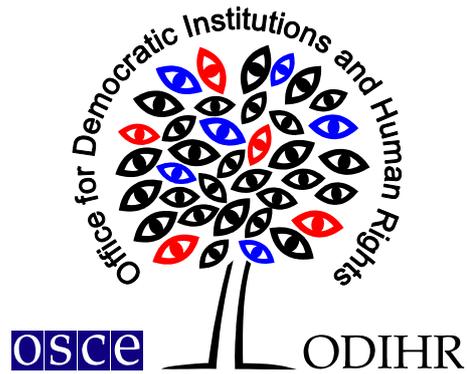


Warsaw, 6 May 2008

[Opinion-Nr.: FOI –
ARM/107/2008 (IU)]

www.legislationline.org



**OSCE Office for Democratic
Institutions and Human Rights**

**OSCE Office of the
Representative on
Freedom of the Media**

**JOINT OSCE ODIHR AND OSCE RFOM OPINION
ON THE DRAFT LAW OF THE REPUBLIC OF ARMENIA
ON INFORMATION, INFORMATION TECHNOLOGIES
AND PROTECTION OF INFORMATION**

TABLE OF CONTENTS:

1. INTRODUCTION

2. SCOPE OF REVIEW

3. EXECUTIVE SUMMARY

4. ANALYSIS AND RECOMMENDATIONS

I. INTRODUCTION

1. On April 2, 2008, the OSCE ODIHR was requested by the OSCE Office in Yerevan to review the draft Law of the Republic of Armenia on Information, Information Technologies and Protection of Information (hereinafter referred to as “Draft” or “draft Law”). The OSCE Office in Yerevan had in turn been requested to arrange for a review by the Ministry of Transport and Communications of the Republic of Armenia.
2. The Opinion is jointly endorsed by the OSCE ODIHR and the OSCE Office of the Representative on Freedom of the Media (OSCE RFOM).
3. This Opinion has been prepared based on the Armenian original and the unofficial English translation of the draft Law.

II. SCOPE OF REVIEW

4. The Opinion analyzes the draft Law in terms of its compatibility with relevant international and regional standards and OSCE commitments. The Opinion also examines the Draft in light of both relevant case law and international good practice relating to information security and data protection.
5. In addition to standards which are legally binding upon the Republic of Armenia, this Opinion also refers to non-binding international instruments including documents of a declarative or recommendatory nature which have been developed for the purpose of interpreting the relevant provisions of international treaties.
6. The OSCE ODIHR and the OSCE RFOM note that the opinion provided herein is without prejudice to any other opinions or recommendations that the OSCE ODIHR and the OSCE RFOM may wish to make on the issues under consideration.

III. EXECUTIVE SUMMARY

7. The draft Law addresses an increasingly important issue of information security and information management, and may become a welcome addition to other domestic laws dealing with access to information and data protection issues, provided that a number of concerns are adequately addressed. These concerns include insufficient clarity and specificity of some provisions of the Draft, which reduces their predictability and is likely to create problems with interpretation and implementation. Another concern is with the requirement for information holders and/or persons disseminating information to disclose their identity, since mandatory identity disclosure does not offer a viable solution to cybercrime problems and is at odds with freedom to impart information and ideas. Narrowly tailored provisions criminalizing impersonation and identity theft are recommended as a substitute. Moreover, the Draft does not provide for effective and dissuasive mechanisms to deal with breaches. In particular, this concerns the issue of unsolicited electronic communications (“spam”). One final concern is with the inadequate realization that protections should also extend to personal data collected and stored by private sector entities.
8. Below follows a detailed list of recommendations:

