Authorship and authenticity in cyberspace[1]

Patricia Akester, University of Cambridge

"Authenticity" in recorded information connotes precise, yet disparate, things in different contexts and communities. From an intellectual property viewpoint, the discussion on authenticity focuses on the accuracy of reproduction of the presented material as compared to the initial source. There may be inaccuracy in attribution of authorship or content, which may harm the author's moral rights of identity and integrity, the public interest in knowing who the author is and the public interest in accurate information. Concerns about authenticity in sources are not new but with the ubiquity of digital representations and the proliferation of source information on the Internet, these issues are further complicated. This article explores the issues involved.

The digital environment poses particular challenges for establishing authenticity

The digital environment poses particular challenges for establishing authenticity. Many people feel that this environment is characterized by pervasive deceit. This distrust of the intangible world of digital information is accompanied by considerable faith in the potential for technology to address concerns about authenticity of works, such as encryption, monitoring of web sites, use of non-editable forms, digital signatures, Public Key Infrastructure (PKI), digital watermarks and new tracking services, which have been widely used by numerous companies and organizations – such as the Recording Industry of America. This technology has found a certain amount of legal backing, such as the WIPO Treaties, the Information Society Directive (Dir. 2001/29/EC), and the Digital Millennium Copyright Act, and is fundamental in order to provide verifiable proof for claims related to authorship and integrity of works that would usually be taken at face value in the physical world.

A. What is "authenticity"?

Authenticity of information resources connotes precise, yet disparate, things in different contexts.[2] Examples will be given as to these meanings, denoting the constant importance of authenticity, independently of the context in which it appears.

From an academic viewpoint, interpretation, and re-interpretation, of primary and secondary sources is the foundation of much humanistic scholarship. Construction of a solid argument depends on the authenticity of source materials. From a sociological viewpoint, if documents are meant to be reliable surrogates for human beings, then it makes perfect sense that we would be critically concerned with their authenticity. Much as we rely on one another, we also have come to rely on documents in the making and maintaining of our social order. This is why words such as trust, reliability, and truthfulness, which are fundamentally social, apply to documents as much as to people.[3] From a philosophical viewpoint, at its extremes, authenticity carries with it all the philosophical problems of truth.[4] From a public interest viewpoint, the authenticity of a digital object refers to the degree of confidence a user can have that the object is the same as that expected based on a prior reference or that it is what it seems to be.

From an intellectual property viewpoint, the discussion on authenticity focuses on the accuracy of reproduction of the presented material as compared with the initial source. There may be inaccuracy in attribution of authorship or content, which may harm the author's moral rights[5] of identity[6] and integrity,[7] the public interest in knowing who the author is and the public interest in accurate information.[8] Therefore, its meaning is not restricted to the verification of authorship, but is intended to include issues of integrity, completeness, correctness, validity and faithfulness to an original.

B. Is authenticity a new issue?

In the middle ages, books were copied by hand, mostly by monks. Different copies of a book contained different errors, due to misconstrued transcription or deliberate "improvements" of capricious scribes. The art of Johannes Gutenberg made it possible to freeze the text once it was printed.[9] The edition became a constant, not the individual copy. Through more than 500 years we have grown accustomed to written information being something relatively unchangeable and reliable. Of course, the authenticity of works has long been a concern, but it has not been a major issue in the past, because of the technical barriers to altering works, and because of the difficulty with which such copies entered an authoritative information stream.

C. What has changed?

So, concerns about authenticity in sources, are not new, but with the proliferation of source information on the Internet, these issues are further complicated. The digital environment poses

Computer Law & Security Report Vol. 20 no. 6 2004 ISSN 0267 3649/04

particular challenges for establishing authenticity, because the underlying technology makes it easier and more tempting to alter digital material. Information in digital format is intangible and can be copied indefinitely with no loss of quality. Works in digital form can be reproduced instantaneously, and unlike copying by traditional methods, with total accuracy and no effort. Information in digital form can be manipulated without restrictions. Furthermore, increases in the capacity of the Internet have made it easier to distribute works at high speed and with little cost. Digital technology also eases the retrieval of existing works across the Internet, by means of mechanisms such as the World Wide Web and search engines and allows their manipulation into new works. Any user equipped with a modem and an Internet connection can reproduce and distribute multiple, high-quality copies of altered audio and video works.[10]

The easy access to electronic information is both their strength and their weakness: the result might be a gradual alteration as is the case with oral transmission.

D. Inaccuracy in attribution of authorship or content

Information available on the Internet is often of varying quality with little assurance regarding its true origin. The question is whether one can rely on the accuracy of works and related subject matter available on the Internet. The issue of reliability concerns both authorship and the work itself. One has to ask whether the apparent author of the work is its true creator and, secondly, whether the work has been subject to manipulation.

Such inaccuracy may take the shape of false claim of authorship,[11] attribution of structurally altered work,[12] or even distortion of work.[13] This is the moral right aspect. As regards public interest, inaccuracy in attribution of authorship or content may be contrary to the public interest in knowing who the author is and in accurate information.

