The Birth and Rise of International Conventions on Cybercrime, the Five-Act Tragi-Comedie

By Gus Hosein, Privacy International

As early as 1997 the scene was set. Background: a growing 'information society', budding electronic commerce, e-government. Lights on: a sinister hacker, pimple-faced fifteen year-old, hacking at a computer using reversed engineered software, searching for child pornography and hacking into overseas government servers, depositing Trojan horses. The audience gasps in alarm (as the GASP neon lights shine in the room of the oblivious audience). Enter: the Council of Europe (CoE), the 41-member state organisation to save the children, the copyright holders, the corporations, network administrators, and law enforcement agencies of the world from sure annihilation from this 15-year old master of deception.

Continuing the dramatic twists and turns, the audience waits, in continued obliviousness, to see what the great, the bright, and the good from the CoE, plus the advising countries of Canada, Japan, South Africa, and the United States of America, can construct. We wait. We wait. We waited until April 2000 for version 19 of the Draft Convention on Cybercrime. Civil society received this document hesitantly: where were the other 18 drafts? The response from the CoE was that we should be appreciative of getting a draft: for the CoE to circulate a draft of a convention was previously unheard of.

The immediate suspicion is that this organisation of states is undemocratic, or some type of rubber-stamp process. Perhaps; but this CoE is the very same organisation responsible for the European Convention of Human Rights (ECHR), or the Convention For The Protection Of Individuals With Regard To Automatic Processing Of Personal Data (CoE 108). This is also the same CoE, however, that has released the European Convention On Mutual Assistance In Criminal Matters, and the 1995 follow up CoE Recommendation No. R (95)13 Concerning Problems of Criminal Procedure Law Connected with Information Technology. This leads us to the entrance of the main actor of this play.

Act I, Scene 19 -- The Birth of a Convention

When the public showing of the play finally began in April 2000, civil society was already in fray. We only heard recently that the G-8 was working on a consultation meeting with industry on cybercrime; the world was reeling from yet another virus, this time called "I LOVE YOU" (that amusingly plagued the love-lorn UK Parliament); and the first wide-spread Distributed Denial of Service Attacks had just occurred a few months earlier. Cryptography liberalisation was finally completing its course, but in the UK there was a full battle under the Regulations of Investigatory Powers Bill (now Act, July 2000). The CoE had just added itself to this fray, and introduced, with little fanfare, their solution to many of these problems (and they didn't mind saying so): version 19.

Version 19 was incomplete and where complete, it was in disarray. Entire sections were missing; paragraphs outlining the Interception of Communications were blank. Definitions were made of terms that were never used. And the terms liberties and rights were nowhere to be found, except in the former under 'deprivation of', and the latter, upon balancing with the needs of law enforcement. The ECHR and the Data Protection principles enshrined in other conventions were not even considered; while conventions on criminal matters were referenced to indicate consistency with previous CoE acts.

This play regarding the rise of the convention had three goals. First, the convention aims to create a level of consistency among signatory states on the nature and form of legislation criminalizing cybercrime. Yes, consistency in legal definitions and authority may be considered, but where the convention lacked in content regarding constraints of powers, it compensated with its broad scope. Covering basic types of crime, such as illegal access to systems and communication, and interference to these systems, the convention also includes forgery, fraud, child pornography, copyright crimes, and the criminalisation of devices that assist in hacking, . Version 19 was brutal in its wording, and blatant in its intentions. Many groups, including industry, were appalled by the linking of child pornography with copyright protections, and the notion of deeming tools 'illegal' because they could be used to commit crimes, while these very same tools are used for network security purposes.

The second apparent goal is that the convention assures that signatory states had consistent powers for investigating such crimes. Yes, consistency of powers of investigation may be considered, there was no consideration at all on unilateral protection of rights. The model was one of increasing the powers of

law enforcement without even considering the rights of the individual. These powers include search and seizure, preservation of data, disclosure of traffic data, and interception. Version 19 was unrewarding to the interests of civil libertarians and contained wording reminiscent of the UK's RIP Bill, while government access to keys was stated in a constructively ambiguous manner within the text of the convention.

