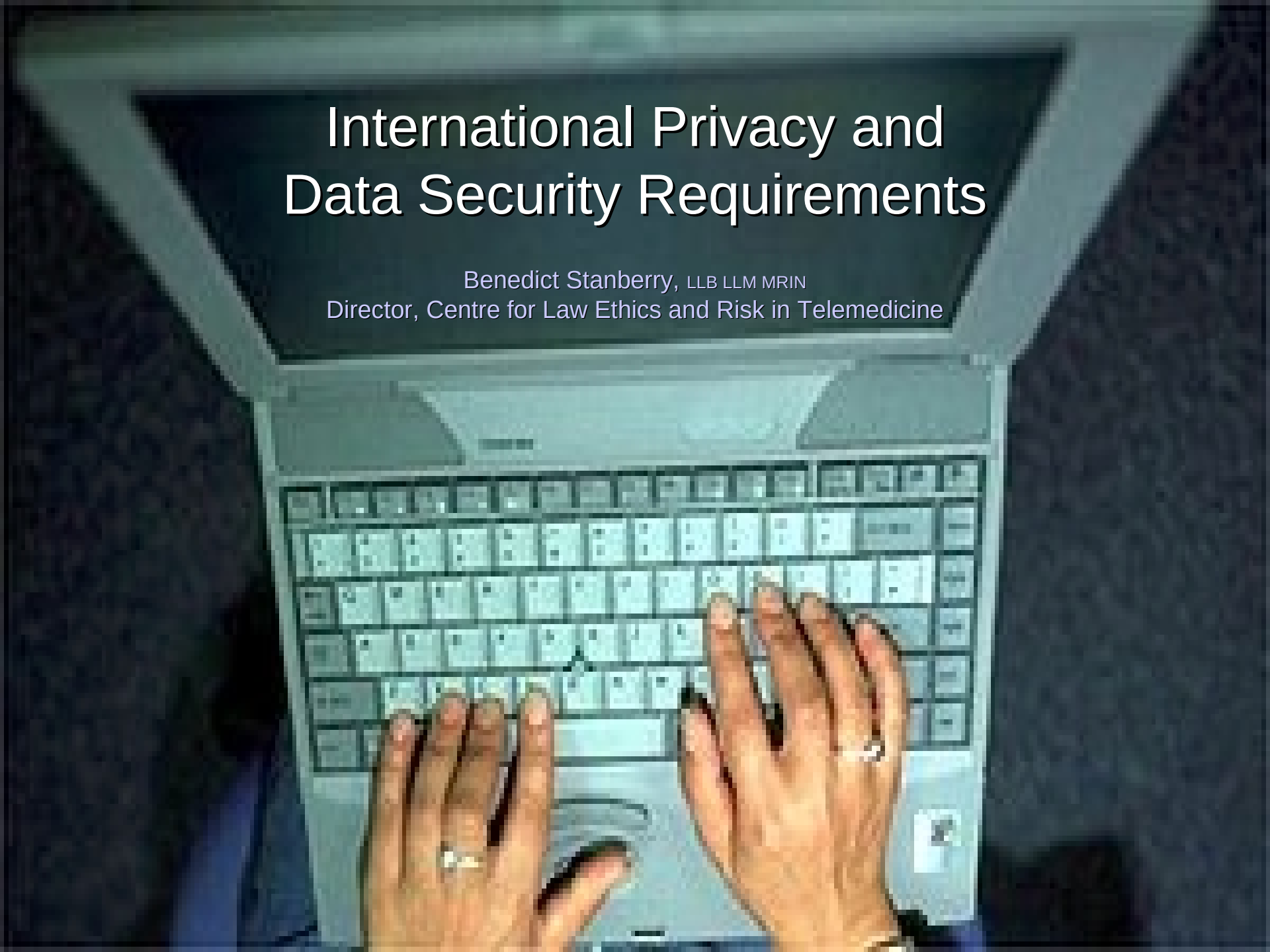
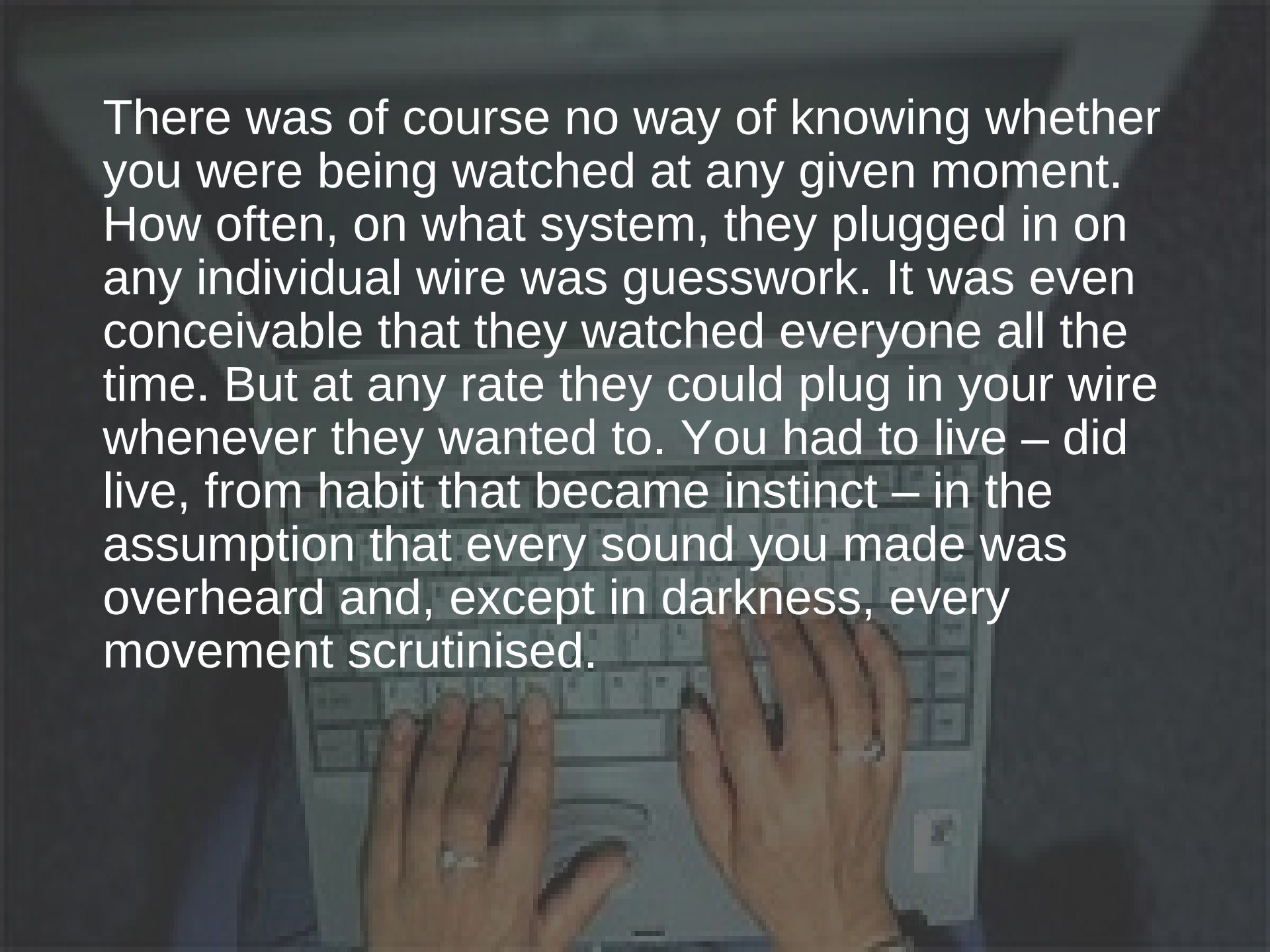
International Privacy and Data Security Requirements