E. Public interest in knowing the author's identity and in accurate information

The development of digital technology caused a shift from a society based on physical assets to an information society where intellectual property is a major asset. In the information society, the Internet is constantly used to exchange information with different degrees of economic relevance. Thus, the economic relevance varies where G sends H an e-mail expressing his views about a football match, where I, an employee of the headquarters of a bank in America, sends J, who works with a branch of that bank in the United Kingdom, business plans and strategies for the year 2000 and where K does some Internet shopping and downloads his credit card details in order to pay the bill. Once information is modified, subsequent users who rely on the information may be affected. Reliability of transmitted information is crucial for the information society as a whole. Ideally everyone should be able to rely on images and information obtained on the Internet.

The public may be affected by means of attribution of unauthorised political content,[14] attribution of unauthorised legal content,[15] attribution of unauthorised religious content,[16] and even attribution of unauthorised medical content.[17] This is where the interest in protecting author's moral rights and the general public interest overlap.

F. What can we do? Does the answer to the machine lie in the machine?[18]

1. Encryption

The best method for preventing modifications to copyright works is to encrypt it. Encryption is a technological method used to obscure the meaning of a message. There are various types of encryption. Asymmetric encryption is the best suited for e-commerce, since it uses two different keys and only public keys need to be distributed (there is no need to distribute any private keys). Each user generates two keys that are different: a private key and a public key. They keep their private key secret but send their public key to other users. The sender encrypts a message with the public key of the intended recipient and then sends it on to the recipient. Only the recipient's private key can be used to decrypt the message. But encryption is not infallible.

A record company, for example, will encrypt its music and then make it available on its web site. A user will need a player to decrypt, decompress and play the music, but he may still be able to access and store the decrypted and decompressed data from the player. This file can then be compressed in a widely available compression form, like MP3, and then placed on the World Wide Web.

In **Universal City Studios, Inc. v Reimerdes**,[19] the film studios filed a suit under the Digital Millennium Copyright Act to enjoin web site owners from placing DeCSS, a computer program

which decrypted digitally encrypted films on DVDs, on the Internet, and from including hyperlinks to other web sites that made decryption software available. The District Court found that such activities violated the Digital Millennium Copyright Act. The court awarded the plaintiffs an injunction enjoining the defendants from placing decryption software on the Internet and hyperlinks to other web sites offering decryption software.

(a) Feasibility

Whereas asymmetric encryption can only be used to stop intermediaries from accessing and/or modifying a document, symmetric encryption (e.g. secret key in the player/reader) attempts to stop anyone from accessing or modifying a document (such as a music file or an e-book). In addition to this, e-mail programs facilitate encryption but require the receiver to have a public/private keys (some programs require the receiver to have a certificate).

Confidence in the integrity of the object is only as good as our confidence in the authenticity and integrity of the digest

2. Monitoring of web sites

Encryption techniques have to be used in parallel with monitoring, by means of search engines, to see whether there are web sites redistributing unauthorised decrypted versions of works and if there are to trace them and to have them closed down.

(a) Feasibility

Monitoring of websites is a complex task for individuals, requiring resources which generally are only owned by big companies. However, specialist tracing companies may make tracing possible for all.

3. Use of non-editable forms

Another method of deterring modifications to copyright works is saving information in a non-editable form (some PDFs, for example, are not editable), which consists of a bit-map. If information is saved in this form the only way to manipulate it is by applying optical character recognition, which converts the bit-map back to editable form. This process does not prevent manipulation of data altogether, but it adds an extra level of difficulty to acts of modification of copyright works

(a) Feasibility

Non-editable forms are not easy to make. Conversely, it is easy to accidentally create a PDF where the text is selectable.

4. Digital signatures

Another possibility would be to use digital signatures. Digital signatures, which are encryption based, should be used to assure that a work has not been manipulated and then attributed to the original author. When an author digitally signs his work, an end user will still be able to delete the digital signature of the author, insert his own digital signature and assume authorship of a document not created by him. However, the user will not be able to modify the document and disseminate it under the name of the author of the original work.

A digital signature resembles a sequence of unintelligible alphabetic and numeric characters, providing assurance about the origin and integrity of the communication. It allows the recipient to ascertain if the sender is who he purports to be and whether the message was altered after it was digitally signed. As a digital signature is derived from the document, it is unique for each document signed.[20]

If the object is accompanied by an authenticated ("digitally signed") digest, we can check whether the object is consistent with the digest (and thus whether its integrity has been maintained) by recomputing the digest from the object in hand and then comparing it with the authenticated digest. But our confidence in the integrity of the object is only as good as our confidence in the authenticity and integrity of the digest. We have only changed the locus of the question to say that if the digest is authentic and accurate, then we can trust the integrity of the object.

(a) Feasibility

Digital signatures can be easily generated, in the sense that e-mail software automates the process to a large degree, but the sender must have a public/private key pair. In addition to this, some software requires the sender to obtain a certificate.

