

University of New South Wales
University of New South Wales Faculty of Law Research Series
2011

Year 2011

Paper 53

30 years on: The review of the Council of
Europe Data Protection Convention 108

Sylvia Kierkegaard*

Nigel Waters†

Graham Greenleaf‡

Lee Bygrave**

Ian Lloyd††

Steve Saxby‡‡

*University of Southampton

†University of New South Wales

‡University of New South Wales

**University of Oslo

††University of Southampton

‡‡University of Southampton

This working paper is hosted by The Berkeley Electronic Press (bepress) and may not be commercially reproduced without the permission of the copyright holder.

<http://law.bepress.com/unswwps-flrps11/art53>

Copyright ©2011 by the authors.

30 years on: The review of the Council of Europe Data Protection Convention 108

Sylvia Kierkegaard, Nigel Waters, Graham Greenleaf, Lee Bygrave, Ian Lloyd,
and Steve Saxby

Abstract

The Council of Europe celebrates in 2011 the 30th Anniversary of its Data Protection Convention (usually referred to as Convention 108) which has served as the backbone of international law in over 40 European countries and has influenced policy and legislation far beyond Europe. It is the only legally binding international treaty dealing with privacy and data protection. With new data protection challenges arising regularly, the Council is revising Convention 108 to attempt to meet and overcome these challenges. This paper was a joint submission by its authors on behalf of Computer Law and Security Review (CLSR), the International Association of IT Lawyers (IAITL) and ILAWS, University of Southampton, in response to the Expert Committee's public consultation on the Convention. Some of the main submissions made are:

- The Convention should remain a simple, concise and technologically neutral instrument, while at the same time recognising and addressing some new characteristics of the present and future technological environment.
- It would not be helpful to try to define the right to privacy in a data protection Convention. It would be helpful to include "collection" in the definition of automatic processing so that all of the principles apply, where relevant, to collection. Both the proportionality principle (which should apply to all operations carried out on the data) and the data minimisation principle (which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible) are significant principles which could valuably be added, and we strongly support their inclusion.
- A right to be forgotten in respect of online data (that is, people should be able to give informed consent to every site or service that processes their data, and they should also have the right to ask for all of their data to be deleted).
- The concept of consent, if it is used, it needs to be expressly defined as meaning free, voluntary, informed and revocable at any

time, and not bundled with other consents. • Compatibility (of secondary uses) is a subjective concept, and would be better expressed as “uses or disclosures” which are within the reasonable expectations of the data subject (to which a “reasonable person” test would be applied). • Full application of privacy principles to the behaviour of private individuals would be onerous and oppressive e threatening other important freedoms and rights, but some controls and restrictions are justified. This is best handled by a broad statement of privacy protection in the ECHR and similar human rights instruments, at the international level. • A right for data subjects to be informed of data breaches affecting them that meet specified threshold criteria should stand alone as a separate principle. • There would be no need for separate principles or rules for traffic or location data if personal data is defined as expressly including any information which enables or facilitates communication with a person on an individualised basis, whether or not it meets the current definition of personal data. • There should be an obligation to demonstrate that measures have been taken to ensure full respect for data protection rules, but “accountability” cannot be and must not become an alternative to data export restrictions. • Allowance for anonymity should be made a basic data protection principle in itself, with pseudonymity as the first fall-back option when anonymity cannot be achieved for legal or technical reasons. • One particular task of a supervisory authority that needs to be spelled out is the obligation to account for their performance of their complaint investigation obligations, including by reporting to the public, on objectively determined criteria, of cases investigated (anonymised to the extent necessary to protect privacy but not otherwise), and by statistics including those on outcomes and remedies. • It remains appropriate to require an adequate level of protection as a condition of cross-border transfer.

available at www.sciencedirect.comwww.compseconline.com/publications/prodclaw.htm

**Computer Law
&
Security Review**

30 years on – The review of the Council of Europe Data Protection Convention 108

Sylvia Kierkegaard^a, Nigel Waters^b, Graham Greenleaf^c, Lee A. Bygrave^d, Ian Lloyd^e, Steve Saxby^f

^a President International Association of IT Lawyers, CLSR Editorial Board Member, Senior Research Fellow, ILAWS, Visiting Professor, University of Southampton, United Kingdom

^b Visiting Fellow at UNSW, Law Faculty and formerly Deputy Commonwealth Privacy Commissioner, Australia

^c CLSR Editorial Board Member, Professor of Law & Information Systems, University of New South Wales (UNSW), Co-Director, Australasian Legal Information Institute (AustLII), Founding Director, Cyberspace Law and Policy Centre, UNSW, Australia

^d Norwegian Research Centre for Computers and Law, Department of Private Law, University of Oslo, CSLR Editorial Board Member, Norway

^e Senior Research Fellow, ILAWS, University of Southampton, CLSR Editorial Board Member, United Kingdom

^f Research Director and Director of ILAWS, Faculty of Business and Law, University of Southampton, United Kingdom, Editor-in-Chief CLSR

