

Online Privacy
Professor Ponnurangam Kumarguru
Department of Computer Science
Indian Institute of Technology, Hyderabad
Week 1
Fair Information Practices

Now, let us take a look at Fair Information Practices. What is Fair Information Practice mean.

(Refer Slide Time: 00:25)

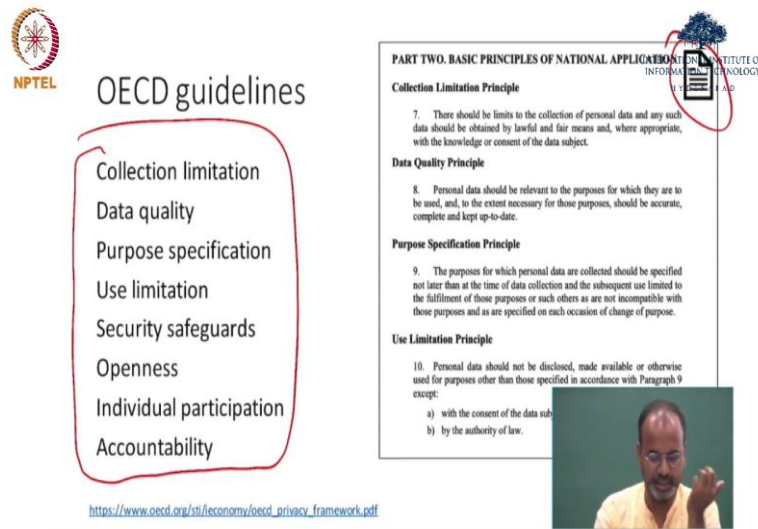


Fair Information Practices



So, this is basically information that is being collected from us. Practices, let us break the word fair. Is it fair, fairly being used information that is collected from users, consumers, citizens, practices for practices that is being done, how that information is being used. That is what we are going to look at. The, the next let us take part of this, just keep a watch on some of these topics. These are extremely important topics in terms of privacy, important concepts, also in terms of actually privacy.

(Refer Slide Time: 01:05)



The slide features the NPTEL logo on the left and the International Institute of Information Technology Hyderabad logo on the right. The main content is divided into two parts. On the left, a red-bordered box lists the 'OECD guidelines' as follows: Collection limitation, Data quality, Purpose specification, Use limitation, Security safeguards, Openness, Individual participation, and Accountability. Below this list is a URL: https://www.oecd.org/sti/economy/oecd_privacy_framework.pdf. On the right, a document snippet titled 'PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION' is shown. It contains three principles: 'Collection Limitation Principle' (Paragraph 7), 'Data Quality Principle' (Paragraph 8), and 'Purpose Specification Principle' (Paragraph 9). Below the document snippet is a small video inset of a man speaking.

So, this one, this is OECD guidelines. This is the European organization which actually looks at setting up these kind of policies, public policy, discussions, guidelines, everything. So, they came up with this list of guidelines, which says, I will go through each one of them very carefully, each one of them. But for now, quickly, it is collection, limitation, data quality, purpose specification, use limitations, security safeguards, openness, individual participation, and accountability. Those are the 8 pieces of guidelines that they created. As such these images there, so we will actually go to the OECD guideline itself. I will actually walk you through the OECD guidelines document itself.

(Refer Slide Time: 02:05)



The slide features the NPTEL logo on the left and the International Institute of Information Technology Hyderabad logo on the right. The main content is a yellow banner with the text 'THE OECD PRIVACY FRAMEWORK' in black. Below the banner is a decorative graphic of a network of nodes and lines. A small video inset of a man speaking is located in the bottom right corner.

And show you the parts where they have defined these and how these plays a role in the discussion of privacy that you will having. You will be able to relate to almost all of them because I think as users as consumers of different tools, we actually see them all over us. One discussion about WhatsApp privacy also. WhatsApp privacy policies change and what happened, we will connect to you easily when we look at the topics. So, here is the here are the definitions of the, the guidelines.

(Refer Slide Time: 02:49)

Guidelines may be affected by the division of powers in the federation.

6. These Guidelines should be regarded as minimum standards which can be supplemented by additional measures for the protection of privacy and individual liberties, which may impact transborder flows of personal data.

PART TWO. BASIC PRINCIPLES OF NATIONAL APPLICATION

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means, and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

The slide also features a small video inset of a man speaking in the bottom right corner.

First, Collection limitation principle. It reads as there should be limits to the collection of personal data. And any such data should be obtained by lawful and fairness fair means and where appropriate with the knowledge or consent of the data subject. Data subject is us, as the users. Collection limitation basically means that the, the information that is collected, right should be limited to the collection of personal data. The information that is needed only should be collected.