5. Public Key Infrastructure (PKI) and Pretty Good Privacy (PGP)

The use of digital signatures in conjunction with a public key infrastructure (PKI) offers a little more. This is based on the use of certificates: special documents, which allow one to prove one's identity in electronic transactions. They are issued by certification authorities – independent and trusted parties who check the validity of customers' details and issue certificates. It is most important that certification authorities be trustworthy and independent entities, since certificates are only as reliable as the entity responsible for their issuance. Broadly speaking, certification authorities ascertain the identity of a person and certify that a certain public key used to create digital signatures belongs to that person.

PKI can also be used to provide a means for determining when a key pair/identity binding has been compromised, expired, or revoked and should no longer be considered valid.

Determination of authenticity of works in the digital environment often depends on trust. Identity in the digital world means that someone has agreed to trust an association between a name and a key pair, because they have directly verified it or trust an intermediary, such as a PKI operator, that records such an association. Trust plays a central role, yet it is elusive. PGP allows one to trust a claim if one trusts the holder of a key pair, and PKI allows one to trust the identity of the holder of a key pair and the claim if one trusts the operator of the PKI. Trust is not necessarily an absolute, but often a subjective probability that one assigns case by case. The probability of trustworthiness may be higher for some PKIs than for others, because of their policies for establishing identity.

(a) Feasibility

Certificates are not too difficult to use, as existing software automates the process of using them.

6. Digital watermarks

Another possibility resides in the use of digital watermarking. Watermarking, sometimes called fingerprinting, allows copyright owners to incorporate into their works invisible identifying information. Digital watermarks are bits embedded in digital content, usually invisible in the absence of the proper software to detect and decode it. The watermark can contain information such as the author's name and e-mail address, ID number and a URL, information about who owns a work, how to contact the owner and whether a fee must be paid to use the work. A watermark can only be effective if the playback and record devices look for the watermark in that particular piece of content.

In the most general sense, watermarking can be viewed as an attempt to ensure that a set of claims is inseparably bound to a digital object and thus can be assumed to travel with the object. The most common use of watermarks today is to attach a copyright claim to an object.

The desirable properties of watermarks include being very hard to remove computationally (at least without knowledge of the private key as well as the algorithm used to generate the watermark) and being resilient under various alterations that may be applied to the watermarked file (lossy compression, for example, or image cropping).

The House of Lords[21] recognised that authentication technologies, however advanced, may be eventually circumvented. Therefore, technology must keep ahead of circumventers. They added: "in all of these processes the only thing that you can do is make it very difficult, and if you can make it difficult enough, such as that the process takes too long, then you are at least achieving part of your aim", concluding that "watermarks can be used to great advantage: they can provide a high level of security in conjunction with an audit trail and the cost of introducing a watermark to an image is likely to be low relative to the costs of trying to circumvent it."

(a) Feasibility

The process of adding a watermark should be easy for an author (since the software should carry it out), but such software is not widely used at present.

7. New tracking services

Digital watermarking should also be used in parallel with new tracking services,[22] allowing copyright owners to find all illegal copies of their works on the Internet and to take appropriate legal action. The software now exists to track and monitor Internet content on a scale and to a degree that previously has not been possible. The Recording Industry Association of America has been taking people to court because it *has* the technology to track illegal Internet file swapping.[23]

(a) Feasibility

The software used by new tracking services is currently beyond the availability and understanding of most individual authors.

G. But technology requires legal backing

Technology per se cannot supply an adequate solution. Technological measures for copyright protection must be validated by laws prohibiting their circumvention and thus assuring that they are respected. In this context special attention will be paid to some provisions of the TRIPS Agreement, the WIPO Treaties, the Convention on Cybercrime, the Electronic Signatures Directive (Dir. 99/93/EC) and the Information Society Directive (Dir. 2001/29/EC),

1. WIPO Treaties

At the WIPO Diplomatic Conference, of December 1996, two treaties were achieved: the WIPO Copyright Treaty and the WPPT.[24] The treaties establish a legal framework to protect the interests of

creators, performers and phonogram producers in cyberspace. Since Contracting Parties to the WCT have to comply with Articles 1 to 21 of the Berne Convention,[25] this Treaty also protects moral rights. In addition to this, for the first time, performers are given certain moral rights.[26] The WCT contains obligations regarding technological measures[27] and rights management information.[28] It states that Contracting Parties must adopt remedies against devices created to overcome technical measures for protection of copyright or to remove, alter etc. rights management information.[29] The WPPT establishes similar provisions.[30] The WCT entered into force on 6 March 2002 and the WPPT on 20 May 2002.

The Convention on Cyberspace is the first international instrument devoted to crimes committed via the Internet

2. The Convention on Cybercrime

The Convention was drafted under the auspices of the Council of Europe. The main aim of this instrument, set out in the preamble, is to protect society against cybercrime by means of a common criminal policy. Contracting Parties are required to establish as criminal offences wilful infringements of copyright and related rights arising from certain international agreements[31] to which they are Parties,[32] when such infringements have been committed by means of a computer system and on a commercial scale.[33] This obligation does not extend to any moral rights conferred by such instruments.[34] In addition, the Convention contains various provisions on procedural law, foreseeing powers for expedited preservation of stored computer data, search and seizure of stored computer data and real-time collection of computer data.[35] The Convention is not in force yet. It requires ratification by five States, including at least three member States of the Council of Europe.