Benedict Stanberry, LLB LLM MRIN
Director, Centre for Law Ethics and Risk in Telemedicine



Aims of this Presentation….

- To provide a brief overview of the evolution of international data protection laws and regulations
- To briefly explain the social and cultural influences on this evolution
- To explain what international provisions exist today
- To explain the main features of these provisions, with particular emphasis upon the European Directive on Data Protection



There was of course no way of knowing whether you were being watched at any given moment. How often, on what system, they plugged in on any individual wire was guesswork. It was even conceivable that they watched everyone all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard and, except in darkness, every movement scrutinised.

There was of course no way of knowing whether you were being watched at any given moment. How often, on what system, they plugged in on any individual wire was guesswork. It was even conceivable that they watched everyone all the time. But at any rate they could plug in your wire whenever they wanted to. You had to live – did live, from habit that became instinct – in the assumption that every sound you made was overheard and, except in darkness, every movement scrutinised.

- George Orwell, *1984.*

Background to International Data Protection

- World's first data protection statute was enacted in the German state of Hesse in 1970
- Germany acted, at least in part, from the memory of the misuse of records under the totalitarian Nazi regime and with the desire to place controls over those wishing to obtain and process personal data
- The first national statute emerged from Sweden in 1973

Background to International Data Protection

- Freedom of information is a basic tenet of Swedish life – even tax returns are a matter of public record
- System came to a halt when *Abba* were at the height of their fame – fans all claimed a (free) copy of the band's tax return which included a photograph!
- Data protection laws continued to be developed in European countries throughout the 1970s

The First International Data Protection Convention

- 1981: Council of Europe adopts Convention on the Protection of Individuals with Regard to the Automatic Processing of Personal Data
- Allows for free flow of information between signatory states and tries to prevent emergence of differing standards that would enable data processing that was illegal in one country to be “farmed out” to another, with corresponding consequences for the effective protection of the rights of the data subject
- States were required to have data protection laws which conformed to basic standards laid down in the Convention
- UK and some other countries were therefore forced to adopt data protection legislation whether they felt it necessary or not

The First International Data Protection Convention

- Recommendations issued concerning the interpretation and application of the Convention principles in particular sectors:
  - Recommendation (81)1: Regulations for Automated Medical Data Banks
  - Recommendation (83)10: Protection of Personal Data Used for Scientific Research and Statistics (Amended by Recommendation 97(18))
  - Recommendation (97)5 on the Protection of Medical Data

For texts of these instruments see: http://www.coe.fr/DataProtection/edocs.htm

- One US observer, commenting on the Council of Europe Convention of 1981 stated:

  "…. The draft convention appears to regulate a function, that is, it appears to regulate automated or electronic data processing and what the automated data processing industry may do with records about individuals. To our mind the draft convention is, in essence, a scheme for the regulation of computer communications technology as it may be applied to personal data record-keeping. The establishment and exercise of individual rights and the privacy of the individual seem to be treated in a secondary fashion…. I would note particularly that the word "privacy" is rarely mentioned in the Convention and is not included in its title."

Text of US Department of State Telegram, quoted in Transnational Data Report, Vol 1, No 7 at 22

Other International Conventions:

Organisation for Economic Co-operation and Development (OECD)

- 1980: Guidelines Concerning the Protection of Privacy and Transborder Flows of Personal Data
- These Guidelines are broadly in line with the proposals submitted by the US delegation
- April 1985: Declaration on Transborder Data Flows

United Nations (UN)

- February 1990: Guidelines Concerning Computerised Personal Data Files
- Identify 10 principles which represent the “minimum guarantees that should be provided in national legislation”
- Provision made for application of principles by international agencies
- Principles can be extended to manual files and to files concerning legal persons

- One explanation of the difference in approaches between the Council of Europe and the more US-influenced OECD:

  “In the final result, although substantially similar in core principles, the Convention and the Guidelines could be analogised, albeit in a rough fashion, to the civil and common law approaches, respectively. Common law systems proceed pragmatically formulating the rules of legal behaviour as they acquire experience, while the civil tradition tends to rely upon codification of rules in advance of action.”