- a) It is recommended that the definition of “information” be revised to clarify that the draft Law concerns information irrespective not only of the form, but also of the medium. [Article 4]
- b) It is recommended that the Law on Personal Data be added to the list of laws in Article 2, and the provisions of the Draft concerning personal data protection be substituted or complemented with references to the Law on Personal Data to ensure clarity and consistency across the array of relevant domestic legal acts. [Article 2]
- c) It is therefore recommended that the provisions concerning guarantees and key principles be revised to improve clarity and specificity. In particular, it is recommended that the provisions concerning the power to make exceptions only on the grounds provided for by the Constitution and as prescribed by law be complemented by the requirement that exceptions may only be made where strictly necessary in democratic society, as well as by a list of restrictively enumerated legitimate grounds for exceptions. It is also recommended that the guarantee of “*protection of everyone’s privacy*” be replaced by a ban on collecting or processing information in unlawful ways and reinforced by adding principles such as that of the purpose specification, of interested person access and of non-discrimination. [Articles 4 and 5]
- d) It is recommended that the provisions concerning categories of information banned from dissemination be reviewed for better clarity, which may entail making changes to other related provisions of the draft, in particular Article 3 that concerns definitions. The placement of Article 4(4) under the provisions concerning guarantees may also be reconsidered due to a high level of specificity of the issues it aims to address. In particular, it is recommended that definitions of what constitutes “*national, racial or religious hatred*” be added to Article 3 in compliance with the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems. In addition, it is recommended that the ban on disseminating child pornography be strengthened and expanded to prohibit also producing, importing, exporting, offering, selling or possessing child pornography. It is also recommended that a definition of child pornography consistent with that given by the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography be added to Article 3. [Articles 3 and 4(4)]
- e) It is recommended that the typologies introduced by Article 7 be reviewed and streamlined, as well as references to relevant domestic legislation provided where applicable. The Draft would also benefit from incorporating the overriding public interest test. [Article 7]
- f) It is recommended that the requirement for information holders and/or persons disseminating information to disclose their identify be removed, and a prohibition of identity theft and impersonation, as well as a prohibition of altering routing information to disguise the origins of the electronic communication, be incorporated. [Article 12(2)]

- g) It is recommended that the Draft be revised to single out those types of unsolicited communications that result in costs imposed on parties other than the sender, and to introduce effective and dissuasive remedies against the prohibited conduct. In particular, it is recommended that the Draft create a possibility for end recipients as well as for equipment owners (such as owners of networks and/or servers) to sue spammers. [Article 12(3)]
- h) It is recommended that the Draft include a provision forbidding organizations, as a condition for supplying a product or a service, from requiring individuals to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service. [Article 12(4)]
- i) Since companies and organizations cannot bear absolute responsibility for preventing information security incidents, it is recommended that Article 21 be reviewed to require that corporate entities bear a general duty to provide reasonable controls to protect the integrity, confidentiality, availability and authenticity of data. It is also recommended that the wording of the provision requiring entities to timely detect information security breaches and to issue “*warnings on the possible unfavorable effects*” be clarified to ensure clarity and consistency in its interpretation. If its intent is to make it mandatory for organizations and companies to notify information security breaches to law enforcement bodies and to data subjects who may be affected or injured (such as customers whose personal data are stored by a company), then the provision is very welcome. [Article 21]

IV. ANALYSIS AND RECOMMENDATIONS

4.1 Definitions and relationship with other relevant domestic legislation

- 9. The Draft would benefit from better consistency of its definitions with those contained in relevant domestic legislation, most importantly, the Law on Freedom of Information and the Law on Personal Data. In particular, it is recommended that the definition of “information”¹ be revised to clarify that the draft Law concerns information irrespective not only of the form, but also of the medium, as already done by the definition given by the Law on Freedom of Information.
- 10. In addition, some provisions of the Draft, in particular those concerning the protection of personal data,² appear to be redundant as the issues they intend to regulate are already addressed by other domestic laws. Redundancy here is a cause for concern by virtue of the vagueness and uncertainty that it creates, ultimately resulting in problems with statutory interpretation, especially given that both the Draft and the Law on Personal Data are specialized legal acts and the principle *lex specialis derogat legi generali* would therefore not apply. It is recommended that the Law on Personal Data be added to the list