The Convention on Cyberspace is the first international instrument devoted to crimes committed via the Internet and other computer networks, paying particular attention to certain matters, such as infringements of copyright and violations of network security, but, unfortunately, this Convention does not cover moral rights.

3. The Digital Millennium Copyright Act

In 1998, the Digital Millennium Copyright Act was signed into law, ending many months of turbulent negotiations regarding its provisions.[36] Chapter 12 is devoted to copyright protection and management systems.

Section 1201 addresses circumvention of copyright protection systems, making it a crime to circumvent anti-piracy measures built into protected works[37] and outlawing the manufacture, sale, or distribution of devices used to circumvent technological measures for protection of copyright.[38] However, it allows the circumvention of copyright protection devices to assess product inter-operability,[39] to conduct encryption research,[40] and to test computer security systems,[41] also providing exemptions from anti-circumvention provisions for non-profit libraries, archives, and educational institutions under certain circumstances.[42]

Section 1202 is the provision dealing with the obligation to protect the integrity of copyright management information. Subsection (c) defines copyright management information as identifying information about the work, the author, the copyright owner, and in certain cases, the performer, writer or director of the work, as well as the terms and conditions for use of the work. Information concerning users of works is explicitly excluded. Subsection (a) prohibits the knowing provision or distribution of false copyright management information, if done with the intent to induce, enable, facilitate or conceal infringement. Subsection (b) bars the intentional removal or alteration of copyright management information without authority, as well as the dissemination of copyright management information or copies of works, knowing that the copyright management information has been removed or altered without authority. Section 1202 is subject to a general exemption for law enforcement, intelligence and other governmental activities.[43] It also contains limitations on the liability of broadcast stations and cable systems for removal or alteration of copyright management information in certain circumstances where there is no intent to induce, enable, facilitate or conceal an infringement.[44]

4. The Electronic Signatures Directive (Dir. 99/93/EC)

The objective of the Electronic Signatures Directive is to remove obstacles, particularly, concerning the legal recognition of electronic signatures and the free movement of certification services and products between the Member States.[45]

The Directive covers the legal recognition of electronic signatures and a legal framework for certification services.[46] Electronic signatures allow the on-line recipient of electronic data to verify the origin of the data (authentication of data source) and to check that the data is complete and unchanged (integrity of data).[47] Verification of the

authenticity and integrity of data does not necessarily prove the identity of the signatory who creates the electronic signatures. Such information can be confirmed by trusted third-parties, the certification service providers.[48] Electronic signatures certificate[49] which fulfil certain criteria will be legally equivalent to a hand written signature and be admissible as evidence in legal proceedings.[50] Each Member State will recognise the certification authorities of another Member State[51] and will also recognise a certification authority based outside of the European Community if it complies with certain requirements.[52]

5. The Information Society Directive (Dir. 2001/29/EC)

The Information Society Directive updates the protection of copyright and related rights in line with the issues raised by the digital environment and obligations arisen from the WIPO Treaties, 1996.[53] Member States have to adopt remedies against devices designated to overcome technical protection measures and to interfere with rights management information.[54] The provision on technological measures goes beyond the WIPO Treaties. Its scope of protection covers any activities designated to overcome technical protection measures, including preparatory activities that facilitate or enable the circumvention of such devices. It requires knowledge by the person liable for the circumvention, which implies that only activities and services whose purpose is to circumvent technological protection devices are covered by this provision. The provision covers not only infringement of author's rights and related rights, but also that of the *sui generis* right of database makers.[55] Article 7 on rights management information is not as detailed as its counterparts in the WIPO Treaties, but its protection is extended to the *sui generis* right of database makers.

H. Conclusions

Certifying that a digital object is the product of its author and has not been modified is difficult when the object is disseminated in electronic form. We can reasonably expect that some digital objects will warrant greater scepticism than their analog counterparts. It took centuries for users of print materials to develop the web of trust that now underlies our current system. It will be necessary to provide proof for claims related to authorship that would usually be taken at face value in the physical world.

Many technical methods are being developed that address the issues of authenticity of information and the relevant industries are starting to take a leading role in monitoring the Internet and tracking infringing copyright material across it. Some of these mechanisms are more accessible than others.[56]

Technological measures for copyright protection and rights management systems, need to be backed up by laws guaranteeing that they are complied with – thus the importance of legal instruments such as the WIPO Treaties, the Convention on Cybercrime, the Electronic Commerce Directive, the Information Society Directive and the Digital Millennium Copyright Act.

A partnership between law and technology will provide authors and owners with new weapons to assure protection of their works and to enforce their rights on the Internet. This is significant for the balance of the copyright system as a whole, since it gives authors control over their works, and consequently an incentive to create.