  Kirsch (1982) *Legal Issues of European Integration* 21 at 45

Progress Towards the EU Data Protection Directive

- Council of Europe Convention signed by all EU member States but only ratified by 6
- Convention gave considerable discretion to signatories regarding the manner in which they comply with their obligations
- Some individual member States had national laws that provided considerably more protection than the Convention's minimum standards
- European Commission decided this was a barrier to inter-community trade and that European citizens still lacked sufficient protection, so brought forward proposals for a harmonising Directive

Progress Towards the EU Data Protection Directive

- 24 October 1995: EU Directive on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data
- Directive had to be implemented within 3 years – by 24 October 1998
- IT WASN'T !!!
- European Commission has raised legal action against Denmark, France, Germany, Ireland, Luxembourg, the Netherlands and the UK

Progress Towards the EU Data Protection Directive

- The very right of the EU to legislate in the area of data protection has not gone unchallenged (is officially a harmonising measure under Article 100A of the European Treaty)

- Since most of the provisions of the Directive are effectively 10 years old there is a danger that it is already out of date with respect to developments such as the Internet
- The Directive has required the strengthening of laws by some countries – other countries have feared the dilution of their laws

Major Differences between the US and European Approaches

- USA has adopted a *sectoral* approach
- A number of statutes have been enacted to regulate specific forms of information handling:
  - Fair Credit Reporting Act 1970
  - Privacy Act 1974
  - Video Privacy Protection Act
  - Children's On-Line Privacy Protection Act 1999
  - Health Insurance Portability and Accountability Act 1996

- European states have instead had an *omnibus* approach
- Legislation usually regulates all (or almost all) instances where personal data is processed by computer
- Supervisory agencies, generally independent of government, created to monitor the activities of data processors
- Many US observers have criticised EU initiatives as being motivated by commercial and economic protectionism rather than a genuine concern for privacy

For texts of these instruments see: http://www.gseis.ucla.edu/iclp/coppa/htm

Major Differences between the US and European Approaches

- USA has adopted a *sectoral* approach
- A number of statutes have been enacted to regulate specific forms of information handling:
  - Fair Credit Reporting Act 1970
  - Privacy Act 1974
  - Video Privacy Protection Act
  - Children's On-Line Privacy Protection Act 1999
  - Health Insurance Portability and Accountability Act 1996

- European states have instead had an *omnibus* approach
- Legislation usually regulates all (or almost all) instances where personal data is processed by computer
- Supervisory agencies, generally independent of government, created to monitor the activities of data processors
- Many US observers have criticised EU initiatives as being motivated by commercial and economic protectionism rather than a genuine concern for privacy

For texts of these instruments see: http://www.gseis.ucla.edu/iclp/coppa/htm

The EU Data Protection Directive

- Member states must protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of *personal data*
- No mention of the word “computer” – Directive refers to data being *processed* “wholly or partly by automatic means” by a *data controller* – so can include manual records
- Applies to any information relating to an identified or identifiable natural person (the *data subject*), whether directly or indirectly identifiable
- Special classification for especially *sensitive data* deserving of special protection - such data is subject to more extensive requirements than is the case with other forms of data

The EU Data Protection Directive

- “Sensitive data” includes data referring to a data subject’s physical or mental health or condition, or his sexual life
- There is a general prohibition against the processing of such data, with a number of exceptional justifications for doing so
- Nominally, sensitive data cannot be processed without the explicit consent of the data subject unless this is necessary for medical purposes and is undertaken by a health professional or by a person owing an equivalent duty of confidentiality
- “Medical purposes” is defined broadly to include “Preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.”