¹ Draft Law on Information, Information Technologies and Protection of Information, Article 3(1) (“*Information: news reports, communications and data irrespective of their form of presentation.*”)

² *Id.*, Article 4 (“*2. Collecting, preserving, using or disseminating information on a person’s private or family life, without their consent, shall be prohibited. 3 Demanding from a natural person to provide information on their private life, including such that constitutes a private or family secret and obtaining such information contrary to a natural person’s will, except for cases envisaged by the law, shall be prohibited.*”)

of laws in Article 2,³ and the provisions of the Draft concerning personal data protection be substituted or complemented with references to the Law on Personal Data.

4.2 Guarantees and key principles

11. It is welcome that the Draft expressly provides for key principles such as free access to information,⁴ power to make exceptions only on the grounds provided for by the Constitution and as prescribed by law,⁵ and presumption of openness.⁶
12. The wording of the provisions is, however, not necessarily clear, which poses a risk of implementation problems once the law is passed, and is at odds with the principle of legality, which requires that the law be clear, ascertainable and the consequences of a breach foreseeable. It is therefore recommended that selected provisions be revised to improve clarity and specificity.
13. First, to improve consistency with international and European standards in the area of access to information and data protection, it is recommended that the provisions concerning the power to make exceptions only on the grounds provided for by the Constitution and as prescribed by law be complemented by the requirement that exceptions may only be made where strictly necessary in democratic society, as well as by a list of restrictively enumerated legitimate grounds for exceptions. In doing so, and in addition to relevant provisions of the European Convention for the Protection of Human Rights and Fundamental Freedoms⁷ (hereinafter referred to as “ECHR”), the legislator may wish to consider relevant provisions of the Council of Europe Convention for the

³ The Draft as it stands now only lists the Laws on Mass Media, on Freedom of Information, on Archiving, on State and Official Secrets, and on Electronic Documentation and Electronic Digital Signature.

⁴ Draft Law on Information, Information Technologies and Protection of Information, Article 5 (“[F]reedom to exercise the right to seek, receive, transmit, produce and disseminate information by any lawful means.”)

⁵ *Id.* (“[R]estrictions on the access to information shall be prescribed by law on the grounds envisaged by the Constitution of the Republic of Armenia.”)

⁶ *Id.* (“Public nature of information on the activities of the bodies of public administration and local self-governance and free access to this information except for cases prescribed by law.”)

⁷ Convention for the Protection of Human Rights and Fundamental Freedoms, Articles 8 (“1. Everyone has the right to respect for his private and family life, his home and his correspondence. 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.”) and 10 (“1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.”)

Protection of Individuals with Regard to Automatic Processing of Personal Data⁸ (hereinafter referred to as “Data Protection Convention”). Albeit not a signatory to the Convention, being a Council of Europe Member State Armenia may find the Convention of high recommendatory value.

14. In particular, the Data Protection Convention prohibits exceptions to its Articles 5,⁹ 6¹⁰ and 8¹¹ may only be made if specifically provided for by law and necessary to protect “*State security, public safety, the monetary interests of the State or the suppression of criminal offences*” or to protect “*the data subject or the rights and freedoms of others.*” Note that the list of legitimate grounds for exception in the case of processing personal data slightly differs from the list of grounds provided for by Article 8 of the ECHR.¹² For instance, protecting public morals cannot be invoked as a ground for exception.
15. Second, it is not clear what is meant by the guarantee of “*protection of everyone’s privacy.*”¹³ It is recommended that this guarantee be replaced by a ban on collecting or processing information in unlawful ways and reinforced by adding principles such as that of the purpose specification, of interested person access and of non-discrimination.
16. The principle of purpose specification as defined by the U.N. Guidelines for the Regulation of Computerized Personal Data Files¹⁴ requires that “*[t]he purpose which a file is to serve and its utilization in terms of that purpose should be specified, legitimate and, when it is established, receive a certain amount of publicity or be brought to the attention of the person concerned, in order to make it possible subsequently to ensure*

⁸ Available on the web at

<http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=108&CM=7&DF=4/11/2008&CL=ENG>

(last visited on April 11, 2008).