Those instruments contain essential provisions in the context of this discussion – the WIPO Treaties, the Information Society Directive and the Digital Millennium Copyright Act outlaw the circumvention of technological measures for protection of copyright and the modification or deletion of rights management information, the Electronic Commerce Directive establishes a legal framework for electronic signatures and the Convention on Cyberspace is the first international instrument devoted to crimes committed via the Internet.

Yet, it is impossible to not notice the piecemeal nature of these solutions. In addition to this, the Convention on Cyberspace does not cover moral rights. Considering the importance moral rights have acquired in the digital world, because of the ease with which existing works can be manipulated, this omission needs to be filled.

It could be argued that these solutions provide for limited protection and that the combined effect of mass access to the Internet, to the World Wide Web and to information delivery on demand, requires more than a few changes to the present copyright system. It could also be asserted that for an effective solution what is needed in today's global village is one law apposite for the digital world and offering uniform principles, since unification of substantive law will provide certainty for Internet citizens regarding on-line activities, because users, service providers and courts need to be able to operate within the same rules.

Ultimately, the ease with which works in electronic form can be modified only heightens the importance of maintaining their integrity, which is of equal concern for authors, information providers and users. The issue of authenticity must be resolved globally before anyone can feel absolutely confident in creating and relying upon digital information.

Dr. Patricia Akester, University of Cambridge
vpa20@cam.ac.uk

FOOTNOTES

1 This text is based on a paper presented in Oxford, in September 2003, at the SLS Conference.

2 Authenticity should not be confused with authentication, an equally important issue in the context of the Internet. Authentication addresses control of access to information resources and is, therefore, grounded in methods of identification of the user. Authenticity is concerned with content assurance and requires methods of identification and verification of the resources themselves.

3 S. Shapin (A Social History of Truth: Civility and Science in Seventeenth-Century England (University of Chicago Press, 1994), engages questions such as how we come to trust our knowledge of the world, or by what means we distinguish true from false accounts, arguing that in seventeenth century England, problems of credibility in science were practically solved through the codes and conventions of genteel conduct: trust, civility, honour, and integrity. These codes formed an important basis for securing reliable knowledge about the natural world.

4 J. Park, Becoming more authentic: the positive side of existentialism (Minneapolis, 4ed 1999) gives a systematic account of the concept of Authentic Existence as defined in existential philosophy and psychology. See also J. Macquarrie, Existentialism (Philadelphia, PA, Westminster, 1972), which contains a chapter on Authenticity called "In Quest of Authentic Existence"; A. Camus, The Myth of Sisyphus and Other Stories (New York: Knopf, 1955 and later reprints), which essay contains the substance of Camus' vision of Authenticity.

5 Moral rights arise automatically with the creation of the work and in general cannot be assigned. They allow the author to control the uses made of the work irrespective of assignment of economic rights. Their aim is to ensure the respect for the author's personality as expressed in the work. See inter alia H. Desbois, "The moral right" (1958) 19 R.I.D.A. 121; H. Desbois, Le droit d'auteur en France (Dalloz, 1978) 469-602; G. Dworkin, "Moral rights in English law – the shape of things to come" (1986) 11 E.I.P.R. 329; G. Dworkin, "Moral rights and the common law countries" (1994) Australian Intellectual Property Journal 5. Moral rights, were inserted in the Berne Convention, the fundamental instrument of international copyright law, by the Rome Revision of 1928, and encompass the right to claim authorship of the work and the right to object to any distortion or modification of the work (Berne Convention, Article 6bis).

6 The identity right entitles the author to demand that his name appear on all copies of the work and whenever the work is performed or to demand that his name not be mentioned, that is to remain anonymous. It also includes the right not to have another's work falsely attributed to another person as author.

7 The integrity right generally prevents any distortion, mutilation or other modification of a work, which endanger the author's legitimate interests in the work, his honour or his reputation.

8 See Realizing the Information Future – The Internet and Beyond, NRENAISSANCE Committee, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics and Applications, National Research Council, National Academy Press, Washington D.C., 1994, 160-165.

9 Actually, it was first developed in Eastern Asia. Around 1400 the Chinese knew the system of "movable characters". Characters on bones, bronze, ceramic and stone slabs give evidence of the use of writing in China already in the 5th millennium before Christ. Printing with movable characters didn't really establish itself in China until the end of the last century. While traditional printing with whole wooden plates required enormous storage space, the panoply of Chinese characters prevented a simple and fast composition of printing plates from movable letters. In comparison it was much simpler for Gutenberg, with 26 characters and a few auxiliary characters to set all words. See J. Thorpe, The Gutenberg Bible: Landmark in learning (Huntington Library Press, 1999); J., Man, Gutenberg: How one man remade the world with words (John Wiley & Sons, 2002); B. Morrison, The justification of Johann Gutenberg (William Morrow & Company, 2002)

