A Draft Commentary on the Council of Europe Cybercrime Convention*

October 2000

One of the most controversial issues on the internet for the past several years has been its use in the commission of crimes, and what should be done to deter it: the great cybercrime debate. The Cybercrime Experts Group of the G8 governments' Lyon Group met in Berlin on October 24-26, where the issue of government/industry cooperation in addressing cybercrime was the focus of discussion. One of the most important documents in circulation that addresses this issue, is the draft Council of Europe Convention on Cybercrime, a document which has been several years in the making and has recently been made available for public comment. This has been until very recently a private discussion among governments of what we believe is a public policy issue of enormous significance in the digital age. This draft paper is a contribution to the debate and to the growth of public awareness of the issues, and analyses the proposed Cybercrime Convention, discussing it in the light of civil liberties and the explosive growth and potential of privacy-enhancing technologies and individual security measures. We are releasing this document as a discussion draft, and invite all parties, but especially civil society and computer and security professionals, to comment and improve the document.

.

* This analysis is a work in progress. It was written by David Banisar, a lawyer and consultant in the Washington, DC area and Gus Hosein of the London School of Economics and represents the opinions of the authors only.

A Commentary on the Council of Europe Cybercrime Convention*

October 2000

General Comments

Numerous elements of the draft convention raise serious concerns from the perspective of civil society and business, and we urge that it not be approved until significant changes are made to many of the sections. The document has been drafted by those primarily concerned with law enforcement, and tends to reflect their concerns to the detriment of civil liberties and industry interests. The value of the protection of personal information and identity in a digital society has not been explicitly recognized, but rather privacy tends to have been set up consistently as being antithetical to public safety. In the name of promoting online security, many provisions, especially expanded data gathering, will likely have an opposite effect and detract from security.

The requirements are extremely expansive in scope, and impose significant burdens on Internet providers, operators, users and equipment manufacturers to collect information, conduct surveillance and provide assistance. New powers are given to law enforcement to conduct investigations and surveillance. New criminal penalties are created which penalize the development of essential tools needed to improve system security. At the same time, no explicit limits are placed on the powers and no mechanisms are created to ensure that they are not being misused.

The October draft defers analysis of many of the controversial sections to an unreleased "explanatory report." This report is given considerable authority, and it is a legitimate concern that as long as this report is still pending, there will be limited debate and needed changes to the text will be deferred. We believe that this report should be released before further work is done on this draft convention, and the convention should not be opened for signature until the explanatory report has been fully understood.

Finally, we find that the process in developing the convention has been antithetical to the creation of public trust, which is surely one of the core goals, and as such is therefore deeply flawed. Industry interests have not been heard until very recently, and have not been explicitly involved in the drafting process, despite several years of policy development. Balance can certainly be achieved even within working groups restricted to government organizations, if varying interests are represented. This could have been promoted by the inclusion of data commissioners, constitutional law authorities, and even economic ministries. Civil liberties and human rights interests are still being excluded from discussions. The consultation process appears to be limited to asking the public to

---

* This analysis is a work in progress. It was written by David Banisar, a lawyer and consultant in the Washington, DC area and Gus Hosein of the London School of Economics and represents the opinions of the authors only.

submit messages to an email address at the CoE. The comments submitted to the CoE following the April draft appear to have had little impact on the text.

This analysis is based on the October 2, 2000 Draft Convention on Cyber-crime (Draft N° 22 REV.) released by the Council of Europe on their web site. It also examines the changes from the draft that was publicly released in April 2000.

Scope of convention

The draft convention on cybercrime is generally expansive and ambiguous with respect to its proposed measures. The document represents the interests of law enforcement, and seems to ignore technological feasibility, scalability, operational costs and risks, and civil liberties. The following commentary expands on these observed flaws, and will attempt to clarify the ambiguities so that certain issues that have been omitted are brought to light, and the ambiguous measures are modified both to be more explicit, and to reflect those other concerns.

In its current form, this convention appears to have two purposes. First, it aims to create a level of consistency among signatory states on the nature and form of legislation criminalizing cybercrime. The concept of "cybercrime" remains vague, not having been sufficiently clarified by the very broad definition provided. We believe that a level of consistency must be sought, but we question the lack of constraints and broad scope. We are also very concerned with proposed measures, providing access to data and systems, as the measures are ambiguously phrased, thus allowing individual states to justify draconian legislation by invoking the convention.

The second apparent purpose of this convention is to provide a mechanism for mutual legal assistance among signatory states. International mutual legal assistance is necessary and consistent with the structure of the Internet. The implementation of such a regime, however, will be exceedingly 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 also export our respect for human rights. 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, vague statements about the need to respect those rights, which will quickly deteriorate in practice, to the lowest common denominator.

This convention appears to aim for high levels of criminalization of cybercrime, and signatory states are expected to implement this convention in legislation, with a few options at their disposal to opt-out of specific clauses, or to at least implement some constraint on the powers of investigation. We call this model: *High-Investigative-Powers/Low-Rights-Protections*.

Such a model does more than ensure a *level playing field* in investigating crimes: it increases the powers of law enforcement agencies across states, irrespective, it seems, of national sensibilities other than to have the disclaimer: "The powers and procedures

referred to shall be subject to conditions and safeguards as provided for under national law." If through this convention we are creating new national legislation for new crimes, we will also require new 'conditions' and new 'safeguards'. It is our contention that the latter issues must be dealt with first, before we legislate against cybercrime. Therefore, we recommend that the model be reversed. A convention on cybercrime must follow from a convention on individual rights and civil liberties and an associated minimization of burdens upon industry, and would thus result in a cybercrime convention model where *High-Investigative-Powers* can be sought because *High-Rights-Protections* are already assured.

Failing this, we would continue to advise a reversal of the current convention model: rather than *High-Investigative-Powers/Low-Rights-Protections*, for the interim we recommend a model that grants a base-case, basic necessities in cybercrime legislation, and then let signatory states, at their own discretion without international pressure through the ambiguous formulation of the requirements of this convention, manage and interpret what is required for their national interests. Such a model would be *Adequate-Investigative-Powers/Adequate-Rights-Protections*. Mutual assistance within such a model, however, is expected to uphold the highest form of protection of the rights of the individual and thus disallow arbitrage among states.

We understand that this is unlikely considering the advanced state of this process, and again we would like to state that this consultation process has engendered neither confidence nor trust in the policy development process. The fruits of a flawed policy process are reaped at the time of implementation, when trust and cooperation are vital to success. Furthermore, we all must share in the task of teaching ethics to the citizens of cyberspace, in a global society with widely differing cultures, histories, and values. Openness and public debate are fundamental to that process, and governments should lead in that process by example..

Implementation of Convention

What instruments will enforce the CoE convention?. If the CoE is insistent on an international treaty on cybercrime, it must insist upon legislative measures as instruments. To implement this convention nationally through the use of light regulation, or *co-regulation*, leaves far too much uncertainty. There is a need for congruity: co-regulation is considered to be more adaptable than legislation, but an international treaty is not easily adaptable, nor should its instruments be. Instruments must be clearly stated, and clearly defined, and clearly implemented; leaving room for interpretation will merely take advantage of ambiguities within the draft convention and we will end up with uneven implementation across signatory states. This will leave industry in a situation of varying burdens and regulatory arbitrage across borders, and an even more confusing state of affairs for industry and for those active in the defence of civil liberties.

A Secretive Process

We are concerned about the timing for this document. It is public knowledge that the Committee of Experts on Crime in Cyberspace began working on the draft convention on computer crime in early 1997. However, prior to the public release of the draft in April 2000, no draft was released and no public input was solicited. We understand that public input is limited to a short period and that it is the intent of the drafters to complete this document by the end of this year and expect it to be open for approval by early 2001.

The development of this convention has been characterized by a lack of transparency and openness in relation to the CoE policy-making process. This process has been exceedingly secretive and has not benefited from any input except from selected law enforcement officials for several years. There have been no open meetings on this held anywhere.

The only public input sought has been through the creation of an electronic mail address at the Council of Europe, and the solicitation of comments. For an issue of the scope and magnitude of this one, merely tabling a semi-final document and opening an email outlet for comments does not constitute openness. From the outset in the policy formulation process, industry and civil society representatives should have been included. Comments submitted following the April 2000 announcement do not appear to have translated into substantive changes in the most recent draft, nor has there been a discussion of their merits, so it is clear that we submit the current comments not from a belief that they will be taken seriously and integrated into the draft, but as a comment on the public record.

We are also concerned that, unlike similar processes at the Organization for Economic Cooperation and Development, independent security experts, computer user groups, professional associations, labour unions, and representatives of civil society, including human rights, privacy, and consumer groups, have been largely excluded from the process. We note that over 30 of the most prominent groups have written to the CoE and urge that their concerns be addressed: <http://www.gilc.org/privacy/coe-letter-1000.html>

Lack of Principles relating to Civil and Human Rights

Unlike other important international agreements and documents on security and encryption, such the 1992 OECD Guidelines on Computer Security and the 1996 OECD Guidelines on Encryption Policy, this document lacks principles recognizing privacy and civil liberties interests that other principles must be subject to.

Invasive investigative techniques are rarely introduced without sufficient safeguards. As we discuss in the body of this response, there are a significant number of new provisions presented in the interests of law enforcement, and nothing to counterbalance these new powers. If the CoE would only show its sincerity behind its light statements on protection of civil liberties through additional clauses valuing and protecting the right to

privacy, the right to free speech, and procedures for due process in investigation and prosecution, then this would be at least a good beginning to a fair and just policy process.

Recommendations:

We urge the CoE to include statements and clauses to this draft convention that uphold the rights of the individual, not only as stated in numerous other statutes, conventions, treaties, and declarations, but also insist upon new instruments considering the international nature of this initiative. The privacy rights of the individual, both in data transmitted across borders and in investigative techniques which reach across borders, need to be formulated explicitly. Any measures that deal with copyright need to be discussed in tandem with the right to free expression, and to fair use of copyright material. As a minimum, we would like to see not only 'recognition' under the preamble, but clauses protecting these rights before we discuss investigative techniques and measures that constrain these very same rights. We recommend that the following principles be considered for the document.

> PROTECTION OF PRIVACY AND PERSONAL DATA
> Each party shall ensure that the fundamental rights of individuals to privacy, including secrecy of communications and protection of personal data, should be respected in national information security policies and in the implementation of this treaty.
> *(from the OECD Crypto guidelines)*
>
> PROTECTION OF PRIVACY AND DATA PROTECTION
> Each party shall implement into law prior to the adoption of this treaty protections for the fundamental rights of individuals to privacy as set out in the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty ETS no. 108). Each party shall ensure that nothing in this treaty shall override the protections in that treaty.
>
> PROTECTION OF PRIVACY AND DATA PROTECTION
> Each party must take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 and the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Treaty ETS no. 108), Directive 95/46/EC of the European Parliament and of the Council of the European Union of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and EU Directive 97/66.