If Amazon has to send the book to your home, the book that you buy, they cannot be asking you for a blood group. They cannot be asking you for let us take your Aadhaar number. So, it is not necessary, they just need to they just do a credit card for taking the money or dress to send the book. So, just limit the collection of information that is necessary for doing the practice. Keep the word fair information practice also in mind, when we are going through all these guidelines.

Data quality principle, personal data should be relevant to the purposes for which they are to be used. And to the extent necessary for those purposes should be accurate, complete and kept up to date. Quality of the information should be there. The Facebook is collecting

information about me. Information that they collect should be kept updated, kept what I had given to them. Let us take I gave them birth, date of birth is a b and c which is month, day and year. They should not change. It should be kept as I have given, the quality of the information that users are sharing should be kept intact.

(Refer Slide Time: 05:05)

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDARABAD

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject; or
- b) by the authority of law.

THE OECD PRIVACY FRAMEWORK

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDARABAD

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

- a) with the consent of the data subject or
- b) by the authority of law.

THE OECD PRIVACY FRAMEWORK © OECD 2013

Purpose specification principle, the purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes. And as are specified on each occasion such change of purpose. It is, a very legal term legal way of writing.

But let us the simple ways that, look I collect, let us take this a form that you fill to attend the, let us take open, open to all sessions for the students in this class. I, I put a form, I send you the Zoom link for joining to that call for discussion of the topic. For example, many of the I asked you to watch the social dilemma. People have watched it, come let us discuss it.

That is a form, I get your email address in that I sent you the Zoom link for joining the call. That call gets done. Next, I actually have a solo seminar, that is going on privacy, I can I actually send it to you. In that email address I collected for the purpose of getting you on the call for open discussion about the topic in the class, can I actually give that information, use that information for sending you something else.

That is the guideline it should not be done is what the guideline or the principle is suggesting. Amazon is taking your cell number for giving it to the third party to deliver the product to you and make sure that you get the product. It should not be the case that the product Amazon uses that cell number to call you and sell some new products of Amazon.

Use limitation, personal data should not be disclosed made available or otherwise used for purposes other than those specified in accordance with the paragraph 9 except, it is basically arguing that purpose specification to should be done, which is to give the, the purpose specification here talks about specifying the purpose for which it is collected.

When the information is collected, I am getting the cell number that time it should be said that all this information is collected because we want to make sure that the third party will have the cell number so that the book gets delivered properly. With the consent of the sub, so when it is asked to be used for something else.

The consent of the user should be taken. If you remember I think earlier, I mentioned about medical the hospital sharing the data when I was mentioning about an anonymity information that the hospital is sharing with a third-party analytics company to get some analysis done. So, the limitation of the use should be specified earlier, the hospital sharing that information with third parties necessary.

But, if the, hospital is sharing that information further, then the user has to be consented into it. I think during that time I also explained about the first physician and the secondary physician, primary physician and secondary, secondary physician getting access to your data, getting access to your medical records, the console from the user has to be there. That is what this is saying with the consent of the data subject or by the authority of law.

(Refer Slide Time: 09:30)



Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. Individuals should have the right:
- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
 - b) to have communicated to them, data relating to them
 - i. within a reasonable time;
 - ii. at a charge, if any, that is not excessive;
 - iii. in a reasonable manner; and



Security safeguards principle. Personal data should be protected by a reasonable security guard this is a typical security measure, which is data should be encrypted data should be kept in a place which is not accessible to many people. That is what it says security guards against such risk as a loss or unauthorized access destructions use modification or disclosure of the data.

Openness principle, that should be a general policy of openness about developments practices, and policies with respect to the personal data mean should be readily available of establishing the existence and nature of the personal data and the main purposes of their use, as well as their identity and usual residence of data.

So, I am reading it, because this is very technical in terms of the definitions. So, I am just reading it otherwise, Openness principle is allowed. So, the company should be open, open about the development practices and be able to actually share it with the users of the data also.

(Refer Slide Time: 10:53)



13. Individuals should have the right:
- a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to them;
 - b) to have communicated to them, data relating to them
 - i. within a reasonable time;
 - ii. at a charge, if any, that is not excessive;
 - iii. in a reasonable manner; and
 - iv. in a form that is readily intelligible to them;
 - c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and
 - d) to challenge data relating to them and, if the challenge is successful to have the data erased, rectified, completed or amended.



Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.