⁹ Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Article 5 (“*Personal data undergoing automatic processing shall be: (a) obtained and processed fairly and lawfully; (b) stored for specified and legitimate purposes and not used in a way incompatible with those purposes; (c) adequate, relevant and not excessive in relation to the purposes for which they are stored; (d) accurate and, where necessary, kept up to date; (e) preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored.*”)

¹⁰ *Id.*, Article 6 (“*Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life, may not be processed automatically unless domestic law provides appropriate safeguards. The same shall apply to personal data relating to criminal convictions.*”)

¹¹ *Id.*, Article 8 (“*Any person shall be enabled: (a) to establish the existence of an automated personal data file, its main purposes, as well as the identity and habitual residence or principal place of business of the controller of the file; (b) to obtain at reasonable intervals and without excessive delay or expense confirmation of whether personal data relating to him are stored in the automated data file as well as communication to him of such data in an intelligible form; (c) to obtain, as the case may be, rectification or erasure of such data if these have been processed contrary to the provisions of domestic law giving effect to the basic principles set out in Articles 5 and 6 of this convention; (d) to have a remedy if a request for confirmation or, as the case may be, communication, rectification or erasure as referred to in paragraphs b and c of this article is not complied with.*”)

¹² Article 8 of the ECHR concerns the right to respect for private and family life.

¹³ Draft Law on Information, Information Technologies and Protection of Information, Article 4(1)(2).

¹⁴ U.N. General Assembly A/RES/45/95. Full text of the Guidelines is available on the web at <http://www.un.org/documents/ga/res/44/a44r132.htm> (last visited on April 10, 2008).

that: (a) the personal data collected and recorded remain relevant and adequate to the purposes so specified; (b) None of the said personal data is used or disclosed, except with the consent of the person concerned, for purposes incompatible with those specified; (c) The period for which the personal data are kept does not exceed that which would enable the achievement of the purpose so specified.”¹⁵ This principle is also provided for, albeit to a more limited extent, by the CIS Model Law on Information, Informatization and Protection of Information which requires that “*the receipt, processing and use of personal data be restricted to the specified purpose they are collected for.*”¹⁶

17. The principle of interested person access is spelled out by the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data. Albeit not a signatory to the Convention, being a Council of Europe Member State Armenia may find the Convention of high recommendatory value. The principle of interested person access requires that anyone be enabled to establish the existence of his or her own personal data file and its main purposes, as well as to obtain rectification or erasure of such data if these have been processed contrary to the provisions of domestic law.¹⁷
18. The principle of non-discrimination prohibits automated processing of data that are likely to give rise to discrimination, such as data relating to racial or ethnic origin, religious beliefs, sexual orientation, political opinions or membership in associations.¹⁸ As already discussed in paragraph 14, exceptions to this rule may only be made if specifically provided for by law and necessary to protect “*State security, public safety, the monetary interests of the State or the suppression of criminal offences*” or to protect “*the data subject or the rights and freedoms of others.*”
19. On a final note, it is recommended that Article 4(4) concerning categories of information banned from dissemination be reviewed for better clarity, which may entail making changes to other related provisions of the draft, in particular Article 3 that concerns definitions. The placement of Article 4(4) under the provisions concerning guarantees may also be reconsidered due to a high level of specificity of the issues it aims to address.
20. In particular, it is recommended that definitions of what constitutes “*national, racial or religious hatred*” be added to Article 3 in compliance with the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems.¹⁹

¹⁵ U.N. Guidelines for the Regulation of Computerized Personal Data Files, Principle 3.