10 See inter alia N. Highman, "The New Challenges of Digitisation" (1993) 10 E.I.P.R. 355-359; E. Samuels, "Copyright Concerns on the Information Superhighway" (1994) Annual Survey of American Law 383-392; F.H. Cate, "Law in Cyberspace" (1996) 39:565 Howard Law Journal 565-57; J.C. Ginsburg, "Putting Cars on the Information Superhighway: Authors, Exploiters and Copyright in Cyberspace" in P.B. Hugenholtz (editor), The Future of Copyright in a Digital Environment (Kluwer, 1996) 189-219; A. Johnson-Laird, "The anatomy of the Internet meets the body of the law", (1997) 22:3 University of Dayton Law Review 467-509; R.A. Kurz and C.M. Jimenez, "Copyrights On-Line" (1996) 39:2 Howard Law Journal 531-564; A. Mille, "Copyright in the Cyberspace Era" (1997) 10 E.I.P.R. 570-577.

11 Example: A publishes a novel on the Internet. Without her consent, B publishes a verbatim copy of the novel on his web page, claiming to be its author.

12 Example: C publishes a novel on the Internet. D reads C's novel, dislikes the sad ending and without her authorisation decides to change it into a happy ending. D then publishes the modified novel on the Internet under C's name.

13 Example: E's painting entitled Portrait of a Woman has been used without his authorisation on the Internet in an advertisement. The image was distorted and the woman has a moustache on. E is concerned because the public will not know whether the image was his original work, who made the additions or why they made them.

14 Example: F took a black and white photograph in Bosnia of some children. The photograph was published in a newspaper and without her consent was manipulated by a member of the public and made available on the Internet. In order to look more aggressive, a wall was put behind the children with graffiti on it saying: "Soldiers get out". This raises, among other matters, questions of distortion of information as well as of the work.

15 Example: G works with a law firm located in the United Kingdom. H, a client with that firm, lives in Honolulu and asks G to draft a legal opinion regarding a tax law issue. H wants to know which is the best way of avoiding heavy taxation on certain revenues. G drafts the legal opinion and sends it to H by e-mail. Before H receives G's e-mail, I, a hacker, gets hold of that e-mail and without any authorisation changes its contents. H, unaware that G's legal opinion has been tampered, takes a decision based on it and, consequently, his revenues are heavily taxed.

16 Example: A Roman Catholic author who is against birth control paints a picture of a happy family consisting of a father, a mother and eight children, called The Blessings of Family Life. J, who is for birth control, sees a photograph of the painting in a magazine and without the author's

consent, scans it on to his personal computer and changes the picture, so that the husband and the wife now look unhappy and the title is now If Only We Had Known. J then makes the changed picture available on the Internet.

17 Example: K, a researcher, after analysing a new chemical product for a manufacturer of chemical products found that the product was not safe. K sent the report to the company via the Internet. A hacker got hold of the e-mail with the report and, without any authorisation, changed it, and then published the report on the Internet, saying that the product was safe.

18 See, inter alia, W. Stallings, Data & Computer Communications (6th edition, Prentice Hall, 2000); S. Tanenbaum, Computer Networks (3rd edition, Prentice Hall, 1996); F. Halsall, Data Communications, Computer Networks, and Open Systems (4th edition, Addison-Wesley, 1996); D. Comer, Internetworking with TCP/IP, Vol. I: Principles, Protocols, and Architecture (4th edition, Prentice Hall, 2000); W. Stevens, TCP/IP Illustrated, Vol. I: The Protocols (Addison-Wesley, 1994).

19 Universal City Studios, Inc. v. Reimerdes 82 F. Supp. 2d 211, 2000 U.S. Dist. Lexis 906 (S.D.N.Y. 2000).

20 The sender needs a public key and a private key. The private key is kept confidential and the public key is disclosed generally where the recipient of the digitally signed communication can access it. To digitally sign an electronic message the sender has to run a computer program which automatically creates what is called a message digest (or hash value) and subsequently encrypts the message digest using the sender's private key. The encrypted message digest - a sequence of bits - is the digital signature. The digital signature is attached to the communication and they are both sent to the intended recipient. The recipient has to run a computer program which automatically decrypts the digital signature using the sender's public key. If the program decrypts the digital signature, that means that the message came from the alleged sender. The computer program then creates a second message digest and compares it to the first message digest. If the two message digests match, that means that the communication has not been altered.

21 House of Lords, Select Committee on Science and Technology, Fifth Report, Chapter 3, Digital Images, 1998, available at: http://www.parliament.the-stationery-office.co.uk/pa/ld199798/ldselect/ldsctech/064v/st0505.htm

22 Such as BayTSP, a provider of anti-piracy, copyright tracking and enforcement services for corporate digital media on the Internet, AdminiTrack, a company that offers a web based bug tracking system designed for software development teams, or Allot Communications, which says its software can track and filter Internet communications and use that analysis to bill consumers.