Individual participation should have the right to obtain data from a data controller or otherwise, confirmation of whether or not the data controller has data relating to them. So, this is again, going back to the policy that we talked about? Can you get access to your data from Facebook? Individual participation, you should be, you should be allowed to have access to that information of yours to be given valid reasons if a request made. So, if you make a request to Facebook, and Facebook is denying to give you the data, there should be some explanation for it.

(Refer Slide Time: 11:33)



14. A data controller should be accountable for complying with measures which give effect to the principles stated above.



THE OECD PRIVACY FRAMEWORK © OECD 2013



Accountability is a data controller should be accountable for complying with measures, which give effect to the principles stated above. So, it is basically arguing that if there is any

problem with the, let us take the breach happens because of in, in LinkedIn? We, we you may have seen that, or LinkedIn data got stolen, Facebook's user name and passwords got stolen. All of this if it happens, what is the accountability of the company?

And that should be stated prior? Should there be some legal action against them? Should they actually go tell all the customers? Should they send out a notification to all Facebook users saying that look, your username and password may be actually compromised? Those are the things that one should take care of. Those are the principles. Again, this is a pretty long document of 154 pages. I am not expecting you to read and I do not think so it is necessary to read. But please go and look at these principles or case more in detail as you get some time. So, that is OECD guidelines.

(Refer Slide Time: 13:03)

The slide is divided into two main sections. On the left, under the NPTEL logo, is the heading 'FTC principles' followed by a red-bordered box containing a list of five principles: 'Notice and disclosure', 'Choice and consent', 'Data security', 'Data quality and access', and 'Recourse and remedies'. Below this list is a URL: https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv_23a.pdf. On the right, under the International Institute of Technology logo, is the heading 'III. FAIR INFORMATION PRACTICE PRINCIPLES'. Below this is section 'A. FAIR INFORMATION PRACTICE PRINCIPLES GENERAL PRINCIPLES' which includes a paragraph of text and a sub-section 'I. NOTICE/AWARENESS' with its own paragraph of text. A small video inset in the bottom right corner shows a man in a yellow shirt speaking.

Next, we will look at FTC. FTC stands for Federal Trade Commission. This is in the US now. They looked at the OECD guidelines and said that look, we can actually change it a little bit and come up with a simpler set of guidelines. They made it notice and disclosure concern, choice and concerned data security, data quality and access, risk recourse and remedies.

Which kind of overlaps with many of the things that are there in the OECD, but also change this a little bit. So, let us see what they are and how they are similar and how they are different. Again, let us go to the document itself. FTC, FTC guidelines. That is the FTC guidelines document. That is the FTC guidelines document, which is published in 1998. And I will take you to the specific page where it is only the definition of what we are looking for.

(Refer Slide Time: 14:13)



A. FAIR INFORMATION PRACTICE PRINCIPLES GENERALLY



Over the past quarter century, government agencies in the United States, Canada, and Europe have studied the manner in which entities collect and use personal information — their “information practices” — and the safeguards required to assure those practices are fair and provide adequate privacy protection.²⁷ The result has been a series of reports, guidelines, and model codes that represent widely-accepted principles concerning fair information practices.²⁸ Common to all of these documents [hereinafter referred to as “fair information practice codes”] are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

I. NOTICE/AWARENESS

The most fundamental principle is notice. Consumers should be given notice of an entity’s information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.²⁹ Moreover, three of the other principles discussed below — choice/consent,



are five core principles of privacy protection: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.



I. NOTICE/AWARENESS

The most fundamental principle is notice. Consumers should be given notice of an entity’s information practices before any personal information is collected from them. Without notice, a consumer cannot make an informed decision as to whether and to what extent to disclose personal information.²⁹ Moreover, three of the other principles discussed below — choice/consent, access/participation, and enforcement/redress — are only meaningful when a consumer has notice of an entity’s policies, and his or her rights with respect thereto.³⁰

While the scope and content of notice will depend on the entity’s substantive information practices, notice of some or all of the following have been recognized as essential to ensuring that consumers are properly informed before divulging personal information:

- C identification of the entity collecting the data;³¹
- C identification of the uses to which the data will be put;³²
- C identification of any potential recipients of the data;³³