A B S T R A C T

Keywords:

Council of Europe data protection Convention
Convention 108
Data protection
IAITL
ILAWS
Transborder data flows

The Council of Europe is engaging in a process of revising its Data Protection Convention (Convention 108) to meet and overcome these challenges. The Council of Europe celebrates this year the 30th Anniversary of its Data Protection Convention (usually referred to as Convention 108) which has served as the backbone of international law in over 40 European countries and has influenced policy and legislation far beyond Europe's shores. With new data protection challenges arising every day, the Convention is revising its Data Protection Convention. Computer Law and Security Review (CLSR) together with the Intl. Association of IT Lawyers (IAITL) and ILAWS have submitted comments in response to the Expert Committee's public consultation on this document. CLSR aims to position itself at the forefront of policy discussion drawing upon the high quality scholarly contributions from leading experts around the world.

© 2011 Sylvia Kierkegaard, Nigel Waters, Graham Greenleaf, Lee Bygrave, Ian Lloyd & Steve Saxby. Published by Elsevier Ltd. All rights reserved.

1. Before the Expert Committee set up under Convention 108

1.1. Modernisation of Convention 108

The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (generally referred to as "Convention 108"), enacted in 1981, is

the only legally binding international treaty dealing with privacy and data protection. The Convention provided the legal framework for the EU Data Protection Directive 95/46.

When Convention 108 was drafted, the computer world was very different to the one which we inhabit today. The Convention was designed to regulate what was in many respects a niche activity. Today, it is difficult to identify any activity which does not involve interaction with computer-

based technology. Developments with contact-less debit cards and the inclusion of payment facilities in mobile phones are bringing even the most basic transactions, such as the purchase of a cup of coffee, into the data processing and protection arena.

There is little in the data protection principles with which anyone could disagree. Application is another matter and 30 years on the prime task for revision of the Convention should be to make the instrument the basis for global consensus regarding the manner in which personal data should be processed.

There appears to be widespread recognition within Europe that significant reforms to data protection law are overdue. In this regard, reference can be made to the review commissioned by the UK's Information Commissioner and published in 2009 and to the consultation launched by the European Commission in 2010.

With new data protection challenges arising every day, the Convention is being overhauled to meet new realities. The review aims at "modernising" the Convention without altering its basic principles, but looking at adding new ones such as those of proportionality and privacy by design. Pursuant to the Notice Published by the Expert Committee under Convention 108, the Computer Law and Security Review, the International Association of IT Lawyers and the Institute for Law and the Web (ILAWS) at the University of Southampton welcomes the opportunity to submit the following comments:

CLSR *Computer Law and Security Review* (www.elsevier.com/locate/clsr), an international journal of technology law and practice edited by Prof Steve Saxby of Southampton University since 1985, provides a major platform for publication of high quality research, policy and legal analysis within the field of IT law and computer security and is available on ScienceDirect™ <http://www.sciencedirect.com>, the world's foremost provider of electronic scientific information to more than 12 million subscribers.

IAITL The *International Association of IT Lawyers* (IAITL) is an international association constituted primarily of lawyers and legal practitioners who have an interest in IT law. The IAITL seeks to promote study and research in the field through international conferences, networking, publication of member's research works, job announcements and the provision of internet resources.

ILAWS is the *Institute for Law and the Web* (<http://www.soton.ac.uk/ilaws>) at Southampton University. It was established in 2006 to work on the legal issues, problems and opportunities associated with the Internet, the Web and digital technology. It is a unique interdisciplinary research centre that combines legal expertise in key domains such as IT law, e-commerce, and intellectual property law.

CLSR, IAITL and ILAWS appreciate this opportunity to provide comments structured around the questions posed in the Consultation Document. Our comments are italicised in the following.

The CLSR, IAITL and ILAWS acknowledge the assistance of materials prepared by Nigel Waters and Graham Greenleaf of the *Cyberspace Law & Policy Centre at UNSW, Australia*.

2. Comments

2.1. Object and scope of the Convention, definitions

1. Convention 108 has been drafted in a technologically neutral approach which keeps it general and simple: can this still be the case or should a more detailed text be prepared?

Submission: The Convention should remain a simple, concise and technologically neutral instrument, while at the same time recognising and addressing some new characteristics of the present and future technological environment, in ways which we explain below.

Whilst context is important and so, for example, a list of 100 target mobile phone numbers in the hands of a private detective might have significant impact upon the individuals concerned, this can be regulated under general criminal law principles rather than data protection rules. The task is not a simple one and the principles of technological neutrality have value. Legal progress, however, should not be neutered by technology. A situation where hundreds of millions of mobile phones come within the legislation, but where there is no realistic prospect of enforcement can only bring the underlying legal concepts into disrepute.

