CYBER CRIME AND JUDICIAL CO-OPERATION

The Hon. Mr. Justice Brian Murray
Judge of the Supreme Court of Ireland

1. Chief Justice Maya, judicial colleagues, ladies and gentlemen.

2. I am extremely grateful to Chief Justice Maya for her invitation to attend and observe these proceedings on behalf of the Courts of Ireland. Ireland is not a member of G20, but I know that our Government was honoured when requested by South Africa to participate in G20 as a guest country during South Africa's presidency. The invitation reflected the strong and deep bonds between our two countries. The Irish judiciary is similarly honoured to be asked to take part in this, ground breaking event and hopes this experience will further cement our relationship with our colleagues here.

3. In fact it struck me while preparing this paper that things have a funny way of coming around. Some of what I will be saying to you shortly touches on important questions of how we protect human rights at an international level. Yet my introduction to international human rights law came at the Law School in Trinity College Dublin in the early 1980s through the medium of Kader Asmal, the inspirational South African barrister, academic lawyer, human rights and anti apartheid campaigner and later Minister in President Mandela's 1994 Government. A lot of Irish folklore is more the product of vivid imagination than of fact, but the folklore has it that the earliest iterations of the South African bill of rights were prepared by Kader and Albie Sachs on the kitchen table in Kader's Dublin home.

4. It is hard not to be impressed by the precision with which the topics chosen for these discussions have captured some of the most important questions facing judiciaries today. Judicial conferences of this kind are of course critical to the process of

enhancing the quality of justice administered in all of our Courts. They afford an opportunity for judges from diverse backgrounds to both identify and in their own work to build upon commonalities of experience and outlook, while at the same time learning from differences in our legal systems. All of that is key to developing workable models of judicial co-operation into the future. And there are few areas in which such co-operation is more practically important in the borderless world to which reference has been made throughout these sessions, than in the area of cybercrime. The reasons that co-operation in that field is so important, is obvious : cyber crime is ubiquitous, dangerous, disruptive and costly. Criminals are not inhibited by national boundaries, and responses to their crimes must be similarly unconstrained, or at least as unconstrained as the due administration of justice and protection of human rights will permit.

5. It is worth taking a moment to reflect on what we are dealing with. As with all legal issues, there are questions of definition. '*Cybercrime*' may be described broadly as computer related crime – any illegal behaviour committed by means of or in relation to a computer system or network. On that basis today, cyber-crime covers a vast swathe of criminal behaviour. It captures not only most financial crimes, but exploitative offences such as child pornography or grooming and sometimes trafficking of vulnerable persons.

6. In fact, outside that parameter, even where digital technology is not a direct or indirect instrumentality of criminal behaviour, digitally stored data often provides strong evidence of crime. It does this because most communications are now reduced to that form and thus evidence relevant to guilt – or innocence – can often only be secured through the interrogation of digital devices.

7. An example from a recent case before our Court shows this. We were told in the course of our hearings that it is very common for inexperienced, first time, criminals who engage in serious wrongdoing to resort to google to inquire about the consequences of what they had just done and how they can avoid detection. They thereby create a permanent record suggesting guilt. That is the price of inexperience. We were concerned with the legal question of what judicial authorisation was required to access a computer seized in the course of a very standard search of a dwelling. It was a murder case tried in the lower Courts on circumstantial evidence. The body had been concealed on a farm after the alleged killing : the evidence included the fact that the accused had, very shortly after the estimated time of death, entered in google the four words '*human body decomposition timeline'*. The point is that evidence derived from electronic devices is everywhere. How the prosecution gets that evidence, is key. As so, therefore, is

the question of where, exactly, it is located and how, precisely, it is to be obtained if outside the jurisdiction.

8. More focussed definitions relate cybercrime to illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Even within that narrower frame, the consequences of such wrongdoing for economies, for public and private institutions and for state infrastructure are potentially horrendous. A study last year concluded that if global cyber crime were treated as a single economy, it would with a value of $10.5 trillion in 2025 be the third largest in the world after those of the United States and China.