DEMOCRACY PRINCIPLE
Each party shall ensure that the security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.
(from the OECD Security Guidelines)

Section by Section Analysis

Preamble:

Commentary:

The preamble is indicative of the problems underlying the entire document. There is not even a pretense that the interests of civil liberties are anything but secondary to enhancing law enforcement powers. Many security experts involved in the study of the protection of the critical information infrastructure will readily acknowledge that the protection of individual privacy is fundamental to good security practice, but that view is not explicit in this document.

The document lists a host of mutual assistance and cybercrime treaties, agreements and statements but the recognition of human rights and privacy interests is limited to the 1950 CoE Convention on Human Rights and the International Convention on Civil and Political Rights. There is no mention of the extensive treaties and agreements on privacy and data protection including the CoE's own 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[1] and the series of guidelines that have been developed by the CoE for the processing of personal information under that treaty. It also ignores the European Union's 1995 Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data[2] and the 1997 Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.[3] It also fails to mention the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data[4] and the OECD's subsequent guidelines on computer security and encryption policy.

Recommendations:

---

[1] Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981. <http://www.coe.fr/eng/legaltxt/108e.htm>.

[2] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, <http://europa.eu.int/comm/internal_market/en/media/dataprot/law/index.htm>.

[3] Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector (Directive 97/66/EC of the European Parliament and of the Council of 15 December 1997), <http://www.ispo.cec.be/legal/en/dataprot/protection.html>.

[4] OECD, "Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data" Paris, 1981. <http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM>.

The preamble needs to recognize the considerable number of documents relating to privacy and data protection. It should include the following principles:

> Remembering that privacy is a fundamental human right that must be protected.
>
> Ensuring that the security of information systems should be compatible with the legitimate use and flow of data and information in a democratic society.
>
> Recognizing that intellectual property protections must be balanced with the right of individuals to freely access and disseminate information.
>
> Ensuring that this convention is consistent with the 1981 Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data[5] and the subsequently developed guidelines, the European Union's 1995 Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1997 Directive Concerning the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector and the Organization for Economic Cooperation and Development's (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data.

Article 1 - Definitions

General comments

We find that the definitions within this draft convention are problematic. They are either too far-reaching, ambiguous, or lacking in support.

One key issue is that if we are dealing with 'cybercrime', we are therefore dealing with digital infrastructure. The arising problem is that any sets of definitions that are drawn from the plain old telephone system are bound to be outdated, insufficient, and possibly misleading. The line drawn between traffic data (who someone calls, when, for how long) and communications data (the content of the telephone call) is drawn from the telephone infrastructure. Adapting this to the Internet in particular is quite different, if at all possible. Is communications the content of packets? Is traffic data just the packet headers? Or is traffic data clickstreams, or http-requests? This would result in a situation where a search such as "http://www.searchengine.com/++aids++homosexuality++symptoms" would appear as traffic data, when in fact it is far more invasive, approaching the sensitivity of communications content, and perhaps exceeding it.

A possible step forward would be to define the notion of *communication*. It seems that the convention plans on calling all interactions over the Internet 'communications'. This

[5] Convention on the Protection of Individuals with regard to the Automatic Processing of Personal Data Convention, ETS No. 108, Strasbourg, 1981. <http://www.coe.fr/eng/legaltxt/108e.htm>.

is very problematic: surfing the Internet is not a communication, rather it is a set of transactions; reading email by connecting through an ISP to then get email from a web-mail provider changes the nature of the email -- the email is more transactional data rather than straight communications once they leave the server using the hypertext transfer protocol and requires greater granularity (and resources); even performing a denial of service (DDOS) attack does not require 'communication' per se, rather it involves Internet transactions, which would require a significant surveillance infrastructure if it is to be monitored in real-time. The working group does not appear to have thought this through, or is not discussing it in full detail. If everything is 'transactions', then we need to treat transactional data with advanced protections, perhaps with even stronger protections than traditional interception of communications due to the invasive nature of transactional data.

Computer System

Text

> `"computer system" means any device or a group of inter-connected or related devices, one or more of which, pursuant to a program, performs automatic processing of data [or any other function];`

Footnote:

> The explanatory report should specify that "computer system" refers to the function of data processing and therefore may include any system that is based on such a function, e.g. telecom systems, and that the "inter-connection" referred to in the definition encompasses radio and logical connections.

Changes from 4/00 draft:

It was expanded in the 10/00 draft to include "related devices."

Commentary:

This is an extremely broad definition. Microprocessors are so pervasive in the modern era and in so many consumer devices that this could be used to cover a wide range of consumer devices from children's' toys to supercomputers. This definition creates criminal penalties for many other devices where merely picking up the device (such as a PalmPilot or turning on a cable TV settop box) would constitute access.

Other countries have more narrow definitions in their laws. The US Computer Fraud and Abuse Act (18 USC 1030 (e)(1)) defines a computer as:

> an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an

automated typewriter or typesetter, a portable hand held calculator, or other similar device;

Recommendation:

This definition should be narrowed to only apply to computer and telecommunications systems.

Computer data

Text

> "computer data" means any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function;

Changes from 4/00 draft:

Now includes programs as part of the definition instead of "set of instructions"

Commentary

This definition raises concerns about creating criminal penalties for modifying of programs for purposes of reverse engineering, security testing and privacy protection. It is also hard to tell where it ends. Is a bar code on a tin of soup computer data?

Service Provider

Text

"service provider" means:

i. any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and
ii. any other entity that processes or stores computer data on behalf of such communication service or users of such service.

Commentary

This is an extremely broad definition. There is no limitation that it is a public or commercial service or on the scale of the network. As written, it covers everything from the smallest home-based local area network to the largest telephone companies.

The CoE definition is much broader than in US law. §230 of the Telecommunications Act defines an "interactive computer service" as "any information service, system, or

access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions."

This broad scope has important ramifications. In Article 18, the providers of "computer services" are required to conduct surveillance or assist in law enforcement activities.

Recommendations

The definition needs to be revised to limit the obligations of manufacturers and providers who are not offering services to the public. It should explicitly exempt services by individual users, organizations and others who are not providing public or commercial services.

It is important that the CoE consider a regulatory impact assessment of the burdens that such an expansive definition would have on smaller organizations and individuals who operate their own services. The CoE must consider how requests will impact large service providers, and smaller service providers such as libraries, or even cybercafes and schools, with open user groups or closed user groups (such as in corporations). Or, if the CoE decides on differing regimes based on the size of service providers, then there is a side-effect on the cost structure of the larger ISPs as interception capabilities become more burdensome for these larger ISPs.

Traffic Data

Text

> "traffic data" means any computer data relating to a communication by means of a computer system, generated by the computer system that formed part in the chain of communication, indicating its origin, destination, path or route, time, date, size, duration or type of underlying [network] service.

Changes from 4/00 draft

The specific reference to location information has been removed.

Commentary

The definition of traffic data is problematic, as has been seen in a similar initiative within the United Kingdom with the debate surrounding its Regulation of Investigatory Powers Act 2000. The data would include IP addresses, telephone numbers, Ethernet numbers within closed networks, DHCP procedures, etc. However, this also introduces significant new powers of surveillance that are unlike any such powers that have existed in the past. As noted above, traffic data within digital infrastructure is more invasive than within the

plain old telephone system; and thus we hope to see more advanced protections of the rights of individuals as a result.

While the specific mention of location information has been removed, it seems likely that that type of information would still be available at the "origin." Tracking physical locations for investigations is improper without the highest form of judicial control; the CoE makes no mention of such controls in later portions of the convention. Moreover traffic data is gathered in many member states under Data Protection regimes; this must be recognized within this draft convention.

Another key concern with the collection is that within a large network, gathering this level of data beyond billing purposes is an onerous task, if it is at all possible. Even more onerous is the physical location as it pertains to mobile phones -- this data is again gathered solely for billing purposes or for the provision of advanced services.

Subscriber information

Text

> "subscriber information" means any information, contained in the form of computer data or any other form, that is held by a service provider, relating to subscribers of its service, other than traffic or content data, by which can be established:
>
> i. the type of the communication service and equipment used by the subscriber and the technical provisions taken thereto;
>
> ii. the subscriber's identity, address, telephone number, or any other information related to *[the subscriber or]* the location of his/her communication equipment.

Changes from 4/00 draft

This section was entitled "subscriber data" in previous draft. It now includes a reference to location information.

Commentary:

The condition should be that "only if this information is available within regular business practices" and we must be careful that this does not become mandatory through market coercion. That is, if service providers are *promoted* or *encouraged* to gather subscriber data, this is a negative intervention on the market and services providers that do not gather such data will lose out on the possibility of selling this data, in complete reversal of data protection regimes.

The crux of the problem is that the physical address of users is not stated explicitly under an exception of “if known." Consider free-ISPs or even AOL CD-ROM users -- this may place a burden on these service providers to gather the physical address of 'users'. A tempting trade-off, which relates similarly to traffic data retention being discussed within the G8, is that to promote the gathering of this information within service providers, governments would have to provide an incentive to service providers, such as allowing service providers to mine and sell this data. Because we support data protection principles, we oppose any such incentive structure.

Article 2 - Illegal Access

Text

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally* the access to the whole or any part of a computer system without right.** A Party may require that the offence be committed either by infringing security measures or with the intent of obtaining computer data or other dishonest intent.

Footnotes

> * - The interpretation of "intent" should be left to domestic laws, but it should not, where possible, exclude "*dolus eventualis*".
>
> ** - The expression ‘without right’ appears in all of the articles of this section and derives its meaning from the context in which it is used. Thus, without restricting how Parties may implement the concept in their national law, it may refer to conduct undertaken without authority (whether legislative, executive, administrative, judicial, contractual or consensual) or conduct that is otherwise not covered by established legal defenses, excuses, justifications or relevant principles under national law.

Changes from 4/00 draft

Same as previous draft.

Commentary

This creates an extremely broad criminal penalty. It also raises the question that criminal offences can arise from violation of contractual and consensual agreements. It also would appear to provide for such criminal offences an onerous level of punishment without regard to harm or damages.

Article 3 - illegal interception

Text

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, as well as electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent.*

Footnote

> * In some countries, interception may be closely related to the offence of unauthorized access to a computer system. In order to ensure consistency of the prohibition and application of the law, countries that require dishonest intent with respect to the offence in article 2 may also require a similar qualifier to attach criminal liability to conduct defined under Article 3.

Changes from 4/00 draft:

This now suggests that only interceptions made with "dishonest intent" should be subject to sanction.

Commentary

This section requires the creation of criminal penalties for interception of communications. However, it creates a broad exemption for "without right" which is currently undefined. It also suggests that the act be committed with "dishonest intent." It is unclear whether that will apply to cases of illegal interceptions by government officials who may not be doing it with "dishonest" intent, or to the actions of overzealous private investigators..

Recommendations

The terms "without right" and "dishonest intent" need to be further defined and limited to ensure that the acts apply equally to all parties - hackers, corporations and governmental officials - who are conducting illegal interceptions.

Article 4- Data Interference

Text

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the damaging, deletion,

deterioration, alteration or suppression** of computer data without right.

Footnotes:

* The Explanatory Report should specify that 'Alteration' also includes tampering with traffic data (spoofing).

** The Explanatory Report should clarify that "suppression of data" has two commonly agreed meanings: 1) delete data so that it does no longer exist physically; 2) "render inaccessible", i.e. prevent someone from gaining access to it while maintaining it

Changes from 4/00 draft:

Same as 4/00 draft.