2. Should Convention 108 give a definition of the right to data protection and privacy?

Submission: No. It would not be helpful to try to define the right to privacy in a data protection Convention – it is a set of interests which manifest themselves in different ways in different contexts, and sometimes need to be balanced against other interests. It is more appropriate to express them as a set of broad principles. There are other instruments such as the European Convention on Human Rights, and the case law interpreting it, where broad statements of privacy protection are appropriate, and different mechanisms used for enforcement.

3. Convention 108 protects against privacy intrusions by private and public authorities, including law enforcement. Should this comprehensive approach be retained?

Submission: Yes, it is important that the Convention and its principles apply broadly – any areas in which derogations from some principles may be justified need to be specific and focussed.

4. Convention 108 does not exclude from its scope data processed by a natural person in the course of a purely personal or household activity. Should this continue to be the case or should a specific exception be introduced (and specifically considered in the context of Web 2.0)?

Submission: This is a difficult issue – full application of privacy principles to the behaviour of private individuals would be onerous and oppressive – threatening other important freedoms and rights. But modern technology

increasingly allows individuals to threaten the privacy of others in ways that were previously only available to organisations, and some controls and restrictions are therefore justified. This is best handled by a broad statement of privacy protection in the ECHR and similar human rights instruments, at the international level. Some consideration could be given to making the privacy protections in those instruments more specific. At the national level, the issue is best dealt with by statutorily defined rights of privacy where interpretation by the Courts has a major role.

5. The definition of automatic processing does not include the collection of data: is it a problem if collection is subject to a special provision? Is it enough? Should other operations be added to the existing list?

Submission: The only principle currently applying to collection is in Article 5 – that personal data undergoing automatic processing shall be: (expressly, in (a)) “obtained and processed fairly and lawfully”, and (implicitly) that data collected should be “adequate, relevant and not excessive ...” (in (c)) and “accurate” (in (d)). We submit that it would be helpful to include “collection” in the definition of automatic processing so that all of the principles apply, where relevant, to collection. The principle needs to be strengthened by inclusion of a specific requirement that collection should not be excessive, and perhaps that it should not be by intrusive means. However, the “data minimisation principle” (see response to Q9) is another way to achieve at least the first objective.

6. The definition of the controller of the file should be reviewed: should several criteria be listed, should such criteria be cumulative, can there be several controllers for one file?

Submission: The definition is satisfactory, criteria are and should be independent and there ought to be allowance made for several controllers for one file.

The classic formulation is that a data controller is the entity which controls the extent to which data may be processed. It is based very largely on the precept that data is held in the same manner that a library may be held to control the books on its shelves. This is less relevant in a networked environment with systems of data sharing and matching being used increasingly in both the public and the private sectors. It is becoming increasingly difficult for data subjects to seek a meaningful answer to the question what data a controller might store when the real issue concerns the extent of the data which the controller might access. There can be no perfect answer but where there are formal systems of data sharing or matching there should be a requirement to nominate one entity as having overall responsibility (as is the case with systems of binding corporate rules under the EU data protection directive). There should also be an obligation upon individual data controllers to include in their response to individual subject information requests data relating to formal data matching or sharing networks in which they participate along with details of the coordinating entity.

7. New definitions may be necessary, such as for the processor or the manufacturer of technical equipment.

Submission: These new definitions would only be necessary if provisions were inserted referring expressly to these entities. This may be necessary if provisions concerning “privacy by design” are included, because it is essential that such a principle should apply to those designing technical equipment and not merely those utilising it, as it may be too late to factor in (or retro-fit) appropriate privacy protections once technologies are built without them. (see response to Q17)

See also response to Questions 15 and 21 below concerning the definition of “personal data”.

2.2. Protection principles

8. New principles could be added to the Convention, such as the **proportionality** principle, which should apply to all operations carried out on the data. Such a principle is also linked to the **data minimisation principle** which aims at limiting the collection of personal data to a strict minimum or even to cease personal data collection when possible.

Submission: These are both significant principles which could valuably be added, and we strongly support their inclusion. At the level of general principles there can be little to object to or criticise in the underlying principles. As always, the devil is in the detail and in some important respects there may be need to update the definition of concepts in order better to meet the needs of modern data-processing realities.

There has been some discussion recently of the value of establishing a right to be forgotten in respect of online data – that is, people should be able to give informed consent to every site or service that processes their data, and they should also have the right to ask for all of their data to be deleted. If companies don’t comply, citizens should be able to sue.

This is a topic which might benefit from expansion of the existing requirement that data shall not be retained for longer than is necessary for the purposes for which it was first processed. Given our increasingly networked world there will be obvious difficulties in ensuring compliance with such an obligation but there might be merit in requiring the original processor to inform the data subject of the period for which data will be retained by them. In the case of a social networking website, it might be feasible to indicate that members will be contacted after 2 years with the request that they confirm whether they wish their details be retained. There might be debate whether an opt in or opt out approach would be preferable. The advantage of the former approach is that many users may have changed emails and forgotten about the existence of a page.

9. Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

Submission: The concept of consent is fraught with difficulty in a data protection context. If it is used, it needs to be expressly defined as meaning free, voluntary, informed and revocable at any time, and not bundled with other consents. Effective consent requires comprehensive information about

the range and origin of linked data, the purpose of the profile and how it will be used, the controller and planned date of deletion. If consent is withdrawn, the profile must be immediately deleted, also by those controllers to which it has been transmitted. There are many current transactions which misleadingly use ‘consent’ when they in reality amount only to “notice, and acknowledgement that nominated uses/disclosures are a condition of the transaction”. There should be a general principle that where genuine consent is a realistic option, it should be the preferred basis of fair processing (subject to other public interest exceptions), consistent with the overall aim of transparency in transactions involving personal data.

Specific areas where there might be need for more explicit legislative provision might include the requirements imposed on data controllers to inform subjects of the uses to which data might be put. In the case of social networking sites, for example, this might include clear statements of privacy options and the positive and negative implications of choices which might be made by subjects. Provision might also be made regarding the default settings associated with such sites and data-processing general. It might, for example, be provided that a minimal range of access to or dissemination of data should be provided unless and until subjects make an informed choice to extend these.

10. Should the legitimate processing be addressed by Convention 108 as Directive 95/46 does in its article 7? Should there be a list of legitimate grounds for data processing?

Submission: No – fair and lawful (i.e. not unlawful), coupled with other general principles of proportionality, data minimisation and non-intrusive collection, are appropriate criteria – a list of positive grounds for processing would inevitably be incomplete.

11. Convention 108 does not expressly mention compatibility in relation to purpose. In today’s context, personal data is commonly used for purposes that go far beyond what may have been initially foreseen, far beyond what may be compatible with the initial purpose of the collection.

Submission: Compatibility is a subjective concept, and would be better expressed as “uses or disclosures” which are within the reasonable expectations of the data subject (to which a “reasonable person” test would be applied). However, it should be made explicit that “reasonable expectations” can only encompass uses or disclosures which a reasonable person would consider to be both fair and compatible with the original purpose of collection.

Uses and disclosures outside “reasonable expectations” should only be permitted with (genuine) consent or under a prescribed exception.

12. **Special categories of data** which benefit of an increased protection are defined very widely which could lead to excessive application of this restrictive regime: is the data sensitive or is its processing? Should other categories of data be added such as (national) identification numbers and biological or biometric data, etc.?

Submission: Unless the Convention is to specify the additional measures, then there is limited value in defining “special categories” or “sensitive data”. Sensitivity is in any case subjective and contextual, and any list is likely to be arbitrary and incomplete. The proposed introduction of proportionality and data minimisation principles (see Q8) could replace the need for a ‘special category’ provision.

Instead, we suggest a general definition of the term “sensitive data” as data which are capable by their nature of infringing fundamental freedoms or privacy, and mentioning specific types of data only as examples. If this provision is to specify the additional measures, it should include additional categories of data (such as biological, genetic and biometric data), and future developments of “new data”. It should avoid conclusive lists of particular data categories subject to a general prohibition on processing, which can be limited by extensive exceptions.

The Convention should, however, explicitly accept the rights of member states to provide a higher level of protection for data which provides a higher level of risk to privacy interests than other personal data, proportional to that higher risk.

13. A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

Submission: There is no need for specific protections for certain categories of data subject. The proposed introduction of proportionality and data minimisation principles (see Q8) should adequately address the concerns about children and other potentially vulnerable groups. The explanatory materials accompanying the Convention could make this clear.

14. Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

Submission: Yes, but not necessarily as part of a security principle – a right for data subjects to be informed of data breaches affecting them that meet specified threshold criteria should stand alone as a separate principle.

Data protection principles should encompass the notion of requiring that data subjects whose data may have been mislaid or which may have been made susceptible to unauthorised access should be informed about this possibility and advised as to possible remedial measures. Taken in a specifically UK context and considering in particular the reluctance of the police to volunteer to individuals information that their voice mail services may have been subject to acts of unauthorised access by private detectives working on behalf of journalists, there might be difficulty in determining where notification responsibilities might best be placed. The general principle of imposing breach notification obligations does seem clear.

15. There are special risks arising from the use of traffic and localisation data (technical data accompanying a communication) since such data can reveal movements, orientations, preferences and associations with others. Do we need special rules for the use of such data?

Submission: There would be no need for separate principles or rules for traffic or location data if personal data is defined as expressly including any information which enables or facilitates communication with a person on an individualised basis, whether or not it meets the current definition of personal data. This would include information about an individual's communications or location, and would include IP addresses, email address, other communications addresses, and geo-location data. (See also response to Q21 for additional inclusion of "behaviour" in the definition)

16. Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

Submission: Yes, there should be an obligation to demonstrate that measures have been taken to ensure full respect for data protection rules. Caution should be taken in the use of "accountability" which has been suggested in recent data protection debates as alternative to specific requirements for compliance with rules. In particular, "Accountability" cannot be and must not become an alternative to data export restrictions.

17. Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

Submission: Yes, privacy by design should be expressly encouraged. See further the response to Q22.

2.3. Rights – obligations

18. The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?

Submission: The right of access should include a right to be informed, on request, of the source of the data, also all recipients of the data (more specific than the general description given in collection notices), and also, where practicable, an explanation of the logic of the processing, e.g. credit scores.

19. The right of opposition is justified in cases where the data processing is not based on the data subject's consent. The articulation between the right of opposition and the right to oblivion could be examined, as well as means to guarantee respect and exercise of this right.

Submission: A right of opposition in the sense used in the EU Directive (Article 14); i.e. a right to opt out of processing,

should be included, even when consent was originally granted, if it is reasonable for consent to be revocable in the circumstances.

A right to oblivion (to be forgotten) needs further consideration, as there may be many circumstances in which it is unreasonable or impractical, and even conflict with other principles such as security or data integrity, or interfere with the audit trail needed for accountability

A "right to be forgotten" should at the very least encompass a requirement that personal data should be deleted or made inaccessible once the purpose for its collection is complete, though this does not meet all situations where such a right is needed or justifiable.

20. Should there be a right to guarantee the confidentiality and integrity of information systems?

Submission: There can be no absolute guarantee of confidentiality or integrity – only those "reasonable" measures or steps are taken. Supervisory authorities do, however, need to be much stricter in their enforcement of these principles.

The Convention (and other data protection codes) needs to be supplemented with more detailed rules on the quality of information systems.¹ More specifically, a set of rules should be drawn up stipulating that the development of information systems shall be oriented to maximising – within the boundaries of what is technically feasible and reasonable – the manageability, reliability, robustness, comprehensibility and accessibility of the systems, both from the point of view of systems users and of data subjects. Useful points of departure for the drafting of such rules are the core principles of the OECD Guidelines for the Security of Information Systems. Despite being somewhat prolix and, on their face, only tangentially relevant to data protection concerns, these principles are worth taking note of given the paucity of equivalent principles in data protection codes. The ideas they express should inspire the drafting of a similar set of rules dealing with the quality of information systems from a data protection perspective. The broad thrust of such rules would be as follows:

- a) Information systems shall be designed so as to improve the extent to which they are able to (i) automatically test aspects of the quality of the data/information they process, and (ii) communicate the results of such tests to the data controllers.
- b) Data controllers shall issue information quality declarations that describe the means by which the quality of information processed by the controllers has been checked, the results of such tests and any remaining uncertainty about the quality. The declarations shall be handed to the relevant data protection authorities.
- c) Formal agreement shall be reached as to (i) which person(s)/organisation(s) is/are directly responsible and liable for the quality of the information in the system concerned and (ii) how this quality is to be monitored.

¹ This part of our submission is drawn from Lee A. Bygrave, *Data Protection Law: Approaching Its Rationale, Logic and Limits* (Kluwer Law International, 2002), chapter 19.

- d) Data processors shall undergo training in order to be made aware of at least the following: (i) the core principles and rules of data protection; (ii) the basic rationale and importance of these principles and rules; (iii) how these principles and rules apply to their own work tasks.²
- e) Data controllers shall subject their information systems to periodical data protection audits by a competent and independent third party.³ These shall ascertain strengths and weaknesses in the data protection measures taken by the controller concerned. The rule should further stipulate conditions for disclosing the audit results to the relevant data protection authorities and the general public.
- f) Extending the latter rule, data controllers should be encouraged, if not required, to undertake ex ante assessments of the impact that their planned data-processing operations or planned changes to the information system(s) supporting such operations, might have on data protection interests. This kind of assessment tends to be championed under the name of “privacy impact assessment”. *The latter nomenclature is somewhat misleading as the assessment is intended to evaluate more than the possible effects of planned activity on privacy as such. Ideally, the assessment should be carried out by a competent and independent third party, and its results made public.*

Additionally, the central rules embodying the information quality principle should be reviewed to determine whether they adequately and consistently capture the various facets of information quality and the various facets of assuring such quality. Looking at current data protection laws, significant variation exists in terms of the degree of detail with which they formulate the dimensions of information quality. Concomitantly, there is some inconsistency in terms of the terminology they employ to describe these quality dimensions and the sorts of steps to be taken in quality assurance. Overall, these rules appear to have been drafted somewhat haphazardly. It is best to have honest rules; i.e., rules giving reasonable guidance, on their face, about what information quality and assurance of such quality involve. Information quality and quality assurance are both multifaceted. Rules on them should accurately reflect this fact, especially in view of the need for legal certainty on the part of data controllers and in view of the importance of ensuring adequate information quality in an age of increasing electronic interpenetration. This notwithstanding, some caution is vital when formulating requirements for quality assurance. Such

² Cf. principle 5.9 of the ILO Code of Practice on Protection of Workers’ Personal Data (1997) which stipulates: “Persons who process personal data should be regularly trained to ensure an understanding of the data collection process and their role in the application of the principles in this code”.