23 Such as crawlers and bot programs that comb through p2p networks, searching for copyright protected material and automatically generating e-mail complaints to ISPs. The first major case, in the realms of p2p was A & M Records, Inc. v. Napster, Inc., in which record companies and music publishers brought a copyright infringement action against Napster, an Internet company that facilitated the upload and download of MP3 files by its users (see A & M Records, Inc. v. Napster, Inc. 114 F.Supp. 2ed 896 (N.D. Cal. 2000) and A & M Records, Inc. v. Napster, Inc. 239 F.Supp. 3ed 1004 (9th Cir. 2001)). Napster's downfall was that its p2p operations were centralized on its own servers, so the RIAA was able to show that Napster was aware of the illegal downloads taking place. Unlike Napster, Napster's progeny decentralized their networks, blinding themselves to activities carried out on their network. Whilst the RIAA succeeded in persuading the courts to shut down Aimster in late 2002, other similar services thrived, such as Kazaa, Grokster, BearShare, and Morpheus. By 2002 the RIAA decided to go after the file sharing users themselves. By July, the RIAA had identified the IP address of a Verizon DSL subscriber who was suspected of downloading more than 600 digital music files in one day. Subscriber X did not host illegal content on Verizon's network; he was a Kazaa client that used Verizon for Internet access, and the disputed content was stored on his hard drive. The RIAA wanted Verizon to deliver the subscriber's name and address (on the basis of section 512 of the US Copyright Act, which allows a copyright holder to subpoena customer information from a service provider when infringement is in question), as well as shut off his access to the Internet. The federal court ordered Verizon to give up the name of Subscriber X, but Verizon appealed (RIAA v. Verizon decision 2003 LEXIS 681 (D.D.C. 2003)). Verizon won the appeal on 19th December 2003 (RIAA v. Verizon U.S. App. LEXIS 25735 (2003).

24 For a critical analysis of both WIPO Treaties see, inter alia, C. Davies "WIPO Treaties – The New Framework for the Protection of Digital Works" (1997) 2:2 Communications Law 46-48; M. Fabiani, "The Geneva Diplomatic Conference on Copyright and the Rights of Performers and Phonogram Producers" (1997) 3 Ent.L.R. 98-102; J. Reinbothe, M. Prat and S. Lewinski "The New WIPO Treaties: A First Resume" (1997) 4 E.I.P.R. 171-176; H. Rosenblatt, "The WIPO Diplomatic Conference, The Birth of Two New Treaties" [1997] 13 C.L.S.R. 307-311; P. Wand, "New Rules for our Global Village" (1997) 5 Ent.L.R. 176-180; K. Weatherall, "An end to private communications in copyright? The expansion of rights to communicate works to the public: Part 1" (1999) 7 E.I.P.R. 342-349. For a critical analysis of WCT see inter alia S. Fraser, "The Copyright Battle – Emerging International Rules and Roadblocks on the Global Information Infrastructure" (1997) 25 Journal of Computer & Information Law 773-783; A. Mason, "Developments in the Law of Copyright and Public Access to Information" (1997) 11 E.I.P.R. 636-643; T.C. Vinje "The New WIPO Copyright Treaty: A Happy Result in Geneva" (1997) 5 E.I.P.R. 230-236. For a critical analysis of the WPPT see inter alia V.A. Espinel, "Harmony on the Internet: WPPT and United Kingdom Copyright Law" (1998) 1 Ent.L.R. 21-29.

25 Which means that the WCT incorporates the obligations of the Berne Convention, (WCT, Article 1(4)).

26 Performers are given the right to claim to be identified as the performer of his performance and to object to any distortion, mutilation or other modification of his performance that would be damaging to his reputation (WPPT, Article 5).

27 According to Article 11 of the WCT, "Contracting Parties shall provide adequate legal protection and effective legal remedies against the circumvention of effective technological measures(…)"

28 According to Article 12 of the WCT, "Contracting Parties must provide legal remedies against any person knowingly performing any of the following acts knowing, or with respect to civil remedies having reasonable grounds to know, that it will induce, enable, facilitate or conceal an infringement of any right covered by this Treaty or the Berne Convention: (i) to remove or alter any electronic rights management information without authority; (ii) to distribute, import for distribution, broadcast or communicate to the public, without authority, works or copies of works knowing that electronic rights management information has been removed or altered without authority. 2) As used in this Article, "rights management information" means information which identifies the work, the author of the work, the owner of any right in the work, or information about the terms and conditions of use of the work, and any numbers or codes that represent such information, when any of these items of information is attached to a copy of a work or appears in connection with the communication of a work to the public."

29 WCT, Articles 11-12.

30 WPPT, Articles 18-19.

31 Berne Convention, TRIPS, WCT, Rome Convention and WPPT. See Convention on Cybercrime, Article 10(1)-(2).

32 Convention on Cybercrime, Article 10: "1. Each Party shall adopt such legislative and other measures as may be

necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party pursuant to the obligations it has undertaken under the Paris Act of 24 July 1971 of the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
"2. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations done in Rome (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such Conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.
"3. A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article." [emphasis added]

33 In line with Article 61 of TRIPS, which requires criminal sanctions in copyright matters only in the case of "piracy on a commercial scale".