Commentary

The issue of alteration of computer data raises questions about its application in the field of reverse engineering and other changes made to programs for privacy protection, fair use and other uses.

The footnote relating to alteration of data that states that traffic data spoofing is now a crime is naïve technologically, as it ignores the very functioning of Internet protocols at the application layer. As protocols are designed, software applications then make use of these protocols and establish a weak binding between the name of the user, the user's mailing address, and even the IP address of the mail transfer point. Email headers as we see and recognize them are merely created by the software applications we use, not necessarily by the protocols themselves. Additionally, mail transfer points do not all implement authentication mechanisms. As a result, all email applications to date (short of implementation of cryptographic techniques) apply weak authentication of email headers. What this condition on spoofing is dictating is that all users must make use of common email software applications, and is thus discouraging working more directly with Internet protocols.

Article 5 - System Interference

Text

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally the serious hindering without right of the functioning of a computer system by inputting, [transmitting,] damaging, deleting, deteriorating, altering or suppressing computer data.

Changes from 4/00 draft:

Same as 4/00 draft.

Commentary

While this article attempts to criminalize cracking computer systems, we believe that a great deal more can be accomplished through best practice codes for raising the security of computer systems. Otherwise there is little incentive to create and use more secure systems; all of the computer *attacks* that we have seen have taken advantage of inherent system insecurity.

Article 6 - Illegal Devices

Text

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right:*

a) the production, sale, procurement for use, import, distribution or otherwise making available of:

1. a device, including a computer program, designed or adapted [specifically] [primarily] [particularly] for the purpose of committing any of the offences established in accordance with Article 2 – 5;

2. a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

with intent that it be used for the purpose of committing the offences established in Articles 2 - 5;

b) the possession of an item referred to in paragraphs (a)(1) and (2) above, with intent that it be used for the purpose of committing the offences established in Articles 2 – 5. A party may require by law that a number of such items be possessed before criminal liability attaches.

Footnote:

*Several comments from industry indicated that the so-called “cracking-devices”, to which Article 6 applies, may also be used legitimately to test system security. The explanatory report shall clarify that the conduct defined by Article 6, when undertaken with such legitimate purposes, would be considered to be “with right”. Furthermore, the burden of proof of the unlawfulness of conduct under Article 6 would lie with the prosecution. In this context, reference should be made to the footnote under Article 2 concerning the meaning of “without right”.

Changes from 4/00 draft:

The text of this provision is the same as the previous draft. There is now a footnote that suggests that a future explanatory memorandum will resolve the problem of defining legitimate conduct and require the burden of proof to lie with the prosecution.

Related changes: Article 23 on extradition now allows for extradition for violation of this section.

Commentary:

This section raises grave concerns about the ability of companies, independent security experts and others to develop, obtain and use tools to test the security of computers and to protect the privacy of users. Article 6 here, as it has previously appeared in domestic legislation in various countries, represents the security interests of some industries (or lack of security), and ignores all else. We wish to increase the level of security in our infrastructure, not obscure it. The focus should be on illegal conduct, not on tools that have many uses.

Restricting any type of technology at a stage where the norms and practices of the Internet and digital media are still being developed is a poor idea. We support the areas of concern as presented by the security professionals organized through Purdue University. Banning these devices will only allow security weaknesses to continue to exist, and this is not in the interests of the development of our digital infrastructure.
<http://www.cerias.purdue.edu/homes/spaf/coe/TREATY_LETTER.html>

The revised footnote describing the future explanatory report is not adequate to address these concerns. The footnote may be useful in addressing the issue of use but it is inadequate on the issue of the development of the tools. Many tools are developed by independent users when a company is presented with a security hole and refuses to act on the knowledge. The tools are then released to embarrass the company into action. Will only large "legitimate" companies such as Norton or NAI be allowed to create tools while independent programmers face prosecution.

There is also the question, given the broad definition of computer systems on how this will affect other issues such as legitimate reverse engineering for the purposes of writing compatible programs and to see how a system affects user privacy or other civil liberties. As more and more of daily life now relies on programs that may have hidden built-in functions or hidden assumptions, it is essential that those inner workings be revealed. Are programs that reveal the inner workings of such consumer devices and software as CueCat, and CyberPatrol now a criminal offence?

There is also the issue of enforceability. By restricting the sale, purchase, import, and distribution of a product that is deemed illegal because it circumvents security protection, we are creating new crimes that are impossible to enforce, particularly considering the global reach of the Internet. This unenforcability was shown in the controversial case regarding DeCSS, where the application was spread quickly worldwide, through a variety

of media, including email, newsgroups, and web sites; pulling down or court action on all of these copies is unreasonable, if possible. The most basic demand that can be made to fix this unenforceable Article is to make its enaction more challenging, by demanding that all parties agree to the "may require" class in 6.2a.

Recommendation

This section should be removed and the focus should be on illegal conduct, not on the creation of tools that can be used for both legitimate and illegitimate purposes.

Article 7 Forgery

Text

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed intentionally and without right the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic*, regardless whether or not the data is directly readable and intelligible. A Party may require by law an intent to defraud, or similar dishonest intent, before criminal liability attaches.

Footnote:

> * The Explanatory Report shall specify that the term “authentic” refers to the issuer of the data, regardless whether the content of the data is true or not.

Changes from 4/00 draft

Same as previous draft

Commentary:

This Article would appear to create a legal requirement that users enter authentic data. Many users, because of legitimate concerns about their privacy, enter incorrect personal information into web sites without an intent to commit fraud. In the United States, recent polls have shown that over 50 percent of users enter inaccurate information into net sites because of their concerns about their personal information being misused.

Recommendations

The final sentence in the Article stating that a party "may require by law an intent to defraud" should be changed to "shall require" to ensure that users legitimately attempting

to protect their privacy are not committing criminal offences if they do so without fraudulent intent.

Article 8 - Fraud

Text:

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing, without right, of a loss of property to another by:
>
> a) any input, alteration, deletion or suppression of computer data,
> b) any interference with the functioning of a computer [program] or system,
>
> with the intent of procuring, without right, an economic benefit for himself or for another.

Changes from 4/00 draft

Same as previous draft

Commentary

As with Article 8, this Article appears to require that users enter legitimate data. Many users, because of legitimate concerns about their privacy, enter incorrect personal information into web sites without an intent to commit fraud.

Recommendations

The Article should be further clarified to ensure that users legitimately attempting to protect their privacy are not charged as criminals.

Article 9 - Child pornography

Text

> 1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law when committed without right[1] and intentionally the following conduct:
>
> a. offering[2] or making available child pornography through a computer system;
> b. distributing or transmitting child pornography through a computer system;

c. producing child pornography for the purpose of its distribution through a computer system[3];
d. possessing child pornography in a computer system or on a computer-data storage medium.

2. For the purpose of paragraph 1 above "child pornography" shall include pornographic material[4] that visually depicts:

a. a minor engaged in a sexually explicit conduct[5];

b. a person appearing to be a minor engaged in a sexually explicit conduct;

c. realistic images representing a minor engaged in a sexually explicit conduct.

3. For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

Footnotes

1. The Explanatory Report should clarify that the terms "without right" do not exclude legal defenses, excuses or similar relevant principles that relieve a person of responsibility under specific circumstances. Therefore, conduct undertaken with artistic, medical or similar scientific purposes would not be "without right".

2. The Explanatory Report should specify that 'offering' also includes giving information about hyperlinks to child-pornography sites and that "making available" is, for example, posting child pornography on the internet or making it available through file sharing technologies.

3. The Explanatory Report should clarify that this provision by no means is intended to restrict the criminalization of the distribution, etc, of child pornography to cases making use of a computer system, but the Convention establishes this only as a minimum standard and States are free to go beyond it.

4. The Explanatory Report should clarify that that the term "pornographic material" is governed by national standards pertaining to the classification of materials as obscene, inconsistent with public morals or similarly corrupt.

5. The Explanatory Report should specify that a "sexually explicit conduct" covers at least actual or simulated: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between minors, or between an adult and a minor, of the same or opposite sex; b) bestiality; c) masturbation; d) sadistic or masochistic abuse; or e) lascivious exhibition of the genitals or the pubic area of a minor.

Changes from 4/00 draft

This section is nearly the same as previous draft.

Commentary:

Child porn production is already illegal in the majority of states. It is unclear why it is necessary to restate this within a treaty that is to focus on cybercrime; we do not do the same for fraud, for instance. This is redundant, and unnecessary, unless there is an investigatory intent to verify the "possess(ion of) child pornography in a system or on a data carrier." We can understand the political advantages to signatory states to agree to this treaty because it deals with child porn, but such a move is based on politics rather than reason. Discussing a crime as sensitive as child pornography within this convention is merely a convenience for laying the grounds for demanding the expanded investigatory powers discussed later in this document, and we find this to be an irresponsible method of reasoning.

There are also two specific areas where the section goes beyond current national law.

According to the footnote, the Explanatory Report will include linking to childporn sites as "offering." Expanding liability to include linking is antithetical to the current operation of the Internet.

There are also constitutional issues to consider. Section 2(c) makes the display of "realistic images representing a minor" a crime. In the United States, the US Court of Appeals for the 9th circuit ruled in December 1999 that "the First Amendment prohibits Congress from enacting a statute that makes criminal the generation of images of fictitious children engaged in imaginary but explicit sexual conduct." (Free Speech Coalition v. Reno, *198 F.3d 1083*, December 17, 1999). In Canada, the Supreme Court is currently deciding whether possession of child pornography is illegal following the decision of the British Columbia Court of Appeal that possession is not illegal.

Recommendations:

This section should be removed from the document. There are already a number of existing treaties that deal with this issue. It is unnecessary to repeat those efforts here and its presence raises questions about its inclusion for solely political reasons.

Article 10 - Copyright

Text

> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Berne Convention for the Protection of Literary and Artistic Works the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed intentionally*, on a commercial scale** and by means of a computer system.

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed intentionally, on a commercial scale and by means of a computer system.

Footnotes:

* Some delegations preferred to use the word “willfully” instead of “intentionally” in both paragraphs 1 and 2, on the ground that “willfully” is used in article 61 of the TRIPS agreement (governing obligation to criminalize) and in some legal systems connotes a specific intent to infringe a copyright on a commercial scale.

**There are still discussions concerning criteria that would allow Parties to exclude minor offences from the scope of this provision.

Changes from 4/00 draft

The section has been revised. It now states that criminal liability is limited to an "infringement of copyright…where such acts are committed intentionally on a commercial scale and by means of a computer system."

Commentary

The term "commercial scale" is problematic. Rather than using a phrase such as "commercial profit" or another term that requires a financial gain from the action, this term appears to be broad enough to impose criminal liability on any user or organization that puts any copyrighted material on the net. Furthermore, a footnote for this states that "There are still discussions concerning criteria that would allow Parties to exclude minor offences from the scope of this provision." If this section were limited to only offences for criminal gain, would minor offences still be exempted?