³ This sort of rule is present in section 9a of Germany’s Federal Data Protection Act of 1990 (as amended) (“Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und –programmen und Datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten sowie das Ergebnis der Prüfung veröffentlichen lassen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt”).

requirements have the potential of generating operating costs for data controllers which are disproportionately high relative to the risk of error causing detriment to the data subjects. Some form of “reasonable steps” standard is probably most appropriate. At the same time, this standard should not be determined solely or primarily by the needs of data controllers; rather, it should be linked primarily to what is necessary to ensure fair data-processing outcomes for the data subjects. A point of departure for drafting a general rule on information quality could be the following: “All reasonable steps shall be taken to check and ensure that data are correct, complete, relevant and not misleading in relation to what they are intended to describe and in relation to the purposes for which they are processed. In assessing what is reasonable, primary regard shall be given to the extent to which data-processing error can have detrimental consequences for the data subject(s).”

21. Should a right ‘not to be tracked’ (RFID tags) be introduced?

Submission: There is no need for a separate “right not to be tracked”, if personal data is defined as expressly including information about an individual’s communications, location or behaviour (See response to Q15)

22. Should everyone have a right to remain anonymous when using information and communication technologies?

Submission: An absolute right to anonymity is unreasonable and impracticable in many circumstances. Consideration should nonetheless be given to including more explicit and systems-active provisions on anonymity. Opportunities for anonymity should be promoted more obviously in the rules embodying the minimality principle. Indeed, allowance for anonymity should be made a basic data protection principle in itself. A principle similar to that already included in the Australian data protection law as the “anonymity principle”⁴ could be included. Suggested wording:

“Individuals must have the option of not identifying themselves when dealing with an entity, or of using a pseudonym, except where there is either a legal requirement for identification or where it is impracticable for the entity to deal with individuals who have not identified themselves or who use a pseudonym.”

At the same time, however, the Convention should additionally be infused with provisions explicitly addressing the need to develop organisational–technological infrastructures that promote transactional anonymity. A useful model provision in this regard is s 3a of Germany’s Federal Data Protection Act (“Gestaltung und Auswahl von Datenverarbeitungssystemen

⁴ See NPP 8 in Schedule 3 to Australia’s federal Privacy Act (“Wherever it is lawful and practicable, individuals should have the option of not identifying themselves when entering transactions”) and IPP 8 in Schedule 1 to the Information Privacy Act 2000 of the Australian State of Victoria (“Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation”).

haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht⁵). What is fairly unique about this provision⁵ is that it explicitly addresses the need to design information systems and other technological platforms to support the goal of minimality. This characteristic ought to be emulated in the Convention. This relates closely to the question of whether privacy-enhancing technologies (PETs) ought to receive greater legal support and if so, how. The answer is yes they do need such support and the rules on point can be easily formulated without breaking regulatory principles on technology-neutrality etc. The rules could be formulated so that they primarily stipulate the goals to be reached (e.g., of anonymity and/or pseudonymity), and their specification of the means for reaching these goals (e.g., in terms of systems development) could be done without singling out and promoting a specific PET.

Following on from the latter points, it is desirable that rules promoting anonymity be supplemented by rules promoting pseudonymity. The appropriate rules should stipulate anonymity as the primary option with pseudonymity as the first fall-back option when anonymity cannot be achieved for legal or technical reasons.

The above proposals should be augmented by rules dealing specifically with profiling. One such rule should be along the lines of § 21 in Norway's Personal Data Act which lays down a duty on the part of a data controller to supply a person with certain types of information about a profile when it (the profile) is used to establish contact with or make a decision about the person. The provision does not require notification of the logic or assumptions behind the profile concerned; nor does it specify the time frame in which the information is to be provided. New rules modelled on § 21 should correct the latter omission by specifying that the information be supplied at the time contact with the person is made. They should additionally require notification of the logic or assumptions behind the profile, at least when it is used to ground a decision significantly affecting the person's rights or interests. The new rules should also make clear that the duty they lay down applies not just in relation to specific profiles but also abstract profiles. The introduction of a duty of information along the lines drawn here will also involve a duty on the part of data controllers to document the profiles and the logic used to generate them.

The traditional definition of 'personal data' should be made more flexible by supplementing the identifiability criterion with a contactability/reachability criterion. More specifically, "personal data" would be defined as data that facilitate either identification of a particular individual or contact to be made with him/her.⁶ This strategy might well prove useful in an Internet context where there is uncertainty as to whether, say,

a machine address is "personal data", yet where the person(s) using the address are subjected to profiling or to measures instituted on the basis of profiling.

23. Should Convention 108 address the question how to strike the balance between the protection of personal data and freedom of expression (new notion of press and journalism in the context of Web 2.0)?

Submission: It is not appropriate for the Convention itself to try to balance every aspect of these interests, but some recognition of the public interest in freedom of expression would be desirable.

2.4. Sanctions and remedies

24. Should class actions be introduced in the Convention? Should more scope be given to alternative dispute resolution mechanisms?