9. Research also suggest that much of this is not being prosecuted, and one of the reasons it is not being prosecuted is because of the difficulties encountered by investigators in accessing information necessary for that purpose. This presents the

prospect that cyber crime presents the irresistible combination of high yield and low risk. Some of the technical problems are fairly obvious. Evidence may be on devices. It may be in the cloud but accessible by investigators only through the agency of the service provider. It may be in data centres. It may have been in a data centre in one jurisdiction, only to have been moved to another. By the time investigators come to look for information, it may have been destroyed. Or it may appear to have been destroyed, but be capable of reconstruction.

10. All of this is grist to the mill of lawyers who will argue issues of jurisdiction, not merely over crimes, but even over the ability of Courts to facilitate its disclosure. In particular, nice legal questions arise as to whether individual States have power under their own laws to require companies based in their jurisdictions to disclose information housed in data centres outside those jurisdictions. Similar questions arise around where data in the cloud legally exists.

11. So, evidence of a single crime of this kind may be located at the same time in several jurisdictions. It may at the same time be located in no jurisdiction. Offences may be both contemporaneously committed in many places, yet very difficult to connect to any one State. Even if it has no physical manifestation, accessing various different strands of an investigation or prosecution, will require co-operation between states.

12. The crucial role for mutual assistance between Courts is thus self-evident. Cyber crime is an international problem, and the solutions to the unique challenges it presents are inevitably products of diplomacy, politics, agreements between States and legislation. These are necessarily conditioned by sometimes differing perceptions of the scope and limits of national sovereignty. To work effectively, that requires structured and considered multi-lateral treaties. For almost twenty five years there have been various Conventions seeking to regulate mutual

judicial assistance in this field, starting with the Budapest Convention in 2001, and concluding most recently with the United Nations Cybercrime Convention agreed on Christmas Eve last year. There have also been regional agreements, including those of the League of Arab States in 2010 and the African Union in 2014.

13. All of these attempts to provide frameworks for judicial co-operation have to address difficulties and complexities inherent in the subject matter. There are, altogether, six aspects of this I want to specifically mention.

14. First, some of these conventions were drawn for a different time. The Budapest Convention – which was the first, most influential and to date the most widely ratified - predated the explosion of the internet, the emergence of the internet of things, cloud computing, and the transformation of almost all forms of communication to digital formats. While it has been

the subject of two Protocols, questions remain as to its fitness today.

15. Second, certain requests for assistance can be addressed under police to police co-operation, or in at least some jurisdictions by direct dealings between the requesting state and the service provider holding information in another jurisdiction. That is relevant to the collation of voluntary statements, and provision of witnesses who are prepared to present as witnesses and in many systems for non content data such as subscriber details. In that situation, the intervention of the courts is not required.

16. Third, however, in many jurisdictions service providers will not co-operate in the compulsory disclosure of data, and in particular of content data, unless compelled by legal authority to do so. Certainly in the EU jurisdictions the combined effect of the data privacy rights provided for in the EU Charter of Rights and Freedoms and certain EU Directives is to require an

assessment by a court or court-like body prior to the making of such disclosure. That will require that those whose data is thus to be disclosed, be enabled to make representations as to why this should not occur. It is thus at that interface that judicial co-operation comes into focus. As we all know, when matters move into the judicial domain, pressures on resources, the need to ensure due process, the complexity of legal argument, and the availability of appeals can slow down any procedure dependent on judicial resolution.

17. Yet – and fourth - speed in accessing data may be absolutely key to some of these investigations. Digital evidence is volatile, it can be manipulated, moved from one jurisdiction to another and indeed erased or seemingly erased. That problem is exacerbated by the fact that some Constitutional Courts have set their face against mandatory data retention rules, and the consideration that data minimisation requirements imposed by

some laws or Courts force service providers to delete data more quickly.

18. Fifth, the most intrusive form of mutual assistance – the extradition of those accused of offences to another jurisdiction – is complicated by the fact that many States require correspondence of offences. In the case of new and involved offences falling within the description of '*cybercrime'* this is not always easy to establish.