The EU Data Protection Directive

- With regards to health related information:
  - Access may be refused if granting it would cause serious harm to the health of the data subject or any other person
  - Special provisions for access by the parents or guardians of children or persons suffering from mental incapacity
  - There is a strong presumption in favour of access in all cases other than those involving psychiatric illness
  - In cases where the data controller is not a health professional, any decision to grant or refuse access may be made only after consultation with an “appropriate health professional”

The EU Data Protection Directive

- Data Protection Commissioners and Tribunals created
  - These supervisory agencies have powers of investigation, intervention and prosecution on both their own initiative and following a complaint by a data subject
  - All data users must register with the competent national supervisory authority (e.g., Data Protection Registrar in the UK) and notify the authority of the details of their processing
  - There are some limited exceptions to the notification requirements (e.g., staff administration)

The EU Data Protection Directive

- Article 6 of the Directive provides five principles. Member States must ensure that personal data is:
  - processed fairly and lawfully
  - collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes
  - adequate, relevant and not excessive in relation to the purposes for which they are collected and / or further processed
  - accurate and where necessary, kept up to date; every reasonable step must be taken to ensure that date which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified; and
  - kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed

The EU Data Protection Directive

- Member States must also ensure that:
  - Appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data – especially where the processing involves the transmission of data over a network (Article 17.1)
  - Data controllers must take a risk-based approach in determining the relevant standard of security
  - BS 7799 contains both a Code of Practice and a Specification for Information Security Management
  - Trade associations, professional organisations and other such bodies are strongly encouraged to create codes of practice to facilitate the operation of the Directive

The EU Data Protection Directive

- Member States must also ensure that:
  - Personal data is not transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data (Article 25.1)
  - Determination of “adequacy” has been highly controversial, requiring reference to both substantive and structural provisions in the third country to be made by a European Commission Working Party
  - Where the level of protection is deemed inadequate, the express consent of the data subject to the proposed data transfer is required and a number of other criteria laid down in Article 26.1 must be met
  - Contracts can be used to ensure equivalency of protection and some model contracts have already been evolved

The EU Data Protection Directive

- The “Safe Harbour” Principles:
  - July 2000: after extensive discussions between the European Commission and the US Department of Commerce a set of conditions generally known as the “safe harbour” principles were accepted, which include a set of Frequently Asked Questions (“FAQs”) and answers
  - The Commission will accept use of the principles by US-based institutions and companies as ensuring conformity with European requirements
  - US-based organisations will usually be self-certifying by means of a letter to the Department of Commerce containing certain minimum information
  - Principles are compatible with OECD Guidelines though there are some concerns over the limited jurisdiction of the FTC