Submission: The Convention does not currently expressly provide for complaints about breaches of the principles/rules – only for remedies where requests for correction etc are denied (Article 8(d)). If the Convention is to include a requirement for complaint or ADR mechanisms, then it would be appropriate for it to expressly recognise the value of representative complaints (class actions).

2.5. Data protection applicable law

25. Should a rule determining the applicable law to the data processing (in cases where different jurisdictions are involved) be considered?

Submission: There may be more than one applicable law – both general and sectoral data protection laws and other laws with privacy related provisions. Insofar as data protection laws are concerned, it would be of value if, in relation to likely areas of conflict of laws, the Convention did state a choice of law rule.

2.6. Data protection authorities

26. How to guarantee their independence and ensure an international cooperation between national authorities

Submission: Supervisory authorities are only provided for expressly in the 2001 Additional Protocol to the Convention (CETS 181), and these provisions could usefully be incorporated in the Convention itself (see response to Q26 below). Clause 3 of Article 1 of the Protocol mandates independence, while Clause 5 requires international cooperation. It is probably not appropriate for the Convention to try to specify how these requirements are to be met.

We welcome the intention of strengthening and clarifying the status and powers of the data protection authorities and to fully implement the concept of "complete independence". National authorities are notoriously understaffed. To be effective they must have the resources as well as the powers to do their job.

⁵ There is some trace of it also in recital 30 of the preamble to EU Directive 2002/58 ("Systems for the provision of electronic communications networks and services should be designed to limit the amount of personal data necessary to a strict minimum").

⁶ Cf. § 21 of the Norwegian Act. 2.

27. Should their role and tasks be specified?

Submission: Article 1 of the Additional Protocol (CETS 181, 2001) specifies roles and functions of supervisory authorities. This should be incorporated in the Convention itself.

One particular task of a supervisory authority that needs to be spelled out is the obligation to account for their performance of their complaint investigation obligations, including by reporting to the public, on objectively determined criteria, of cases investigated (anonymised to the extent necessary to protect privacy but not otherwise), and by statistics including statistics concerning outcomes and remedies. Supervisory authorities must be able to demonstrate that they deliver remedies to complainants; otherwise their existence can simply be a cover for expanded surveillance activities.

The establishment of dedicated supervisory authorities has become a key component of European notions of data protection. In most countries, a single agency has been established. This does perhaps raise an initial issue. If an organisation is subject to review by another regulator such as one operating in the financial services sector there may be an undesirable element of overlap if it is also subject to the data protection authorities. Just as the European data protection Directive sanctions the establishment of independent data protection supervisors within undertakings as serving to exempt that body from some elements of the normal supervisory regime, so the role for sectoral supervisory authorities whose remit extends beyond data protection might be considered.

Alongside supervisory agencies, systems of licensing/registration/notification have become a key component of legislation. The time may have come to consider whether they serve any useful purpose. Cross reference might be made to the regulation of telecommunications in the EU where established systems requiring prior authorisation have been swept away and replaced by ex post regulatory schema. There may well be data-processing systems whose potential and intended impact on society might require some system of prior assessment, but it is not clear that the current systems of near universal registration offer benefits commensurate with the cost implications for both data controllers and the supervisory authority. A much more focused approach is required to avoid the danger that a disproportionate amount of the supervisory agency's resources are expended in ensuring that controllers have ticked the most appropriate boxes.

In line with approaches in telecommunications regulation, the vast proportion of data controllers should, whilst remaining subject to the requirement to comply with substantive legislative requirements, be exempted from the procedural burdens associated with notification. Apart from the suspicion that many controllers may not have notified details of their processing activities to the supervisory authority, it is difficult to see what value there is for the public in having a register of data-processing activities. If a subject knows of a particular activity, there will be no need to consult a register. If they do not know, such registers will offer little practical help in determining who processes the subject's personal data and for what purpose. The only practical value

of notification in countries such as the United Kingdom is as providing the only significant source of revenue to the supervisory authority. Again, lessons might usefully be learnt from recent reforms introduced into the European telecommunications legislation which impose an obligation on Member States to ensure that regulatory agencies are adequately resourced in terms both of financial and human resources. The latter point may be of significance in many instances. Criticisms have been made that the staff of supervisory have lacked the technical knowledge necessary to investigate activities such as the acquisition of large amounts of personal data by Google in the course of its Street Views project. Again, whilst there is a case for making those whose processing activities are capable of impacting on large numbers of data subjects or which relate to sensitive data, it is difficult to justify the imposition of what is effectively a tax on computer users. Again borrowing from the telecommunications sector, charges for the services provided by supervisory agencies should be proportionate to the costs incurred and benefits provided. For the majority of data controllers, it is unclear that costs are incurred by supervisory agencies or that any benefit is obtained by the controller.

2.7. Transborder data flows

28. The aim of Convention 108 was to reconcile effective data protection with the free flow of information, regardless of frontiers. The Convention's principles have been further developed in an additional protocol (CETS 181, 2001). In principle, an adequate level of protection must be ensured.