¹⁶ CIS Model Law on Information, Informatization and Protection of Information, Article 4 (“[O]граничение получения, обработки и использования персональных данных целями, для которых они собираются.”)

¹⁷ See Footnote 10.

¹⁸ See Footnote 9.

¹⁹ Ratified by the Republic of Armenia on October 12, 2006. The Additional Protocol defines “*racist and xenophobic material*” as “*any written material, any image or any other representation of ideas or theories, which advocates, promotes or incites hatred, discrimination or violence, against any individual or group of individuals, based on race, colour, descent or national or ethnic origin, as well as religion if used as a pretext for any of these factors.*” Full text of the Additional Protocol is available on the web at <http://conventions.coe.int/Treaty/Commun/QueVoulezVous.asp?NT=189&CM=7&DF=4/11/2008&CL=ENG> (last visited on April 11, 2008).

21. In addition, it is recommended that the ban on disseminating child pornography be strengthened and expanded to prohibit also producing, importing, exporting, offering, selling or possessing child pornography. This would improve the compliance of the provisions in question with the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography.²⁰ It is also recommended that a definition of child pornography consistent with that given by the Optional Protocol²¹ be added to Article 3.

4.3 Typology of information

22. The Draft distinguishes between “*information in the public domain*” and “*information with restricted access*” based on the degree of access criteria. It also groups information according to dissemination procedure into the following categories: public/non-classified (“*freely disseminated information*”); information access to which cannot be limited (“*information subject to provision or dissemination by law*”); restrictable information (“*information with restrictions on dissemination including information provided with restrictions established with the consent of persons that are parties to the relations*”); and information classified as secret by law (“*information whose dissemination is prohibited by law or international treaty.*”)²²
23. The line between the two typologies is blurred, both essentially being based on the degree of access criterion. It is recommended that the typologies be reviewed and streamlined. While there are no international standards governing information classification specifically, and the domestic legislator is certainly in the best position to assess potential solutions and choose the one best suited to the national context, it may be recommended that the Draft distinguish between categories of (a) public/non-classified information; (b) information access to which is restricted or prohibited by law (including personal data; state and official secrets; or information subject to legal privilege, such as attorney-client or physician-patient privilege); and (c) information restrictable by the information holder (such as trade secrets of the information holder). It is also recommended that the Draft clearly indicate which types of information are covered by each of the categories, and

²⁰ Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, Article 3(1) (“*Each State Party shall ensure that, as a minimum, the following acts and activities are fully covered under its criminal or penal law, whether such offences are committed domestically or transnationally or on an individual or organized basis: [...] (c) Producing, distributing, disseminating, importing, exporting, offering, selling or possessing for the above purposes child pornography as defined in article 2.*”) The Optional Protocol was ratified by the Republic of Armenia on June 30, 2005. Full text of the Optional Protocol is available on the web at <http://www2.ohchr.org/english/law/crc-sale.htm> (last visited on April 11, 2008).

²¹ *Id.*, Article 2(c) (“*Child pornography means any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes.*”)

²² Draft Law on Information, Information Technologies and Protection of Information, Article 7 (“*1. Depending on the degree of access, information shall be classified into information in the public domain and information with restricted access. 2. Depending on the means of dissemination or provision, information shall be classified into: 1) freely disseminated information; 2) information subject to provision or dissemination by law; 3) information with restrictions on dissemination, including information provided with restrictions established with the consent of persons that are parties to the relations; 4) information whose dissemination is prohibited by law or international treaty. 3. The legislation of the Republic of Armenia may define types of information according to the content and administrator of information.*”)

provide references to relevant domestic legislation (such as the Law on Freedom of Information, the Law on State and Official Secret, and the Law on Personal Data) where applicable. Furthermore, it may be recommended that the Draft spell out the types of information access to which cannot be restricted. This can be possibly done via including references to relevant provisions of the Law on Freedom of Information. Finally, the Draft would benefit from incorporating the overriding public interest test. This means that where public interest in disclosure of a particular record outweighs the potential harm or injury arising from such disclosure, the disclosure should be made possible.