The final apparent purpose of the convention is to provide a mechanism for mutual legal assistance among signatory states. Yes, international mutual legal assistance may be necessary and is consistent with the structure of the Internet, as crimes can be enacted in one country an actor, say our by our pimply-faced hacker, within another. Considering any such multilateral regime, however, is difficult, as we must ensure that adequate controls are again in place, and more importantly, as we export our warrants and legal notices, we must ask whether our respect for human rights get exported as well? The various countries signing to this convention have different legal protections and safeguards -- the US has judicial warrants for interception, Canada has notice after interception, while the UK has neither. Across borders, which regime takes precedence? From the civil society point of view, our perspective continues to be adamant on this purpose: We insist that the highest level of protection of individual rights be maintained across multiple parties, rather than, as is currently provided within this convention, with vague statements about the need to respect those rights, which will quickly deteriorate in practice, to the lowest common denominator.

Put all together, this convention creates a consistent set of laws in various countries, creates consistent powers for investigation (not necessarily limited to these crimes), and creates a means for investigation across borders. Each of these purposes have their own set of flaws; but when combined the convention is particularly problematic. Co-operation between law enforcement agencies across jurisdictions, the requirements for dual criminality are weak if at all existent. This strain becomes particularly apparent in version 25 (see Act IV below) when the issue of hate speech arises, but also applies to the particularities of copyright crimes, and others. So arises the question that begs to be asked: why bother with harmonizing laws and procedures but then refrain from then demanding dual criminality when these investigations go across borders? A country, say the US, could very well end up intercepting communications of a citizen within their own country at the request of another

country, say France, even though the crime being investigated in the US is not necessarily a crime in the US.

After all, at the Paris summit for the G8 Lyon Group on cybercrime, one government delegate mentioned that he looked forward to seeing China signed on to the convention. This is not surprising considering the growing use of the Internet in China; but when China makes a request on a UK ISP, which regime of investigation applies? Which regime of due process applies? The original press release for version 19 stated that cases such as the I LOVE YOU virus gave rise to the need for such a convention; considering that the virus was created in the Philippines, which at the time had very little in the statute books on hacking, one would think that the first goal of the convention would fix that. If this is the purpose of the convention, that is to ensure that statutes are established in each country and then assistance ensues, why not require dual criminality for such assistance? Considering the Philippines is not part of the Council of Europe, it is only a matter of time before this convention reaches beyond the ECHR-signing member-states of the Council of Europe.

Act II, Scene 22 -- Additions and Sharpening

In October 2000, our main actor on the scene matured when a further draft was released, version 22.

Until then, the only public input sought had been through the creation of an electronic mail address at the Council of Europe, and the solicitation of comments. Merely tabling a semi-final document and opening an email outlet for comments does not constitute openness, however. From the beginning of this play in 1997, industry and civil society representatives could have been included in consultation, but apparently were not -- at least not transparently. Comments submitted following the April 2000 announcement did not appear to have translated into substantive changes in version 22.

Following an uproar on illegal devices, the relevant article was appended with a statement that confusion regarding legitimate use of such devices would be fixed in the future. However at the same time the crime of using such devices was made extraditable. There was further elaboration (but no improvement) on the production orders that could require access to decryption keys and secured data.

It was in version 22, at last, we were introduced to the interception regime within the convention including access to the content of communications (who is saying what?), and transaction data (who is communicating with who?). The capacity introduced here is to "compel a service provider to either collect through technical means or co-operate and assist the competent authorities in the collection or recording of....content data." The crimes for such investigations are not limited to those in sections 2-11 but can include any crimes that the national government deems important enough to warrant surveillance. Content data requests were outlined without acknowledging the invasiveness of such requests within the environment of the Internet, despite various national government initiatives that encountered this fact (US with Carnivore, the UK with RIPA, the EC with Data Protection). Again, there are differences among various countries regarding the types of crimes that warrant surveillance, and this is addressed only partially later in the convention where countries retain the rights to refuse assistance to other countries if such requests prejudice the sovereignty, security, and ordre public, with the addition in version 22 of political acts as further grounds for exception. This change indicates that the CoE is aware of the differences between legal systems and respect for due process, but the CoE has continued to act in such a way that the lowest common denominator for protection of civil liberties is to prevail.