Submission: It remains appropriate to require an adequate level of protection as a condition of cross-border transfer. Member states of the Convention should require that the personal data concerning their citizens is protected if it leaves their jurisdiction. The provisions of the additional protocol should be moved inside the Convention.

The Convention (and the European Directive) provide as a start point to their provisions on data transfers outside Member States that these are automatically sanctioned only if the recipient state will ensure an adequate level of protection. In spite of the mechanism for making findings of adequacy under the Directive, few states of any size or significance have been acclaimed as ensuring adequacy.

A dictionary definition of adequacy refers to notions of acceptability or basic fitness for purpose. Many of the Decisions reached by the European Commission on the issue of adequacy seem to require something closer to equivalence. This may be of considerable significance. A Volkswagen Golf is an adequate motor car but it probably would not be considered equivalent to a Rolls Royce. A more precise definitional approach in a revised Convention might make the process more transparent than is currently the case and could serve as a spur for the development of widely accepted standards of data protection. The Convention affords states the possibility of applying higher standards internally and this should be maintained. The current approach towards transborder data flows is not working. The early English/Danish King, Canute, is famous for commanding the incoming sea tide to go back –

and getting his feet wet as a consequence. The tale is generally held to depict the vanity and stupidity of the King. An alternative and perhaps more plausible interpretation is that he was trying to show over-deferential courtiers that he was not all powerful. On this account, the folly lay in those seeking to impose controls on forces which could not be mastered. In our networked world, there are limits to the extent to which data flows can be (as has been discovered by states such as Egypt and Tunisia) or should be controlled.

The current European approaches towards transborder data flows are not working effectively. They are burdensome to those whose motives are benign and ineffective towards those more malignly inclined. Problems are, of course, exacerbated by widely differing national approaches towards the regulation of transborder data flows. Whilst some states require prior approval, others have systems of notification whilst others have no *ex ante* controls whatsoever. These matters could certainly be addressed with more precision in a revised Convention, but the basic problem is perhaps that legislative structures designed for an era of stand-alone mainframe computers struggle to cope in a networked environment. A prime focus of any revision of Convention 108 should be to make it a more attractive instrument for ratification by non Member States.

29. Do we need to reconsider the notion of “transborder data flows” altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?

Submission: Globalisation of “minimum rules” is not desirable at all. It would simply be a “race to the bottom” which would destroy any value in cross-border privacy protection. The Convention should establish the standard of protection it requires for citizens of member states, and adhere to that.

30. Should there be different rules for the public and private sector? In particular as regards the private sector, should more use be made of binding corporate rules, possibly combined with rules on accountability of the final recipient to ensure respect for such rules?

Submission: The same basic principle of cross-border transfer conditions should apply equally to the public and private sectors.

2.8. Role of the consultative committee

31. Convention 108 established a committee to facilitate its application and, where necessary, to perfect it. Should

the so far primarily consultative role of the committee be strengthened? If so, which functions should be developed further? Standard-setting, dispute resolution, monitoring functions?

Submission: The monitoring and standard-setting functions of the Consultative Committee should be strengthened.

3. Conclusion

There is little in the data protection principles with which anyone could disagree. Application is another matter and 30 years on the prime task for revision of the Convention should be to make the instrument the basis for global consensus regarding the manner in which personal data should be processed. The modernisation of the Convention reflects the recognition of the broadening scope of data protection guideline which would enable a universal regulation for Europe and the rest of the world.

We hope that the Expert Committee of the Council of Europe takes in consideration our view and proposals in respect to the modernization of the Convention.

Respectfully Submitted

Prof Sylvia Kierkegaard, (Sylvia.Kierkegaard@iaitl.org) President International Association of IT Lawyers; CLSR Editorial Board Member; Senior Research Fellow, ILAWS; Visiting Professor, University of Southampton.

Nigel Waters, (nigelwaters@iprimus.com.au) Visiting Fellow at UNSW Law Faculty and formerly Deputy Commonwealth Privacy Commissioner.

Prof. Graham Greenleaf, (graham@austlii.edu.au) CLSR Editorial Board Member; Professor of Law & Information Systems, University of New South Wales (UNSW); Co-Director, Australasian Legal Information Institute (AustLII); Founding Director, Cyberspace Law and Policy Centre, UNSW.

Assoc. Prof. Lee A. Bygrave, (l.a.bygrave@jus.uio.no) Norwegian Research Center for Computers and Law, Department of Private Law, University of Oslo; CLSR Editorial Board Member.

Prof. Ian Lloyd, (i.lloyd@soton.ac.uk) Senior Research Fellow, ILAWS, University of Southampton; CLSR Editorial Board Member.

Prof. Steve Saxby, (s.j.saxby@soton.ac.uk) Research Director and Director of ILAWS, Faculty of Business and Law, University of Southampton, United Kingdom, Editor-in-Chief CLSR.