Furthermore, the addition of copyright offences will result in dramatically expanding the resources for criminal investigation used in prosecuting this offence, which is generally and best treated as a civil matter. Copyright offences are costly to industry, but they do not warrant many of the powers in this treaty such as 24/7 networks, surveillance, extradition, etc except in the most extreme cases, which this document does not differentiate from minor cases.

In addition, the diverse number of programs legally available on the net to exchange materials that may be protected by intellectual property rights, such as FreeNet, Eternity Services, Taz Servers, etc., make enforcement of this too challenging to take seriously.

Recommendations:

This section should be removed from this treaty. There are already a number of treaties which deal with the issue of intellectual property. Those treaties are the proper fora for addressing issues relating to the creation of criminal laws for violations of intellectual property.

Article 11 - Aiding and Abetting

Text

1. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally aiding or abetting the commission of any of the offences established in accordance with Articles 2 – 10 of the present Convention.

2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally attempt to commit any of the offences established in accordance with Articles 3 through 5, 7, 8, 9 (1)b and 9(1)c of this Convention.

3. Each State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that it reserves the right not to apply, in part or in whole paragraph 2 of this article.

Commentary:

This article requires criminal penalties for "intentionally aiding or abetting the commission of any of the offenses" in Articles 2-11. It also requires penalties for attempting to violate articles 3-5, 7, 8, 9 (1)b and 9(1)c.

It is unclear under this section the scope of "aiding and abetting." Will this include linking to other sites such as has been held in the DeCSS case? How is this affected if the link is to a site in a jurisdiction where the material is not unlawful (for example: security tools covered under Article 6 or intellectual property under Article 10)?

ISP liability is also unclear. If an ISP does not follow an order to remove or block material that is created by a third party, can they then be subject to this section?

Article 12 - Corporate Liability

Text

1. Each Party shall adopt such legislative and other measures as may be necessary to ensure that legal persons can be held liable for the criminal offences established in accordance with this Convention, committed for their benefit by any natural person, acting either individually or as part of an organ of the legal person, who has a leading position within the legal person, based on:

   - a power of representation of the legal person; or
   - an authority to take decisions on behalf of the legal person; or
   - an authority to exercise control within the legal person;
   - as well as for involvement of such a natural person as aidor or abettor, under Article 11, in the above-mentioned offences.

2. Apart from the cases already provided for in paragraph 1, each Party shall take the necessary measures to ensure that a legal person can be held liable where the lack of supervision or control by a natural person referred to in paragraph 1 has made possible the commission of the criminal offences mentioned in paragraph 1 for the benefit of that legal person by a natural person under its authority.

3. Liability of a legal person under paragraphs 1 and 2 shall not exclude criminal proceedings against natural persons who are perpetrators, aidors or abettors of the criminal offences mentioned in paragraph 1.

Changes from 4/00 draft

This section is unchanged from the 4/00 draft.

Commentary

This section needs to be further clarified to ensure that ISPs are not held liable for actions under Articles 2-11 or other laws when they do not have direct control over content created by a third party. This would include cases such as access to web sites, local web pages that link to other sites, web caches, mirrors, providing electronic mail services, and materials that comes over USENET newsgroups. Imposing liability of ISPs in these cases would have a chilling effect on free speech, scientific inquiry and many other fundamental rights as ISPs would need to act aggressively to ensure that they would not be held liable. In addition, corporate liability should not be imposed for not blocking access to sites that provide tools that may be covered under Article 6.

In the United States, ISPs are exempt from liability for most of the content on their services if they are not responsible for its creation. For example, 47 USC §230(c)(1), states that: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." The US Court of Appeals noted that "The amount of information communicated via interactive computer services is therefore staggering. The specter of tort liability in an area of such prolific speech would have an obvious chilling effect. It

would be impossible for service providers to screen each of their millions of postings for possible problems. Faced with potential liability for each message republished by their services, interactive computer service providers might choose to severely restrict the number and type of messages posted. Congress considered the weight of the speech interests implicated and chose to immunize service providers to avoid any such restrictive effect." Zeran v. America Online, 129 F.3d 327 (4th Cir. Va. 1997).

Similarly, Section 512 of the US Copyright Act and Section 2.4(1) of the Canadian Copyright Act limit liability for service providers who are merely providing a conduit. Section 5 of the 1997 German Law for Information and Communication limits responsibility to cases that providers "have knowledge and are technically able and can be reasonably be able to block the use of the system." Merely proving access and automatic and temporary storage do not cause liability.

However, it is also important to note that imposing liability to ISPs who fail to act on notice about third party content also raises substantial concerns. The court in the Zeran case recognized that imposing liability after receiving notice would also create a substantial burden on providers:

> If computer service providers were subject to distributor liability, they would face potential liability each time they receive notice of a potentially defamatory statement -- from any party, concerning any message. Each notification would require a careful yet rapid investigation of the circumstances surrounding the posted information, a legal judgment concerning the information's defamatory character, and an on-the-spot editorial decision whether to risk liability by allowing the continued publication of that information. Although this might be feasible for the traditional print publisher, the sheer number of postings on interactive computer services would create an impossible burden in the Internet context.

The same concerns about the burden on ISPs would also be invoked by several other sections of the convention.

Recommendations

This section should be further clarified to ensure that service providers are not held liable for the actions of third parties in any case. Service providers should be treated as carriers for material for which they are merely providing the conduit.

Article 13 - Sanctions

Text

```
Each Party shall take the necessary measures to ensure that the
criminal offences established in accordance with Articles 2 – 11
are punishable by effective, proportionate and dissuasive
sanctions, which include deprivation of liberty.
```

Each Party shall ensure that legal persons held liable in accordance with Article 12 shall be subject to effective, proportionate and dissuasive criminal or non-criminal sanctions, including monetary sanctions.

Changes from 4/00 draft

This section now recommends that for violations of sections 2-11, that jail time should be imposed. A provision on extradition was removed.

Commentary

States should ensure that punishments are proportional to the offences, especially in regard to imprisonment. This section could have a chilling effect on civil and human rights and on technological development if the punishments are expansive. This is particularly important in sanctions for violations of intellectual property under Article 10 and for unlawful possession, distribution and use of security tools under Article 6.

As stated above, service providers should not be held liable for third party content that they did not produce or knowingly distribute.

Article 14 - Search and Seizure of Stored Computer Data

Text:

1. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:

    a) a computer system or part of it and computer data stored therein; or
    b) a computer-data storage medium in which computer data may be stored

   in its territory for the purposes of criminal investigations or proceedings.

2. Each Party shall take such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, using the measures referred to in paragraph 1 (a), and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, such authorities shall be able to expeditiously extend the search or similar accessing to the other system.

3. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2 in view

of their possible use in criminal investigations or proceedings. These measures shall include the power to:

a. seize or similarly secure a computer system or part of it or a computer-data storage medium;
b. make and retain a copy of those computer data;
c. maintain the integrity of the relevant stored computer data;
d. render inaccessible or remove those computer data in the accessed computer system.

4. Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to order for the purposes of criminal investigations or proceedings any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide all necessary information, as is reasonable, to enable the undertaking of the measures referred to in paragraphs 1 and 4.

5. [Where measures referred to in paragraphs 1 and 2 have been taken in respect of a computer system or part of it, or computer data stored therein, the custodian of the system or of the storage medium shall, when reasonably practicable, be duly informed about the executed measures.]

Footnotes:

The Explanatory Report shall clarify that this provision refers to persons having an actual (physical) control over the computer (system). This would normally include the owner of the premises where the computer is located or the owner/user of the computer itself.

Changes from 4/00 draft

A provision on notice to system administrators that their computer data has been seized is now an optional section.

The requirement that the powers be subject to conditions and safeguards has been removed.

Commentary

The Article imposes substantial burdens on users and companies. Any *expeditious extension* of search and seizure capabilities must follow from the highest form of protections under national laws. The seizure of computer systems must be done under very stringent criteria. Of specific concern is that the nature of the requested data that prompts the seizure is not even defined (relating back to 14.1.a); we are concerned that this would allow for unconstrained access and removal of computer systems for ill-defined reasons, and in the hands of aggressive foreign companies, may become a new weapon in the arsenal of unfair competitive trade practices.

When the CoE mentions 'empowering' competent authorities for investigation (such as in 14.1), we must ensure at the early stages that the clause is included: "with significant controls, i.e. judicial warrants, and under probable cause based on evidence acquired elsewhere." This is a philosophical point, but must be mentioned early on, and not as some add-on. Otherwise this convention is all about granting powers to law enforcement agencies, and dismisses the CoE's own claim to be respectful of human rights. In creating a legislative infrastructure for searching, surveillance, and seizure, to not discuss the constraints on such a system denies all that we have learned about political systems. To leave it up to national discretion basically mandates increasing powers, while not raising the levels of protection of individuals.

Of particular concern, the Article requires that countries enact laws that would require users to disclose their decryption keys and other data to allow for law enforcement access. Section 14 (4) requires countries to enact laws guaranteeing that law enforcement can "order ... any person who has knowledge about ... measures applied to secure the computer data therein to provide all necessary information."

These "lawful access" provisions have been extremely controversial. The OCED considered and rejected requiring lawful access in the OECD Cryptography Guidelines.. Only India, Singapore, Malaysia and the United Kingdom have enacted laws that would require users to disclose their keys or face criminal penalties. In those countries, police have the power to fine and imprison users who do not provide the keys or the plaintext of files or communications to police. The UK law is likely to face a legal challenge under the European Convention on Human Rights.

Such approaches raise issues involving the right against self-incrimination, which is respected in many countries worldwide. The privilege against self incrimination forbids a government official from compelling a person to testify against himself. It has a long history in law originally developing from Roman and Canon law and was subsequently adopted by the Common law.[6] In the United States, this issue has not been directly addressed by any courts yet but many legal scholars believe that it would not be permissible under the 5th Amendment to the Constitution to force an individual to disclose an encryption key or passcode that was not written down anywhere.[7]

Many European legal scholars also believe that requiring disclosure violates the European Convention on Human Rights.[8] The European Court of Human Rights has

---

[6] See R. H. Helmholz, "Self-Incrimination: The Role of the European Ius Commune", 65 NYU L Rev 962 (1990). See also L. Levy, Origins of the Fifth Amendment: The Right Against Self-Incrimination (2d ed. 1986).

[7] Doe v United States, 487 US 201, 219 (1988), Justice Stevens wrote in dissent, "[a defendant] may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe--by word or deed." See Kathleen M. Sullivan, "Privacy in the Digital Age: Encryption and Mandatory Access" before the Subcommittee on the Constitution Federalism and Property Rights, Committee on the Judiciary, United States Senate, March 17, 1998; Greg S. Sergienko, *Self Incrimination and Cryptographic Keys*, 2 RICH. J.L. & TECH. 1 (1996) <http://www.richmond.edu/jolt/v2i1/sergienko.html>, For the US government view, see Phillip R. Reitinger, Compelled Production of Plaintext and Keys, The University of Chicago, 1996 U Chi Legal F 171

[8] "In the Matter of the Draft Electronic Communications Bill and in the Matter of a Human Rights Audit for Justice and FIPR", October 7, 1999. <http://www.fipr.org/ecomm99/ecommaud.html>.

stated that the right of any "person charged" to remain silent and the right not to incriminate himself are generally recognized international standards which lie at the heart of the notion of a fair procedure under Article 6 of the European Convention on Human Rights. The burden of proof cannot be reversed for the suspect to provide the requested evidence or prove his/her innocence.[9] Article 8 of the Convention, which protects the right to respect for private life and correspondence also sets out limits on surveillance that would affect interception.