19. Sixth and finally, while the transmission of evidence to enable courts in other jurisdictions to proceed with their investigations and prosecutions is important, it cannot be enabled without regard to data privacy rights that may be engaged by compulsory disclosure of private information to foreign state authorities. In many cases these can be protected by a proportionality analysis weighing the interest in disclosure against the nature of the impairment, and while that can be time

consuming, this is the least of the problems. Judiciaries must also consider what constraints will be placed on the use, or onward disclosure of seized information, and whether those restrictions – together indeed with rules on retention – provide adequate protection for data privacy rights having regard to the requirements imposed by the law of the requested state. They must consider whether any restrictions on onward transmission or derivative use will be observed. State governments must consider even broader issues, many of which have troubled the Court of Justice of the European Union over the past decade : aside entirely from targeted requests for access to data for specific purposes of particular investigations, what personal data of their citizens is generally being taken from their jurisdictions abroad, and what constraints on such transfers should they impose.

20. Our overall objective as judges when negotiating this maelstrom is as easy to express as it is hard to implement. The

commitment of judges to the due administration of justice within our respective jurisdictions demands that such legal powers as are available to us are deployed in the protection and vindication of victims of such crimes, and the deterrence of unlawful interferences with the integrity of our society's economies, infrastructure and institutions. We must at the same time balance these considerations against our commitment to the safeguarding of the human rights of our citizens. This demands that powers of this kind be exercised so that entitlements to informational privacy are not impaired any more than is necessary to achieve these objectives. We must, also, endeavour to ensure that the private data of our citizens is not removed from jurisdictions in which those privacy rights and protected, to those in which data may be abused by state or non-state actors.

21. Judicial co-operation has, of course, a crucial role to play in the process of investigation and prosecution of offences in these

situations. As I said earlier, much of this is resolved through non-judicial channels - diplomacy, politics, agreements between States and legislation. But the one certainty is that our judicial systems will have to negotiate more and more of these issues, and our ability to do so can be significantly enhanced.

22. First, we can reduce delays by ensuring as between judiciaries that there are clear and documented understandings of how applications must be presented to judges by other States, and how they must be substantiated. Before the streamlining of Extradition requests in the EU, we often saw unnecessary delays in proceedings that ought to have been quite because assistance was sought by jurisdictions in terms that the requesting states found unacceptable, or could not understand, or that did not provide sufficient information for the purposes of considering the request in accordance with the law of the requested state. This can happen for reasons of language, but also legal tradition. Judicial liaison at international levels can streamline information

management processes and ensure that requesting states are fully cognisant of the demands of particular legal systems. These are best explained by and to judges.

23. Second, there are strong arguments for enhancing liason between and common education of judges in States that have executed bilateral or multi lateral treaties of this kind, not only as to the law governing these requests and the way in which colleagues in other jurisdiction have navigated the balance between the public interest in the investigation and prosecution of crime, and the private interest in one's own data, but also education as to the constantly developing technologies.

24. Third, we must acknowledge the legal imperative that there must be judicial supervision of access to data for the purposes of cross border investigations, and the factual reality that that supervision comes at the cost of delay. We need to devise mechanisms that mitigate the effects of this : for example the Court of Justice of the European Union has suggested

freezing orders preventing the deletion of data for cause, which can be used to maintain evidence pending legal proceeding.

25. Finally, within our own systems we perhaps need to consider how our own domestic law inhibits the fast and effective provision of assistance of this kind. In some jurisdictions it may well be possible for judges to use interpretative methods to align the law with the objectives of mutual assistance in these areas. This may, for example, be of relevance when it comes to defining and refining the scope of data protection rights that may be in play where such assistance is sought. The reality is that as the effects of cyber crime become more and more evident, and as technology increasingly enables the concealment of wrong doing, we need to constantly review with the benefit of ongoing experience where the and how that balance is properly drawn. That experience can be meaningfully enhanced by understanding how our colleagues in other jurisdictions have navigated their law.