harvesting of teledata of people not under suspicion, not people against whom there was the least allegation, but against everyone who happened to have an account with Verrizon. That news emerged in June of last year.

As a result of that, certain persons, including a Mr. *Klayman*, an American colleague, who perceived that they were potentially being listened to or having their information supplied to government brought proceedings under the Foreign Intelligence Surveillance Act in the United States to challenge the manner in which government was conducting itself. That case was heard in the US District Court. A decision was rendered in December. The first part of the decision, which I think it is very relevant to colleagues, is that there is nothing that could avail the citizens under the legislation because the legislation proceeded on the basis that the person, the data subject, would not know that they were the subject of government intrusion. And if you do not know that you are so subject, you cannot have a remedy or an opportunity to apply, to correct or erase or recover the data. That is precisely the legislative framework that we are operating with within Europe.

The idea that you would be left without a remedy simply because the framers of the legislation thought that the only affected parties were the Data Controller and the Government and not the Data Subject I think lies uneasily on us lawyers because we work on the principle where there is an injustice there must be a remedy – *ubi justitia ibi remedium.* So, in that case the court in the United States, having found that there was nothing within the specific legislation, fell back on ordinary constitutional provisions and found that the surveillance was unjustified. The particular judge, Judge *Leon*, found as a fact that no evidence had been presented by the government to the effect that the level of surveillance they were engaged in had contributed to preventing a single terrorist outrage. It is simply ineffective; it is unfortunately over-enthusiasm on the part of prosecutors and investigators with no practical benefit. So, that was the finding of fact.

The second finding of fact, which should cause us all concern, is that the government repeatedly lied to its own courts in misleading them in relation to the scale of the surveillance, and the purpose to which the infor-

mation was being put. They had to be subjected to specific rulings from the court to restrain their conduct and they violated those rulings. So, this is a government in contempt not only of its citizens but of its court. So, it was particularly outrageous to see during this week that the chief of the Central Intelligence Agency had defended this conduct and wants more powers. So, we should really be on our guard as to the motivation of governments; and the United States are perhaps just one bad example, but they might not be the only bad example.

Last week (and I am sure that many of you might have seen it) the Australians – who might be considered by the rest of the world as fair players, decent and non-partisan – spied on an American law firm, which was representing the government of Indonesia in a trade dispute with the United States and passed the information they had received on to the United States, who were happy to receive it. This is truly scandalous, subversive conduct, following the low standards of the kind they claim to be out to suppress.

This week we learned that GCHQ, the UK's intelligence agency, has been taking photo shots from the *Yahoo* website, a chatroom that is very popular, including sexually intimate photos people have sent in the context of purely private discussions. I am not sure, but I imagine that many of us in the room have children for whom this is a straight-forward routine social media. The idea that their privacy has been violated by Her Majesty,s Government in this fashion is appalling. So, what can we do about this?

The obvious place to look is data protection. And this is why the two measures that are presently being considered at European Union level are so important. The first observation that the CCBE would make in relation to the European measures is that we do not understand why they have split criminal from civil. There is no logic, in our view, to limiting the protections that are available to a citizen simply because government has decided they are putting us in one category rather than another. We very strongly support the view expressed by the European Data Protection Supervisor, which is worth quoting in full: "*[. . .] that the poor setting of personal data in the area of police and judicial cooperation in criminal matters, which by its very nature poses specific risks for the citizen, requires a level of data protection as least as high as under the proposed regulation, if not higher, due to its intrusive nature and the major impact that such processing may have on the individual's life.*"

I do not think that as lawyers we have to trouble ourselves at length as to why government did split or why governments – through the Commission – have split the two proposals because they simply do not wish to comply with rules governing their conduct of harvesting data. They are creating a legislative framework, which immunises them from scrutiny. But colleagues, they are the people we must scrutinise most closely. So, I suggest the strong view of the CCBE that the criminal measure which effectively permits the data gatherer and governments to exclude from protection anything that they say falls within the criminal justice area is quite simply a colourable device to avoid accountability. It must be resisted, and we must do everything we can to prevent such a development.