Moreover, even if the said 'person' is not a suspect, they must not be coerced into disclosing decryption key data. To merely state 'as is reasonable' allows for far reaching interpretation, while already powers of law enforcement seem to be increased. Even for a non-suspect to disclose a key is an unreasonable breach of key security.

In a related way, any disclosure of secured data must not conflict with corporate security issues, i.e. stronger statement than 'reasonable', because this may involve corporate decryption keys. The person in charge of the system must be notified as soon as the security of a system has been compromised, particularly in the corporate environment. In this environment, the lowest acceptable measure is to follow the amendment to the UK RIP Act 2000, where an amendment was introduced that whenever the security of a system is compromised (in the RIP situation, this was a decryption key of an employee within a corporate environment), the Managing Director would also need to be served with a notice. We would like to extend this notification method to any data removed from a system but we still demand the provision of a judicial warrant. Meanwhile, we emphatically oppose any access to decryption keys.

Secret searches, i.e. where the owner of the system, is not informed, is essentially hacking done by law enforcement, and must be minimized, if allowed at all.

Article 15 Production Order

Text

```
Each Party shall take such legislative and other measures as may be
necessary to empower its competent authorities to order, for the
purpose of criminal investigations or proceedings:

    a) a person in its territory to submit* specified computer data
       under this person's control, which is stored in a computer
       system or a computer-data storage medium;

    b) a service provider offering its services in its territory to
       submit subscriber information under that service provider's
       possession or control;
```

[9] See the following judgments of the Court: Funke v. France, 25 February 1993, Series A no. 256-A, p. 22, ß 44; John Murray v. the United Kingdom, 8 February 1996, Reports of Judgments and Decisions 1996-I, p. 49, ß 45; and Saunders v. the United Kingdom, 17 December 1996, Reports 1996-VI, p. 2064, ß 68; Serves v. France, 20 October, 1997, Reports 1997-VI). Our thanks to Yaman Akdeniz for this information.

c) [Option 1: a person in its territory to process specified computer data under this person's control in order to yield the information necessary for that purpose and submit it to the competent authorities] [Option 2: a person in its territory to produce, within that person's technical ability, specified information by processing data under that person's possession or control].*

Footnote:

*A Party may, by implementing this power in domestic law, require additional criteria and/or conditions, such as "in the manner specified in the order".

**Paragraph 1/c is still under discussion. It would allow to oblige private persons to process data for law enforcement purposes, e.g. analyze them according to certain criteria relevant for law enforcement or apply to them "data-matching" techniques for these purposes. It may look like being a far-reaching, intrusive power, but it could offer more guarantees for the protection of private life than it seems. If a private person applies "data-matching", only the result will be available for the law enforcement authorities. Without such an obligation, it might be necessary that these authorities obtain vast amounts of data or complete files – e.g. through the power provided for under article 15 - in order to do "data-matching" themselves.

Changes from 4/00 draft

This section has been expanded from the previous version. It also includes controversial and likely unconstitutional requirements of access.

It now states "Each Party shall take such legislative and other measures as may be necessary to empower its competent authorities to order … person in its territory to submit specified computer data under this person's control, which is stored in a computer system or a computer-data storage medium. A footnote suggests that the data must be decrypted, "A Party may, by implementing this power in domestic law, require additional criteria and/or conditions, such as 'in the manner specified in the order.'"

It also proposes two draconian requirements that individuals must assist in investigations of themselves in section 1/c. A footnote attached to the section dubiously describes how this is actually a privacy protective suggestion.

Commentary:

This Article raises substantial concerns also included in the analysis of Article 14 about forced disclosure of encryption keys by users. As noted in the analysis for the previous article, this is a clear violation of a general human right against self-incrimination that is protected in common-law countries and under the European Convention on Human Rights.

It also raises questions about controls on the seizure of data. We expect that once controls are properly implemented at the convention level on the search/seizure of computer

data/systems, that Data Protection principles will be upheld; that is, the seized data will be held securely, will be managed appropriately, and deleted after a specified amount of time.

The optional paragraph suggesting that users could be forced to process the personal information and that this would be a privacy enhancement is preposterous. There is no legitimate legal system in the world that would require users to assist in their own prosecution. In the United States, it has been long held that that individuals cannot be compelled to assist investigations against themselves. The Fifth Amendment states in part "No person… shall be compelled in any criminal case to be a witness against himself." Article 11 of the Canadian Charter of Rights and Freedoms states, "Any person charged with an offence has the right … not to be compelled to be a witness in proceedings against that person in respect of the offence." Similarly, under Article 6 of the European Convention on Human Rights, this type of forced assistance is a violation of human rights protected by the Convention, which is required to be in force in all members of the CoE.

Furthermore, the suggestion that this would enhance privacy because government officials would only seize the limited amount of evidence based on the assertions of a suspect that this is the only evidence is implausible. Typical police practice in the United States and most other countries is to be expansive in their searches and seizures. The end result of this recommendation would be for users to be forced to disclose incriminating evidence and still lose their equipment and privacy. This appears to be a clumsy attempt by law enforcement officials to dodge their responsibilities for proving a case against an individual by making the individual assist in their own prosecution. This may be acceptable practice in some less-developed counties where human rights are not respected but surely it is not acceptable or legal in any CoE country.

Article 16 - Expedited preservation of data stored in the Computer System

Text

1. Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or otherwise obtain, for the purpose of criminal investigations or proceedings, the expeditious preservation of data that is stored by means of a computer system, at least where there are grounds to believe that the data is subject to a short period of retention or is otherwise particularly vulnerable to loss or modification.

2. Where a Party gives effect to paragraph 1 above by means of an order to a person to preserve specified stored data in the person’s possession or control, the Party shall adopt such legislative and other measures as may be necessary to oblige that person to preserve and maintain the integrity of that data for a period of time as may be ordered pursuant to domestic law.

3. Each Party shall adopt such legislative or other measures as may be necessary to oblige a person to whom the procedures of preservation referred to in this Article are directed, to keep confidential the undertaking of such procedures for a period of time as permitted by domestic law.

Changes from 4/00 draft

The text of this provision is unchanged from the 4/00 draft

Commentary:

This Article on expedited preservation of data is very unbalanced and likely to create substantial burdens on service providers and violate the privacy of users. It would require substantial redesigns to computer systems to be able to collect and store the information.

It is missing a proportionality constraint for the preservation of data and a 'within-reason' constraint as well. Much of the data created in computer systems is quite temporary for good reason. In one instance: there are some cryptographic keys that are destroyed immediately for security reasons. Often such keys are generated and destroyed immediately within the cryptographic hardware, and cannot be reasonably managed or preserved; this defeats the 'within-reason' constraint that is currently lacking. Likewise, these keys, if compromised, can drastically reduce the security of other data that is outside of the data preservation warrants (presuming there are warrants). If the general security of the system is hampered by this request, the request and investigated crime must be proportionate in its nature.

Again, secrecy orders compromise corporate security policies, and are thus not recommended. If this involves decryption keys of non-suspects particularly, then such a gag order must not disallow revocation.

Article 17 Expedited preservation and disclosure of traffic data

Text

Each Party shall, with respect to undertaking the procedures referred to under article 16 in respect of the preservation of traffic data concerning a specific communication, adopt such legislative or other measures as may be necessary to:

a) ensure the expeditious preservation of that traffic data, regardless whether one or more service providers were involved in the transmission of that communication; and

b) ensure the expeditious disclosure to the Party's competent authority, or a person designated by that authority, of a

```
sufficient amount of traffic data in order to identify the
service providers and the path through which the
communication was transmitted.
```

Changes from 4/00 draft

The article is the same as the 4/00 draft.

Commentary:

This type of retention must occur only in specific cases under reasonable demands; again precluding fishing expeditions. However there are significant technological challenges to the preservation of data, and this must be discussed in detail before a high-level statement is made. Many countries have weak controls on access to traffic data; but when this comes to mobile telephony and Internet transactions, the landscape is entirely different, and greater controls are required; the CoE convention must acknowledge this.

At the G-8 meeting in Paris in May 2000, there was considerable debate among industry representatives about how long the logs were to be held. The EU was reported to be demanding a 1year log retention period. One Italian company that headed the Italian delegation offered to become a supranational log retention company that would store logs from all ISPs around the world and only give them out when required by law.

Data Protection issues again can not be ignored, and should be sustained within this convention; this article relates directly to the EU Directive of 1997 on Telecommunications Data and the Recommendation 3/99 from the Working Party on Data Protection, where the definitions of the various types of data are more developed than within this convention.

There is also the issue of mandatory identification of users or machines to facilitate logging. We are concerned by Section V of the discussion paper for workshop 1B of the October G8 meeting in Berlin, that suggests the creation of unique id numbers for each computer to facilitate identification of users. This would have profound effects on privacy. The creation of such a number would likely result in the systematic monitoring of net users and its use and abuse by e-commerce companies and by government agencies around the world. The public would also vigorously oppose this effort. As we saw with the considerable public interest over the processor Serial Number in the Pentium III chip and the use of GUIDs in Microsoft products and most recently with ad networks such as DoubleClick, users do not want to be identified when they are casually using the Internet. It is disingenuous for proponents of such a system to pretend that a machine is not a person and that this is not personal information. We should all be aware by now of the trends to ubiquitous computing and to the expansion of formerly single use items such as a cellphone or palm computer to become multifunction and strongly associated with only one individual. The generation of increasing amounts of very sensitive data from these devices is an issues that has yet to be addressed fully by data protection authorities, who we hope will comment on this discussion soon.

Article 18 - Interception of Electronic Communications

Text

Each Party shall take such legislative and other measures as may be necessary, for the purpose of criminal investigations or proceedings related to serious offences [to be defined by domestic law] to empower its competent authorities to:

(a) collect or record through application of technical means on the territory of that Party, and

(b) compel a service provider to:

(i) collect or record through application of technical means on the territory of that Party, or

(ii) co-operate and assist the competent authorities in the collection or recording of,

content data of specified communications in its territory* transmitted by means of a computer system.

Footnote

* The Explanatory Memorandum shall clarify that there is a communication on a country's territory if one of the communicating parties (human beings or computers) is located there.

Changes from 4/00 draft

This is a new section that was not included in the 4/00 draft.

Commentary

This section requires countries to adopt laws 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 are not limited to those in sections 2-11 but can include any crimes that the national government deems important enough to warrant surveillance.

This would require service providers to choose between two options: redesigning their networks to allow for an intercept capability operated within the service provider such as under UK's RIP Act 2000, or performed off-site as under Russia's SORM, or allow for third party technology owned and operated by law enforcement agencies, as is the case with the FBI's Carnivore system.