Act III: Scene 24, take 2 -- La plus ca change...

After meetings in November 2000 and a rise of public dissatisfaction, including a letter signed by over 30 civil liberties organisations around the world, some changes were introduced to this actor, and version 24-2 was released in late November 2000. Another letter was written from the Global Internet Liberty Campaign that stated from the outset:

To our dismay and alarm, the convention continues to be a document that threatens the rights of the individual while extending the powers of police authorities, creates a low-barrier protection of rights uniformly across borders, and ignores highly-regarded data protection principles.

With arising attention to the concerns of US Industry and civil society, changes were made to cater for states that had to exclude themselves from some of the more expansive powers of the convention due to national sensitivities (or

human rights inconveniently enshrined in law). Dual criminality remained unapproached despite calls for its consideration in all cases of cross-border assistance. Self-incrimination through the government access to decryption keys remained; and the lack of consideration to the shifting nature of content-data continued.

Act IV: Scene 25 -- Once more into the Breach

After a final meeting in December 2000, version 25 was released. The opportunity for a second protocol reared its head when various governments pushed for hate speech to be included as a criminal act; the ruptures in solidarity between countries continues, and its effects remain to be seen.

The impact of the convention in this condition also remains to be seen. Future meetings have been organised (Ottawa in February 2001, perhaps Paris in March 2001) to sort out the final details of the convention, to finalise implementation schemes (the Explanatory Memorandum) to the convention. Expectations are for completion by Spring 2001, and the convention will be on its way to the Council of Ministers for approval shortly thereafter.

Act V: Denoument and Unraveling?

In this convention, the CoE is granting states the terminology and impetus to act against cyber-crime; we had hoped the CoE would take this opportunity to give the signatory states the terminology and impetus to act in the interests of the rights of the individual. We were bitterly disappointed, and disenfranchised. Active consultation has been sorely lacking. It is worth noting that the individuals on the drafting committee for the convention from the UK and the US have been open to questions and responsive to requests for assistance; their exceptional performance has been exactly that: the exception to the rule. Consultation on this convention was not integrative, conciliatory, open; rather it was written behind closed doors, consultation out of reach, with critiques and concerns often dismissed and labelled as misunderstandings.

We are left with a convention that does much to ignore civil liberties, and places due process in investigations at the fancy of international arbitrage. We encounter powers that reach across borders for crimes against copyright, powers that do not accept that we are dealing with a novel technological

infrastructure with unique internal workings, different costs and liabilities, different risks. These concerns were ignored as countries endeavoured to do something about this seemingly apparent tide of lawlessness that is synonymous, apparently, with digital communications.

The only chance for substantive changes and repair to this convention is through appeals to the Council of Ministers to abandon three years of work on this convention; something that hardly seems likely. There is a glimmer, perhaps, at best; but hardly a chance for unravelling this intricate actor. Even then, we have other actors to encounter in other plays, including the G-8 and the European Commission, as they come forward with their own programs of action and civil society suffers from exclusion fatigue.

As a member of civil society, I could say that we may have failed to secure civil liberties within this convention. Perhaps we asked too much of this actor; perhaps we shouldn't have followed the neon instructions. We merely asked that limits to action be stated explicitly, such as in requiring judicial review, assuring against self-incrimination, ensuring data is gathered for specific reasons, using proportionate means at all occasions, and upholding data protection principles; to name a few. But it seems we asked too much. And our actor on the scene, transformed so little throughout this story, prepares to fulfill promises, meet challenges, and continue to abate, and elude the constraints of, what we hold dear: civil liberties.

Gus Hosein
Privacy International
http://is.lse.ac.uk/staff/hosein
February 6 2001