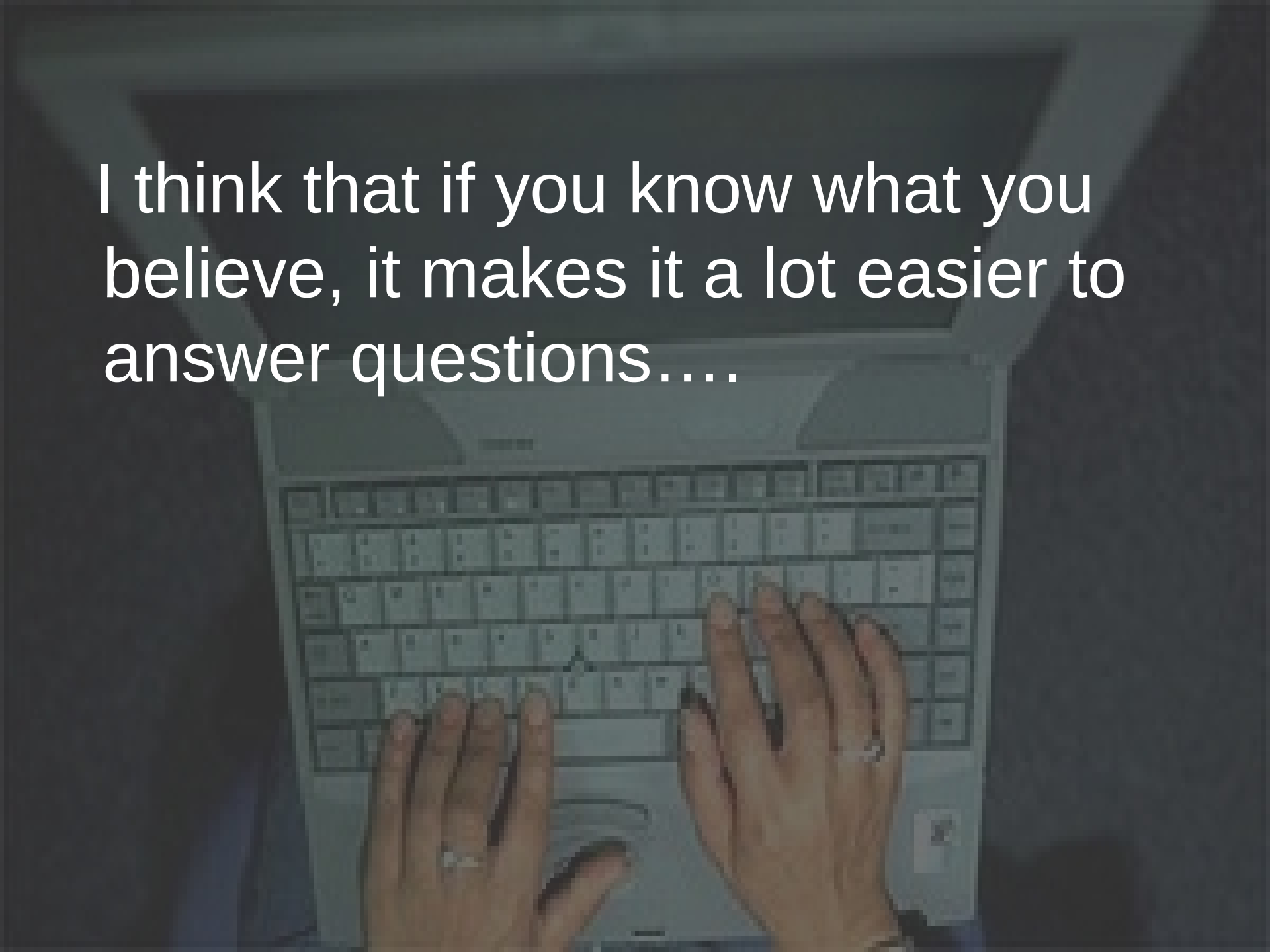
See: http://europa.eu.int/comm/internal_market/en/media/dataprot/news/decision.pdf

What Next?

- 12 July 2000: European Commission adopts a legislative proposal for a new Regulatory Framework for electronic communications – a Directive concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector" (to replace Telecommunications Directive)

  See: http://europa.eu.int/comm/information_society/policy/framework/index_en.htm

- The European Group on Ethics in Science and New Technologies, in its Opinion to the European Commission on Healthcare in the Information Society (No. 13 of 30 July 1999) has recommended that a specific Directive on medical data protection is desirable


I think that if you know what you believe, it makes it a lot easier to answer questions….

I think that if you know what you believe, it makes it a lot easier to answer questions….

- George W. Bush: responding to a question about whether he wished he could take back any of his answers in the first debate, *10 October 2000.*

I think that if you know what you believe, it makes it a lot easier to answer questions: I can’t answer your question.

- George W. Bush: responding to a question about whether he wished he could take back any of his answers in the first debate, *10 October 2000.*