This section imposes significant burdens on an extremely wide range of private persons, organizations and companies. Under Article 1, a service provider is defined as "any public or private entity that provides to users of its service the ability to communicate by means of a computer system, and any other entity that processes or stores computer data on behalf of such communication service or users of such service." There are few if any computer or communications systems that would not fall under this definition. Every new communications tool and system would be required to implement surveillance capabilities.

As previously mentioned, we find that this is an unreasonable burden to place upon smaller service providers. There are always cost issues involved, direct, staff, storage, liability , or risk.

In the United States, the US Congress in the Communications Assistance for Law Enforcement Act (Public Law 103-414, October 25, 1994) explicitly rejected imposing a requirement that "information services" - Internet Service Providers or other online providers - build in wiretap capabilities. Congress has declined to approve proposals that would expand those requirements to Internet companies. In addition, the Internet Engineering Task Force (IETF) rejected a similar request by the FBI that all new Internet protocols have built-in surveillance capabilities earlier this year.

The issue of assistance has been similarly controversial. In the United States, several hearings have been recently held on the FBI's Carnivore system, which is designed to monitor Internet traffic from a sealed box. In Russia, the Supreme Court in October ruled that the SORM proposal violated the Russian Constitution.

Additionally, articles 14 through to 18 together may create a regime where governments may require the disclosure of keys to virtual private networks or other secure infrastructure in order to provide communications in a specified manner even if encrypted.

Recommendations

We demand more clarifications into this requirement both within the convention and within the explanatory notes (and thus we require access to any explanatory notes). The content of the communications must also be defined: is this the interception of clickstreams, i.e. transactional data while a user is on-line, or is it just access to email through specific protocols? Further clarification of the details of these provisions is required.

We also recommend that consistent limitations on the use of interception are established within this convention, rather than rely on national interpretation and implementation, as this raises a significant threat to civil liberties. We must remember that this convention, once agreed by CoE members and members of the G8, will be the model for many other countries in the world where the checks on surveillance and abuse, and redress for those wrongfully imprisoned, are not an inherent part of the legal system, or the culture.

Article 18 Bis Real-time collection of traffic data

Text

> Each Party shall take such legislative and other measures as may be necessary, for the purpose of criminal investigations or proceedings, to empower its competent authorities to:
>
> (a) collect or record through application of technical means on the territory of that Party and
>
> (b) compel a service provider to:
>
> (i) collect or record through application of technical means on the territory of that Party, or
>
> (ii) co-operate and assist the competent authorities in the collection or recording of,
>
> traffic data in real-time, associated with specified communications on its territory transmitted by means of a computer system.

Changes from 4/00 draft

This is a new section that was not previously in the 4/00 draft.

Commentary

This sets the same requirements as the previous section for capturing "traffic data in real-time." See analysis for Article 18(a).

This Article also raises questions about the use of the information by service providers in jurisdictions such as the United States where there are few meaningful limitations on the re-use of personal information gathered by Internet Service Providers and e-commerce companies about customers and visitors. It is likely that this powerful surveillance capability will be misused by these companies as part of their efforts to offset the higher costs incurred in including the capabilities in their systems.

Article 18 Ter - Obligation of confidentiality

Text

> Each Party shall take such legislative and other measures as may be necessary to oblige a service provider to keep confidential the fact of and any information about the execution of any power provided for under Articles 18 and 18 bis.

Changes from 4/00 draft

This is a new section that was not previously in the 4/00 draft.

Commentary

This Article sets requirements on confidentiality. Service providers are required to not disclose that they are conducting or assisting this surveillance. It does not set any guidelines on eventual notice to users. This is contrary to national law in numerous countries where national law requires notice at some point, especially for capture of transactional information.

Article 18 Quarter - General provisions on domestic Procedural laws

Text

1. [Each Party shall apply the measures described in articles 14 through 17, and 18 bis to:

   (a) the offences established in accordance with articles 2-11 of this Convention;
   (b) other criminal offences committed by means of a computer system;
   (c) evidence in electronic form of any criminal offence.]

2. [Each Party may, at the time of signature, or when depositing its instruments of ratification, acceptance, approval or accession, by declaration addressed to the Secretary General of the Council of Europe, declare that it reserves its right to apply the measure referred to in Article 18 bis only to offences or categories of offences specified in such declaration.]

3. For the purposes of Article 18, the range of serious offences covered shall be determined by the domestic law of the Party concerned.

4. The powers and procedures referred to in articles 14 through 18 bis shall be subject to the conditions* and safeguards provided for under the domestic law of the Party concerned.

Footnotes

The terms “conditions and safeguards” refer to procedural modalities of the powers defined in Articles 14 through 18bis. The Explanatory Report shall provide some examples of the kinds of conditions and safeguards, which Parties may wish to require.

Changes from 4/00 draft

This is a new section that was not previously in the 4/00 draft.

Commentary

As we have stated previously, traffic data can be considered equally if not more invasive than the interception of email over the Internet. Therefore we find such measures to be problematic, and should at the very least have stringent controls harmonized within this convention and not left for national interpretation, as recommended under subclauses 1, 2 and 4. Subclause 3, states that the article generally applies to 'serious offences', but countries have widely varying definitions of 'serious crime', and this will have a dangerous impact when mutual assistance is considered.

Article 19 - Jurisdiction

Text

1. Each Party shall take such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 – 11 of this Convention, when the offence is committed

    a) in its territory; or
    b) on board a ship flying the flag of that Party; or
    c) on board an aircraft registered under the laws of that Party; or
    d) on board a satellite [registered in …]; or
    e) by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State.

2. Each State may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, by a declaration addressed to the Secretary General of the Council of Europe, declare that it reserves the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs (1) b – (1) e of this article or any part thereof.

3. If a Party has made use of the reservation possibility provided for in paragraph 2 of this article, it shall adopt such measures as may be necessary to establish jurisdiction over a criminal offence referred to in Article 21, paragraph 1 of this Convention, in cases where an alleged offender is present in its territory and it does not extradite him to another Party, solely on the basis of his nationality, after a request for extradition.

1. This Convention does not exclude any criminal jurisdiction exercised in accordance with domestic law.

2. When more than one Party claims jurisdiction over an alleged offence established in accordance with this Convention, the

Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution.

Changes from 4/00 draft

This section is largely unchanged from the previous version. Paragraph 2 now allows for countries to opt-out of imposing jurisdiction when the activity is on a ship, aircraft and satellite.

19(1)e requires states to establish jurisdiction over nationals that are operating in another country where the action is against the law or "outside the territorial jurisdiction of any state."

Commentary

19(1)e is extremely far reaching, and is an overreaction to the global nature of the Internet. It creates criminal penalties for actions of nationals who have no connection with the country other than holding its citizenship. It also creates grossly unfair situations. An American citizen who has lived for 20 years in Japan who is accused of violating copyright law could be charged in an American court for something that has no connection to the US. It would also appear to be an attack on non-affiliated jurisdictions such as Sealand.

Recommendations:

Remove section 19e due to its supranational reach and threat to sovereignty.

Article 20 - General principles

Text

The Parties shall co-operate with each other, in accordance with the provisions of this chapter, and through application of relevant international instruments on international co-operation in criminal matters, arrangements agreed on the basis of uniform or reciprocal legislation, and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence of a criminal offence.

Changes from 4/00 draft

The article is the same as the 4/00 draft.

Commentary:

This section should not be used as a justification to limit national laws that place more restrictive conditions on investigatory techniques such as electronic surveillance or to limit data protection acts. Any uniform level of legislation should recognize and not undermine existing international agreements on human rights and civil liberties.

We are also concerned that this section and this chapter will apply generally to criminal offences (which remain undefined, or relate to the crimes outlined earlier in the convention). Copyright crimes of sharing MP3s and crimes of fraud where inaccurate data was entered by a user should not warrant supranational reach. Mutual assistance must be afforded with proportionality, and only for *serious crimes*.

Recommendations

We recommend that the only criminal offences that should be covered within this section and chapter be those that are defined as *serious crimes*. Due to the discrepancies on national definitions of *serious crimes* we recommend also that the term be defined within this convention to meet the sovereignty requirements of the signatory states, as well as the highest form of protection of civil liberties.

Article 21 - Extradition

Text

1. This article applies to extradition between Parties for the criminal offences established in accordance with Articles 2 – 11 of this Convention, provided that they are punishable under the laws of both Parties concerned by deprivation of liberty for a maximum period of at least one year, or by a more severe penalty. Where an extradition treaty or arrangement agreed on the basis of uniform or reciprocal legislation is in force between two or more Parties, which requires a different minimum penalty for extradition, the minimum penalty provided for in such treaty or arrangement shall instead apply.

2. The criminal offences described in paragraph 1 of this Article shall be deemed to be included as extraditable offences in any extradition treaty existing between or among the Parties. The Parties undertake to include such offences as extraditable offences in any extradition treaty to be concluded between or among them.

3. If a Party that makes extradition conditional on the existence of a treaty receives a request for extradition from another Party with which it does not have an extradition treaty, it may consider this Convention as the legal basis for extradition with respect to any criminal offence referred to in paragraph 1 of this Article.

4. Parties that do not make extradition conditional on the existence

of a treaty shall recognise the criminal offences referred to in paragraph 1 of this Article as extraditable offences between themselves.

5. Extradition shall be subject to the conditions provided for by the law of the requested Party or by applicable extradition treaties, including the grounds on which the requested Party may refuse extradition.

6. If extradition for a criminal offence referred to in paragraph 1 of this Article is refused solely on the basis of the nationality of the person sought, or because the requested Party deems that it has jurisdiction over the offence, the requested Party shall submit the case at the request of the requesting Party to its competent authorities for the purpose of prosecution and shall report the final outcome to the requesting Party in due course. Those authorities shall take their decision and conduct their investigations and proceedings in the same manner as in the case of any other offence of a comparable nature under the law of that State.

7. (a) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the name and addresses of each authority responsible for the making to or receipt of a request for extradition or provisional arrest in the absence of a treaty.

(b) The Secretary General of the Council of Europe shall set up and keep updated a register of authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

Changes from 4/00 draft

This section now allows for extradition in cases of the production, use of illegal devices set out in Article 6 and removes exemptions limiting extradition in Article 2 to cases where there is intent or damage.

Commentary

Extradition is an extraordinary power between nations and should not be treated lightly. The section lacks any principles except that a similar criminal offense exists in both countries and is punishable by imprisonment. However, for several of these sections, there are concerns about what is a crime in different jurisdictions, even if a similar law is in place. There is no exception in this section for political cases. For example, the sending of mass electronic mail by dissidents in China is considered a computer crime punishable by jail time. In other countries, computer crime is also against the law but this type of unlawful access for Spam is protected or not enforced. Similar questions are raised about Article 10 on the punishment of intellectual property crimes and Article 6 on security tools.

We therefore question whether extradition should apply unless it is to *serious crimes* (see recommendation under Article 20). Even then, extradition should only occur if there are reasonable protections of individual rights within each Party (requested and requesting).

Recommendations

We recommend that extradition only apply where there is dual criminality. We also recommend that this only apply for serious crime, and providing that there are harmonized protection of civil liberties through the investigatory and legal process in both Parties.