4.4 Mandatory information holder/disseminating person identification

24. The Draft makes it mandatory for information holders and/or persons disseminating information to disclose their identity in cases where information is disseminated through channels other than mass media.²³ This requirement virtually outlaws anonymous dissemination of information and raises a serious concern as an encroachment on the freedom to “*impart information and ideas without interference by public authority.*”²⁴ Furthermore, mandatory identity disclosure serves no valid purpose from a pure policy viewpoint, since there already exist ample possibilities under the Code of Criminal Procedure to establish the identity of the person disseminating information in violation of the law. Moreover, individuals knowingly violating the law would be extremely unlikely to provide authentic information about themselves, therefore establishing the perpetrator’s true identity would be ultimately contingent on the technical capacities and resources of the law enforcement bodies. The provision in question, instead of contributing to fighting cybercrime, will ultimately criminalize such legitimate and largely innocuous activities as blogging or participating in social networking, where individuals may have absolutely lawful and compelling reasons – from artistic freedom to low self-confidence – to refrain from disclosing their true identities.
25. At the same time, the law should be able to protect individuals against identity theft and impersonation.²⁵ Curiously, a prohibition of anonymous dissemination of information is likely to result exactly in proliferation, rather than curbing, of identity theft, since making personally identifiable information readily available in the absence of an overriding public interest would make it easier for perpetrators to obtain this information and use it to pursue illegal ends. It is therefore entirely legitimate and in fact desirable to include a provision that would ban fraudulently impersonating another person.
26. Finally, as a measure against the proliferation of unsolicited email (commonly known as “spam”), the drafters may consider including a prohibition of altering routing information

²³ *Id.*, Article 12(2) (“*Information disseminated without the use of mass media shall contain accurate news on the information administrator or the person disseminating it in the form and volume sufficient for identifying this person.*”)

²⁴ See Convention for the Protection of Human Rights and Fundamental Freedoms, Article 10(1).

²⁵ For an example of good practice, see Canada’s Criminal Code, Section 403 (“*Every one who fraudulently personates any person, living or dead, (a) with intent to gain advantage for himself or another person, (b) with intent to obtain any property or an interest in any property, or (c) with intent to cause disadvantage to the person whom he personates or another person, is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years or an offence punishable on summary conviction.*”)

to disguise the origins of the email.²⁶ Anti-spam solutions are discussed in more detail under Section 4.5 “Consent to receive information.”

27. It is recommended that the requirement for information holders and/or persons disseminating information to disclose their identity be removed, and a prohibition of identity theft and impersonation, as well as a prohibition of altering routing information to disguise the origins of the electronic communication, be incorporated.

4.5 Consent to receive information

28. The Draft requires that recipients be given an opportunity to refuse information.²⁷ This provision is apparently intended to address the issue of unsolicited commercial or bulk email (“spam”), and as such is welcome.
29. The provision as it stands now follows the “opt-out” model, i.e. rather than prohibiting spam unless an individual has elected to receive it (“opt-in”), it requires recipients to request senders to stop spamming them. There is no consensus on which model is preferable, and the solution proposed by the drafters is definitely acceptable.
30. The Draft is not, however, sufficiently dissuasive for spammers as it does not envisage any mechanisms to deal with breaches of the anti-spam provisions. Moreover, since the Draft provision in question covers all types of unsolicited communications, it does not account for the unique problems posed by those unsolicited communications (such as spam or junk faxes) which result in costs imposed on end recipients (such as costly computer band) and on network/server owners alike. To address these concerns and to reinforce anti-spam provisions, it is recommended that the Draft be revised to single out those types of unsolicited communications that result in costs imposed on parties other than the sender, and to introduce effective and dissuasive remedies against the prohibited conduct. In particular, it is recommended that the Draft create a possibility for end recipients as well as for equipment owners (such as owners of networks and/or servers) to sue spammers.