34 Convention on Cybercrime, Article 10(1)-(2).

35 Convention on Cybercrime, Articles 16, 19 and 20.

36 For a critical analysis of the DMCA, see, inter alia, J. Band, "The Digital Millennium Copyright Act: A balanced result" (1999) 2 E.I.P.R. 92-94; J.E. Cohen, "WCT implementation in the United States: Will fair use survive?" (1999) 5 E.I.P.R. 236-240; T. Vinje, "Copyright Imperilled" (1999) 4 E.I.P.R. 201-205.

37 DMCA, section 1201(a).

38 DMCA, section 1201(a).

39 DMCA, section 1201(f).

40 DMCA, section 1201(g).

41 DMCA, section 1201(j).

42 DMCA, section 1201(d).

43 DMCA, section 1202(d).

44 DMCA, section 1202(e).

45 See inter alia European Commission, Green Paper on the Legal Protection of Encrypted Services in the Internal Market, 6 March 1996, available at http://europa.eu.int/en/record/green/gp004en.pdf; European Commission, Towards A European Framework for Digital Signatures And Encryption COM (97) 503, 10 October 1997, available at http://www.ispo.cec.be/eif/policy/97503toc.html; The Copenhagen Hearing - European Expert Hearing on Digital Signatures and Encryption April 23 1998 – Theme paper (1998) available at http://www.fsk.dk/fsk/div/hearing/theme.html; C. Kuner, "The Emerging European Legal Framework for Digital Signatures" (1998) 3:21 E.C.L.R. 712-716; C. Kuner, "The Electronic Signatures Directive and the Politics of E-Commerce in Europe" (1998) 3:46 E.C.L.R. 1378-1381; R. Julià-Barceló and T.C. Vinje, "Electronic commerce – Towards a European framework for digital signatures and encryption" [1998] 14 C.L.S.R. 79; R. Julià-Barceló and T. C. Vinje, "Electronic signatures – Another step towards a European framework for electronic signatures: the Commission's Directive proposal" [1998] 14 C.L.S.R. 303; V. Sinisi, "Digital signature legislation in Europe" (December 2000) International Business Lawyer 487.

46 Directive 99/93/EC, Article 1.

47 Directive 99/93/EC, Article 2(1): "Electronic signature" means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication."

48 Directive 99/93/EC, Article 2(11): "Certification-service-provider" means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures."

49 Directive 99/93/EC, Article 2(9): "certificate" means an electronic attestation which links signature-verification data to a person and confirms the identity of that person." See also Annex I which contains certificates' requirements.

50 Directive 99/93/EC, Recitals 16 and 21 and Article 5. See also Articles 2(2) and 2(6).

51 Directive 99/93/EC, Article 4.

52 Directive 99/93/EC, Article 7.

53 For a critical analysis of the Information Society Directive see inter alia G. Cornish, "Libraries and the Harmonisation of Copyright" (1998) 7 E.I.P.R. 241-243; M. Hart, "The Proposed Directive for Copyright in the Information Society: Nice Rights, Shame about the Exceptions" (1998) 13 E.I.P.R. 169-171; T. Hoeren and U. Decker, "Electronic Archives and the Press: Copyright Problems of Mass Media in the Digital Age" (1998) 7 E.I.P.R. 256-266; S. Lewinski, "A Successful Step towards Copyright and Related Rights in the Information Age: The New E.C. Proposal for a Harmonisation Directive" (1998) 4 E.I.P.R. 135-139; T. Heide, "The Berne three step test and the proposed Copyright Directive" (1999) 3 E.I.P.R. 105-109; T. Vinje, "Copyright Imperilled" (1999) 4 E.I.P.R. 206-207; Bainbridge, D., "Copyright in the information society" (2001) 6(4) I.P.&I.T. Law 2-7; R. Calleja, "Copyright Directive adopted – and about time too!" (2001) 3(5) E.B.L. 1-2; S. Augi, "Copyright law: an emergent Community law subject" (2000/01) 6 Eu. L.F. 420-422. See § 1.3.6 – The WCT and § 1.3.7 – The WIPO Performances and Phonograms Treaty.

54 Directive 2001/29/EC, Articles 6-7.

55 Directive 2001/29/EC, Article 6.

56 In fact:
— E-mail programs facilitate encryption but require the receiver to have a public/private keys (some programs require the receiver to have a certificate).

— Monitoring of websites is a complex task for individuals, requiring resources which generally are only owned by big companies. However, specialist tracing companies may make tracing possible for all.

— Non-editable forms are not easy to make. However, it is easy to accidentally create a PDF where the text is selectable.

— Digital signatures can be easily generated, in the sense that e-mail software automates the process to a large degree, but the sender must have a public/private key pair. In addition to this, some e-mail software requires the sender to obtain a certificate.

— Certificates are not too difficult to use, as existing software automates the process of using them.

— The process of adding a watermark should be easy for an author (since the software should carry it out), but such software is not widely used at present.

—The software used by new tracking services is currently beyond the availability and understanding of most individual authors.