Article 22 - Mutual Assistance

Text

1. The Parties shall afford one another mutual assistance to the widest extent possible for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of electronic evidence of a criminal offence.

2. Each Party shall also adopt such legislative or other measures as may be necessary to carry out the obligations set forth in Articles 24 - 29.

3. For the purpose of providing cooperation under articles 24 - 29, each Party shall, in urgent circumstances, accept and respond to mutual assistance requests by expedited means of communications, including fax or e-mail, to the extent that such means provide appropriate levels of security and authentication, with formal confirmation to follow where required by the requested State.

4. Except as otherwise specifically provided in Articles 24 – [29], mutual assistance shall be subject to the conditions provided for by the law of the requested Party or by applicable mutual assistance treaties, including the grounds on which the requested Party may refuse cooperation.

5. Where, in accordance with the provisions of this chapter, the requested Party is permitted to make mutual assistance conditional upon the existence of dual criminality, that condition shall be deemed fulfilled, irrespective of whether its laws place the offence within the same category of offence or denominates the offence by the same terminology as the requesting Party, if the conduct underlying the offence for which assistance is sought is a criminal offence under its laws.

Changes from 4/00 draft

The article is the same as the 4/00 draft.

Commentary:

Subarticle 1 states that mutual assistance should be to the "widest extent possible for the purpose of investigations or proceedings concerning criminal offences". Mutual assistance must only apply, however, if there are similar investigative practices and legal procedures that protect the rights of the individual. Otherwise we see this as a gross invasion of civil liberties. For this reason we continue to advocate that this convention must at least contain standards for investigative practices with respect to the civil liberties of individuals within the signatory states.

This concern continues with Subarticle 2 which states that legislative and 'other measures' shall be adopted by signatory states. We question again the 'other measures', and demand that any mutual assistance be enacted within legislation and not left to other devices short of full agreement from the parliaments and congresses of the signatory states.

Subarticle 3 outlines how urgent requests for assistance can be received via email or fax providing that there is security and authentication. We expect that such requests will still receive judicial authorization, particularly if the investigation is of an invasive nature.

Generally we continue to be concerned with the reluctance towards dual criminality. Dual criminality is a key component to this convention; otherwise the first chapter is superfluous, so long as one country within the Council of Europe criminalizes the acts outlined earlier. For this reason, we continue to advocate that mutual assistance should only apply to *serious crimes*, and that these crimes must be defined clearly within this convention, with agreement from the signatory states.

Recommendations

We recommend dual criminality as being a key requirement for mutual assistance. This is best resolved if mutual assistance is restricted to *serious crimes* which, as recommended earlier, must be defined within this convention.

A further recommendation is that neither party may act unless there are legislative mechanisms to authorize assistance or action.

Article 23 - Mutual assistance

Text

1. Where there is no mutual assistance treaty or arrangement on the basis of uniform or reciprocal legislation, in force between the requesting and requested Parties, the provisions of paragraphs 2 through 10 of this article shall apply. The provisions of this article shall not apply where such agreement, arrangement or legislation is available, unless the Parties concerned agree to apply any or all of the remainder of this Article in lieu thereof.

2. (a) Each Party shall designate a central authority or authorities that shall be responsible for sending and answering requests for mutual assistance, the execution of such requests, or the transmission of them to the authorities competent for their execution.

(b) The central authorities shall communicate directly with each other.

(c) Each Party shall, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession, communicate to the Secretary General of the Council of Europe the names and addresses of the authorities designated in pursuance of this paragraph.

(d) The Secretary General of the Council of Europe shall set up and keep updated a register of central authorities so designated by the Parties. Each Party shall ensure that the details held on the register are correct at all times.

3. Mutual assistance requests under this Article shall be executed in accordance with the procedures specified by the requesting Party except where incompatible with the law of the requested Party.[10]

4. The requested Party may, in addition to conditions or grounds for refusal available under Article 22 (4), refuse assistance:

a) if the request concerns an offences which the requested Party considers a political offence or an offence connected with a political offence;

b) if it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests.

5. The requested Party may postpone action on a request if such action would prejudice investigations, prosecutions or related proceedings by its authorities.

6. Before refusing or postponing assistance, the requested Party shall, where appropriate after having consulted with the requesting Party, consider whether the request may be granted partially or subject to such conditions as it deems necessary.

7. The requested Party shall promptly inform the requesting Party of the outcome of the execution of a request for assistance. If the request is refused or postponed, reasons shall be given for the refusal or postponement. The requested Party shall also inform

---

[10] The explanatory text should specify that the mere fact that the requested Party's legal system knows no such procedure is not a sufficient ground to refuse to apply the procedure requested by the requesting Party.

the requesting Party of any reasons that render impossible the execution of the request or are likely to delay it significantly.

8. (a) Without prejudice to its own investigations or proceedings, a Party may, within the limits of its domestic law, without prior request, forward to another Party information obtained within the framework of its own investigations when it considers that the disclosure of such information might assist the receiving Party in initiating or carrying out investigations or proceedings concerning criminal offences established in accordance with this Convention or might lead to a request for cooperation by that Party under this chapter.

(b) Prior to providing such information, the providing Party may request that it be kept confidential or used subject to conditions. If the receiving Party cannot comply with such request, it shall notify the providing Party, which shall then determine whether the information should nevertheless be provided. If the receiving Party accepts the information subject to the conditions, it shall be bound by them.

9. (a) The requesting Party may request that the requested Party keep confidential the fact and substance of any request made under this Chapter except to the extent necessary to execute the request. If the requested Party cannot comply with the request for confidentiality, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

(b) The requesting Party may request that the requested Party not, without the prior consent of the requesting Party, make use of the substance of the request, [nor of the information obtained pursuant to having executed the request,] for purposes other than those for which it was obtained or for criminal investigations and related proceedings. If the requested Party cannot comply with the request, it shall promptly inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

(c) The requested Party may request that the requesting Party not, without the prior consent of the requested Party, transmit or use the materials furnished for investigations or proceedings other than those stated in the request. If the requesting Party accepts the materials subject to the conditions, it shall be bound by them. If the requesting Party cannot comply with the conditions, it shall promptly inform the requested Party, which shall then determine whether the materials should nevertheless be provided.

10. (a) In the event of urgency, requests for mutual assistance or communications related thereto may be sent directly by judicial authorities of the requesting Party to such authorities of the requested Party. In any such cases a copy shall be sent at the same time to the central authority of the requested Party through the central authority of the requesting Party.

(b) Any request or communication under this paragraph may be made through the International Criminal Police Organisation (Interpol).

(c) Where a request is made pursuant to subparagraph (a) and the authority is not competent to deal with the request, it shall refer the request to the competent national authority and inform directly the requesting Party that it has done so.

(d) Requests or communications made under this paragraph that do not involve coercive action may be directly transmitted by the competent authorities of the requesting Party to the competent authorities of the requested Party.

(e) Each Party may, at the time of signature or when depositing its instrument of ratification, acceptance, approval or accession inform the Secretary General of the Council of Europe that, for reasons of efficiency, requests made under this paragraph are to be addressed to its central authority.

Changes from 4/00 draft

Paragraph 4 now includes a right for a country to deny assistance when it involves a political act.

Commentary

National sovereignty with the aim of protection of civil liberties is ignored within this article. Particularly we question the footnote regarding "that the mere fact that the requested Party's legal system knows no such procedure is not a sufficient ground to refuse to apply the procedure requested by the requesting party." Consistent with our comments in the previous Article, we oppose any actions by the authorities within the requested Party that are not provided for explicitly under a statutory basis. Therefore, not only do we see the need for dual criminality, but legal recognition of the investigatory procedures must be required. Otherwise this will force requested Parties to act in a way that is outside of their mandate and rights, and the procedures of the Party with the lowest form of protections of individual rights will dominate all signatory states.

Just because there is no procedure within the legal system, this does not make the proposed procedure acceptable, and we fail to understand the logic of the drafting team.

This convention continues to fail to recognize that different countries have different legal regimes, with differing protections for the rights of the individual. Until the harmonization of these rights occurs, we will continue to oppose this convention on the grounds that it threatens national sovereignty on the basis of individual rights.

Parties are allowed to refuse requests for assistance "if it considers that execution of the request is likely to prejudice its sovereignty, security, *ordre public* or other essential interests." We would argue that sovereignty is prejudiced when the rights of the

individuals within a Party are diminished due to incompatibility with another Party. If this is too difficult a concept to grasp, then we argue that within the list of exceptions, we can see that "other essential interests" includes "the interest of protection of the rights of the individual under that Party's legal regime."

Subarticle 8a states that a party can forward information to another Party that may assist that other Party in its investigations of criminal offences. We believe that this is invasive particularly if these two Parties have differing concerns on what is defined as *crime* and when these Parties have differing protections on the rights of the individual. We re-iterate that this is why we need to harmonize protections across signatory states, otherwise we fear that this will lead to gross invasions of the rights of individuals. Consider the situation where in an investigation, Party A finds some evidence of a minor crime but believes that either the investigative techniques of Party B may find more evidence (but Party A is prevented from using those techniques due to lack of legal procedures) and/or Party B may have heavier penalties for such crimes than Party A's legal regime, then Party A will share that information with Party B in order to achieve ends that meets the interests of both Parties but to the detriment of the person's civil liberties interests.

Subarticle 9 requires the secrecy of assistance. We do question the conditions of such demands of secrecy, and whether this would preclude the cooperation of the judiciary and other legislative measures already enacted. Particularly, 9c states that "a Party may request that the requesting Party not, without the prior consent of the requested Party, transmit or use the materials furnished for investigations or proceedings other than those stated in the request." In the interest of maintaining the principles of data protection as they apply to law enforcement, we would argue that Parties **must** request that only the requested materials be furnished for use in investigation. A request for mutual assistance should not be a request for roving investigations and the full divulgation of information related to the individual under investigation.

Recommendations

When the authorities in each country cooperate, we recommend that the judicial arms of each country's government also communicate, and thus both provide oversight to the granting of the warrant, the sharing of the warrant, and the enaction of the warrant within the requested state. Only if both judiciaries support the request as being legal and just within both jurisdictions, can the assistance and investigation take place.

To support this, we also recommend that neither Party can use techniques and procedures unless they are legally supported within both Parties' legal regimes.

We recommend that the civil liberties of the individual be protected under the grounds for refusal. This can be done either by explicitly stating that *sovereignty* relates to such protection, or that *other essential interests* explicitly includes the Party's interests to uphold its own laws in the protection of individual rights of its citizenry.

We also recommend that dual criminality be required, as well as common investigative procedures be legally supported in both Parties to a sufficient degree. This returns to the idea that this convention needs to harmonize the protections of the rights of individuals.

We continue to recommend that judicial oversight of investigative techniques be performed by the judicial arm of both Parties. Various countries have varying regimes for investigative authorization: this convention must ensure that oversight is validated in both jurisdictions.

We also suggest that under 9c, the term *may request* be changed to *must request*.

Article 24 - Expedited preservation of stored computer data.