4.6 Consent to provide information

31. The Draft provides that “[t]he provision of information shall be subject to the procedure defined by the mutual consent of the parties of information exchange.”²⁸ This clause does

²⁶ For an example of good practice, see the United States legislation, 15 USC 7701 (Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003) (“(1) PROHIBITION OF FALSE OR MISLEADING TRANSMISSION INFORMATION.—It is unlawful for any person to initiate the transmission, to a protected computer, of a commercial electronic mail message, or a transactional or relationship message, that contains, or is accompanied by, header information that is materially false or materially misleading. For purposes of this paragraph - (A) header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading.”)

²⁷ Draft Law on Information, Information Technologies and Protection of Information, Article 12(3) (“When using those means of information dissemination that allow to identify the recipients of information, including postages and electronic communications, the person disseminating the information shall be obliged to provide the recipient of information with the possibility to refuse it.”)

²⁸ *Id.*, 12(4).

not provide enforceable safeguards against companies that, having inherently greater bargaining power, may require potential customers to agree to provide virtually unlimited amounts of information about themselves as a condition for supplying a product or a service. This would run counter to the purpose specification principle as it concerns information collected, used and stored by private sector entities, and as spelled out by the Resolution of the Committee of Ministers of the Council of Europe on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector.²⁹ It is recommended that this concern be addressed by adding a provision forbidding organizations, as a condition for supplying a product or a service, from requiring individuals to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service.³⁰

4.7 Information security

32. The Draft imposes on the information holder and “information system operator” an obligation to “ensure” proper protection against breaches of information security, such as unauthorized access, to timely detect such intrusions, to issue “*warnings on the possible unfavorable effects of the infringement of the procedure for access to information,*” and to exercise “*permanent control over ensuring the level of information protection.*”³¹
33. It is entirely legitimate to require that corporate entities protect the security of the data they collect and store. However, companies and organizations cannot bear absolute responsibility for preventing information security incidents. It would be more appropriate to require that corporate entities bear a general duty to provide reasonable controls to protect the integrity, confidentiality, availability and authenticity of data.
34. While the Draft requires entities to timely detect information security breaches and to issue “*warnings on the possible unfavorable effects,*” it is not clear what the nature and audience of these warnings is. If the intent of the provision is to make it mandatory for organizations and companies to notify information security breaches to law enforcement bodies and to data subjects who may be affected or injured (such as customers whose personal data are stored by a company), then the provision is very welcome. However,

²⁹ Resolution (73)22 of the Committee of Ministers of the Council of Europe on the Protection of the Privacy of Individuals vis-à-vis Electronic Data Banks in the Private Sector, Principle 2 (“*The information should be appropriate and relevant with regard to the purpose for which it has been stored.*”)

³⁰ As an example of good practice, see Canada’s legislation, Personal Information Protection Act of Alberta, Division 2, 7(2) (“*An organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.*”)

³¹ Draft Law on Information, Information Technologies and Protection of Information, Article 21 (“*An information administrator and an information system operator shall in cases prescribed by the legislation of the Republic of Armenia ensure: 1) prevention of unauthorized access to information and (or) transmission of information to persons that have no right to access to information; 2) timely detection of the facts of unauthorized access to information; 3) warnings on the possible unfavorable effects of the infringement of the procedure for access to information; 4) prohibition on impacting the technical means of information protection as a result of which there may be disruptions to their functioning; 5) possibility of a speedy recovery of the information altered or destroyed as a result of unauthorized access; 6) permanent control over ensuring the level of information protection.*”)

the wording of the provision should be clarified to ensure clarity and consistency in its interpretation.³²

³² As an example of good practice, see the United States legislation, California Civil Code Sec. 1798.29 (“(a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. (b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”) and 1798.82 (“(a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. (b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.”)