To qualify for immunisation, to effectively become lawless, all that the government will have to demonstrate is that the measure that they are defending is necessary and proportionate, with due regard to the legitimate interests of the person, a) to avoid obstructing official or legal enquiries, investigations and procedures; b) to avoid prejudicing the prevention, detection, the investigation or prosecution of criminal offences, to protect public security, to protect national security or to protect the rights and freedoms of others.

Now, I challenge all of you in this room to find a single first-year law student anywhere in the European Union that could not justify an exemption based on those criteria. They are too broad, ill-defined and impossible to challenge. It is just a charter for the violation of personal security and privacy on the part of governments. And as lawyers we should oppose it. It is, we believe, meaningless to contain provisions which entitle people to seek erasure and cancellation of data, if those rights can be postponed simply because government contend that the criteria I have just outlined have been met. As I said we had a great concern that in its original draft, the measure was one that would compel lawyers to release data that we hold to our opposing party and to others. But I am pleased to say that in the course of the current trialogue the European parliamentarians have identified an ameliorating amendment. This will protect us by exempting from disclosure privileged communications that are subject to professional secrecy. I think in passing it, we would like to say, from the Criminal Law Committee,s point of view, that we have found the work of the LIBE Committee in the Parliament and their engagement in the trialogue process to be wholly refreshing. They have approached their work with a commendable application and enthusiasm, with a fair mind. They have listened to arguments that we have made in relation to many proposals, not least under the Procedural Safeguards measures, and they have proven to be a truly worthwhile addition to the European legislative framework. I think we would like to take the opportunity of paying tribute to them for their hard work.

So, I think, we come back to look at the United States. It is really worthwhile to look at how Judge Leon in that case has succeeded in putting civil liberties ahead of the government's intentions. He did so in reliance on the Fourth Amendment to the United States, Constitution, which was the amendment which

prevented unlawful and random searches without probable cause. That amendment was introduced initially in 1789. So we are talking about centuries of concern about governmental overreach and abuse. And in the context of data protection there is a reason for continuing concern, about the conduct of Big Business, which are really mini governments in their own right. Judge *Leon* was stuck with a very unhelpful decision of 1971, where it was held that it was permitted under the Fourth Amendment to do a full intercept of a person under surveillance. This was relied on by the government to justify intercepting everyone, not just people against whom there was a specific suspicion. He deals with this in a very funny section in his judgment: This caselaw had to disapply because in 1971 if somebody wanted to send a text message, they got a pen and a paper, they put it in an envelope and they put a stamp on it. Today it is done under telephony, and this is covered by the government,s random searches. So, Judge *Leon* found that he was entitled to protect people's Fourth Amendment rights and restrained the government's conduct. As this effectively would collapse the intelligence-gathering wing of the United States government, he gave the government a stay in the belief they would in due course appeal to the US Supreme Court. It will be interesting to see whether that court – full of its political appointees – actually defends its Constitution, as it is mandated to do, or whether it will simply stand by the government that appointed them. That will be a real test for them.

At a European level, I think we have to say that the measures that are being proposed are inadequate, that there should be within the measures no difference between a person who is subject to criminal investigation and any other person. The same rights and freedoms must apply. But there must be within the measure a proper judicial review because in the civil measure, if you are dissatisfied with the conduct of the gatherer of information, you can challenge them in court under the terms of the proposal. But in the criminal measure you have far more limited challenges, only to the decision of the data supervisor. And, again as lawyers, we are completely familiar with how you can have your rights stripped away by being limited in that way to a very inadequate form of relief. So, that must go. There must be a meaningful proper independent court to which people can have recourse. There will always be information gathering that is justifiably sensitive but that can be dealt with by having specifically appointed independent lawyers. They are there to protect the rights of the public at large, privy to the information that is secret and government does not want to release to the person they are surveying. In limited cases this is justified but they cannot hide their secret from the public interest. So, dear colleagues, thank you very much.