Text

1. A Party may request another Party to order or otherwise obtain the expeditious preservation of data stored by means of a computer system, which is located within the territory of that other Party and in respect of which the requesting Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

2. A request for preservation made under paragraph 1 shall specify:

   a) the authority that is seeking the preservation;
   b) the offence under investigation and a brief summary of related facts;
   c) the stored data to be preserved and its relationship to the offence;
   d) the necessity of the preservation;
   e) that the Party intends to submit a request for mutual assistance for the search or similar access, seizure or similar securing, or disclosure of the data.

3. Upon receiving the request from another Party, the requested Party shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law. For the purposes of responding to a request, dual criminality shall not be required[11] as a condition to providing such preservation, but may be required as a condition for the disclosure of the data to the requesting Party.

4. A request for preservation as described in paragraph 2 may only be refused if the requested Party believes that compliance with the request would prejudice its sovereignty, security, *ordre public* or other essential interests.

---

[11] Further consideration is necessary on this matter, given that certain delegations expressed reservations as to the possibility of giving up the requirement of dual criminality.

5. Where the requested Party believes that preservation will not ensure the future availability of the data or will threaten the confidentiality of, or otherwise prejudice the requesting Party's investigation, it shall promptly so inform the requesting Party, which shall then determine whether the request should nevertheless be executed.

6. Any preservation effected in response to the request referred to in paragraph 1 shall be for a period not less than 40 days in order to enable the requesting Party to submit a request for the search or similar access, seizure or similar securing, or disclosure of the data. Following the receipt of such request, the data shall continue to be preserved pending a decision on that request.

Changes from 4/00 draft

The article is the same as the 4/00 draft.

Commentary:

Subarticle 2 outlines the information that is to be included in a request for mutual assistance in the preservation of stored computer data. While it includes information regarding the offence, the data to be preserved, and the necessity of the preservation, we are concerned that the requesting Party may not notify the requested Party of the limits of the investigation that the requesting Party must adhere to in order to prosecute.
Following from this, subarticle 3 states that the requested Party "shall take all appropriate measures to preserve expeditiously the specified data in accordance with its domestic law". We expect that the requested Party may not use investigative techniques and procedures that are not explicitly permitted within the requesting Party.

Subarticle 6 states that any expedited preservation shall be held for a period not less than 40 days so that the requesting Party can arrange for the submission of a request for search, seizure, or securing. We question this length of time, and expect that this will only apply to serious crimes.

Recommendations

We recommend that the request for preservation must also specify the investigative constraints that exist within the requesting Party so that the requested Party does not use techniques and procedures that are beyond the powers afforded to the authorities in the requesting Party. Failure to do so may result in the requesting Party receiving materials that may not be used in the requesting Party's courts, but would consist of intelligence procured under illegal means.

We repeat the need for dual criminality and the requirement that the requested Party must not act in ways that are not consistent with the legal regime of the requesting Party.

Article 25 - Expedited disclosure of preserved traffic data

Text

1. Where, in the course of the execution of a request made under Article 24 to preserve traffic data concerning a specific communication, the requested Party discovers that a service provider in a third State was involved in the transmission of the communication, the requested Party shall expeditiously disclose to the requesting Party a sufficient amount of traffic data in order to identify that service provider and the path through which the communication was transmitted.

2. Disclosure of traffic data under paragraph 1 may only be withheld if the requested Party believes that compliance with the request would prejudice its sovereignty, security, *ordre public* or other essential interests.

Changes from 4/00 draft

The article is the same as the 4/00 draft.

Commentary:

There are no exemptions here for political acts, which we are concerned with. Consequently, as stated earlier we would like to see explicit exceptions to be allowed under civil liberties. We continue to note that unless traffic data is appropriately defined, preservation requests could be quite invasive, and require appropriate controls.

Article 26 - Mutual Assistance regarding accessing of stored computer data

Text

1. A Party may request another Party to search or similarly access, seize or similarly secure, and disclose data stored by means of a computer system located within the territory of the requested Party, including data that has been preserved pursuant to Article 24.

2. The requested Party shall respond to the request through application of international instruments, arrangements and laws referred to in article 20, and in accordance with other relevant provisions of this Chapter.

3. For the purpose of expediting the execution of the request under this Article, each Party [shall] [may], subject to its domestic law, ratify or endorse a judicial or other legal authorisation granted in another Party to search or similarly access or seize or

similarly secure the data. Disclosure of the data shall be governed by the instruments, arrangements and laws referred to in paragraph 2.

4. The request shall be responded to on an expedited basis where:

a. there are grounds to believe that relevant data is subject to a short period of retention, or is otherwise particularly vulnerable to loss or modification; or

the instruments, arrangements and laws referred to in paragraph 2 otherwise provide for expedited co-operation.

Changes from 4/00 draft

There are some additions to this article.

Commentary

This article discusses accessing stored data. Subarticle 3 seems to set the standards at the lowest common denominator in the name of sovereignty when it states that "each party [shall][may], subject to its domestic law, ratify or endorse a judicial or other legal authorization granted in another Party to search or similarly access or seize or similarly secure the data." We would prefer that any search or seizure occur with the highest controls in mind, and thus expect that there is judicial authorization required for the requesting Party before the request is made. Lower authorizations may exist, but we wish to harmonize the protection of the rights of the individual first, and maintain national sovereignty second. Secondary to this, we continue to argue that dual judicial authorization is a requirement for mutual assistance.

Recommendation

Judicial authorization for search and seizure must be required for the requesting Party before the requested Party acts upon the assistance request. Additionally, the requested Party must seek judicial authorization within its own legal regime prior to search or seizure.

Article 27. Transborder access to stored computer data not requiring mutual legal assistance

Text

1. A Party may, without obtaining the authorisation of another Party:

a) access publicly available (open source) stored computer data, regardless of where the data is located geographically; or

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

[2. Under discussion]

Changes from 4/00 draft

The 10/00 draft removes a requirement that the data accessed must be so accessed in accordance with domestic law.

Commentary

We expect that any such actions would adhere to the principles of data protection, and disallow information gathered for one reason to be used for another.

Article 28. Mutual Assistance Regarding the Interception of Data

Text

The Parties shall provide mutual assistance to each other with respect to the interception of the content of specified communications transmitted by means of a computer system [to the extent permitted by their applicable treaties and domestic laws].

Article 28 bis - Mutual assistance regarding the real-time collection of traffic data

1. The Parties shall provide mutual assistance to each other with respect to the real-time collection of traffic data concerning specified communications transmitted by means of a computer system. Subject to subparagraph 3, assistance shall be governed by the conditions and procedures provided for under domestic law.

2. Each Party shall provide such assistance at least with respect to [the offences established in accordance with this convention and such other] [the offences established in accordance with articles 2 through 5 and 9 of this convention and such other] criminal offences for which real-time collection would be available in a similar national case.

3. Parties that limit the types of offences for which the measure is available shall consider expanding their ability to provide such assistance to other criminal offences related to computer systems and data.

Changes from 4/00 draft

This is a new section not in the 4/00 draft

It authorizes mutual assistance for the interception of data and the real time collection of traffic data (for sections 2-5, 9) and other criminal offences

Commentary

There is no guidance on the limitations to this power. While many states recognize that interception is intrusive, each state has a different set of constraints and warrant regimes (if at all), with different frequencies of use. This will have the effect of raising the number of interceptions within signatory states (as the state with the more common practice of interception will now require that other states recognize their requests), while the second state and service provider that is served with the request has no assurance of the integrity of the constraints. The CoE must ensure that there are consistent limitations to this investigative technique, and thus respect the cultural values of the signatory countries.

We find particularly problematic the language in Article 28bis.3 where it states that "Parties that limit the types of offences for which the measure is available shall consider expanding their ability to provide such assistance to other criminal offences related to computer systems and data." This is again the expansion of powers of authorities which contradicts national sovereignty. We oppose this subarticle, and we oppose this idea. Additionally, interception must only apply to *serious crime.*

Recommendations

Therefore we recommend that interception and traffic data be acquired only for *serious crime* which must be defined and agreed upon within this convention. We require the highest form of judicial oversight, and dual criminality (which would be resolved if our first recommendation is followed) and judicial oversight by both Parties.

As a result, we recommend that any assistance be rendered only if procedures exist within both Parties, and are compatible.

In response to Article 28bis.3, we recommend the inverse: countries without adequate controls on their interception techniques must decrease their powers to be consistent with the highest forms of protection of the signatory states. Otherwise, the lowest common denominator for protection of civil liberties will prevail.

Article 34 - Accession to the Convention.

Text

1. After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting the Contracting States to the Convention, may invite the European

Community as well as any State not a member of the Council and not having participated in its elaboration to accede to this Convention, by a decision taken by the majority provided for in Article 20d of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

2. In respect of the European Community and any State acceding to it under paragraph 1 above, the Convention shall enter into force on the first day of the month following the expiration of a period of three months after the date of deposit of the instrument of accession with the Secretary General of the Council of Europe.

Changes from 4/00 draft

This is a new section not included in the 4/00 draft

Commentary:

The Article allows countries who are not part of the CoE and who were not involved in the draft to accede to the Convention by invitation of the Committee of the Council of Ministers of the CoE. This dramatically expands the scope of this convention to many nations that do not have the same common background, traditions , and legal protections towards the protection of human rights and civil liberties as the members of the Council of Europe. This is of particular concern since many of the Articles in the document expand law enforcement power but do not explicitly place limitations on those expansions, relying on national laws or practices or outside agreements such as the European Convention on Human Rights to set the framework. Many of the countries that are likely to sign this treaty, such as China and Singapore, are not a party to these agreements and have a history of hostility to human rights interests. The use of criminal laws for political purposes is of particular concern to human rights groups, and raises concerns in the area of mutual assistance.

Recommendations

This treaty should restricted to members of the Council of Europe and other countries that have acceded to the European Convention on Human Rights, CoE Convention 108 on data protection and other essential human rights treaties. Countries should be required to demonstrate that they follow standards of human rights and data protection before they are invited to join.

Article 36 – Relationship to other conventions and agreements

1. *[Under discussion]*

2. If two or more Parties have already concluded an agreement or treaty on the matters dealt with in this Convention or otherwise

```
have established their relations in this matter, or should they in
future do so, they shall be entitled to apply that agreement or
treaty or to regulate those relations accordingly, in lieu of the
present Convention.
```

Commentary:

This article is a logical location for defining the relationship between this treaty and other treaties and agreements such as the Convention on Human Rights and the CoE Treaty 108 on data protection

Recommendations

We recommend that an additional section be added which explicitly states that this convention will be implemented in a way consistent with human rights agreements.

Conclusion

This convention appears to have been developed solely for the interests of law enforcement, despite early statements within the convention that it is the CoE's intention to balance respect for human rights with law enforcement interests. If this desire is sincere, let us see some amendment of the text implementing that respect for human rights. What we do see is an alarming international regime of mutual assistance and consistency being established.. This convention is aiming for the lowest common denominator in the protection of individual rights among signatory states, while consistently increasing powers of authorities.

We therefore recommend that the highest forms of protection for the rights of the individual be established in such a convention. Such a convention must uphold data protection principles, just procedures, and reconsider its mutual assistance articles in the same way that the EU Data Protection Directive deals with transborder data flow: only countries with adequate human rights protections can share investigative data.