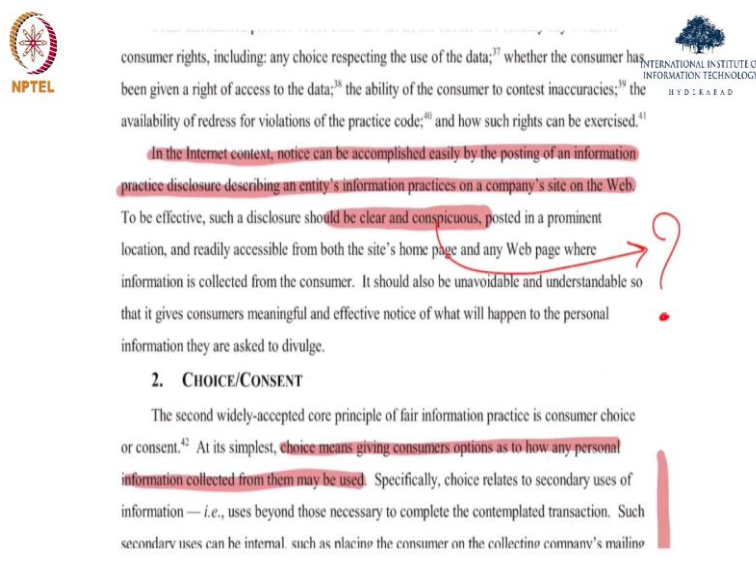
Fair information practice principles, generally. So, it talks about the principles that I have already said in the slide. What is the definition of notice and awareness? That is the first guideline from FTC, which says the most fundamental principle is notice. Consumers should be given notice of an entity's information practice before any personal information is collected without notice as consumer cannot make an informed. See the words that have said before coming back. I said earlier about informed decision as to whether and to what extent to disclose personal information.

Moreover, three of the other principles disclosed below choice concerned access participation and enforcement address this are only meaningful when the consumer notice. Unless the user

knows the privacy policy unless the user is informed about the, the practices of the organization, none of the policies actually are going to make any sense. That is the argument.

It is this saying the while the scope and the content of notice will depend on the entity substantive information practices, notice of some or all of the following have been recognized as essential. Which is identification of the entity collecting the data, identification of the uses to which so this is connecting to the OECD also, how the information is collected, what information is collected, who have, who will have access to that information, all that. That is the bigger list. Let you to go through if you are interested in.

(Refer Slide Time: 16:08)



The slide features the NPTEL logo on the left and the International Institute of Information Technology Hyderabad logo on the right. The main text discusses consumer rights, including choice, access, contesting inaccuracies, and redress. A red box highlights a sentence about internet notice, and a red question mark is drawn next to it. Below this, a section titled '2. CHOICE/CONSENT' discusses the principle of consumer choice and consent, with another red box highlighting a sentence about choice meaning options on how personal information is used.

consumer rights, including: any choice respecting the use of the data;³⁷ whether the consumer has been given a right of access to the data;³⁸ the ability of the consumer to contest inaccuracies;³⁹ the availability of redress for violations of the practice code;⁴⁰ and how such rights can be exercised.⁴¹

In the Internet context, notice can be accomplished easily by the posting of an information practice disclosure describing an entity's information practices on a company's site on the Web.

To be effective, such a disclosure should be clear and conspicuous, posted in a prominent location, and readily accessible from both the site's home page and any Web page where information is collected from the consumer. It should also be unavoidable and understandable so that it gives consumers meaningful and effective notice of what will happen to the personal information they are asked to divulge.

2. CHOICE/CONSENT

The second widely-accepted core principle of fair information practice is consumer choice or consent.⁴² At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information — *i.e.*, uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing

In the internet context, notice can be accomplished easily by posting an information practice disclosure, describing an entity's Information Practices on a company's website. To be effective, such a disclosure should be clear and conspicuous. Alright, so but the question mark here is that, are they? Is the question.

It is going to be we will look at it later in the course also, are these privacy policies legible? Is it is possible to read? If I let you to read the privacy policy? How much will you understand all that. But the, point here is that in terms of internet, it is easy to give the, the first. It is easy to actually deploy the first principle, which is notice and awareness, because it is, we just have to put it on the privacy policy.

(Refer Slide Time: 17:10)



information they are asked to divulge.

2. CHOICE/CONSENT

The second widely-accepted core principle of fair information practice is consumer choice or consent.⁴² At its simplest, choice means giving consumers options as to how any personal information collected from them may be used. Specifically, choice relates to secondary uses of information — i.e., uses beyond those necessary to complete the contemplated transaction. Such secondary uses can be internal, such as placing the consumer on the collecting company's mailing list in order to market additional products or promotions, or external, such as the transfer of information to third parties.



8



The second principle is choice of consent. At its simplest choice means giving consumers options as to how any personal information collected from them may be used. So, it is basically saying that choice, which is also an opt in and opt out, or idea will come in here.

(Refer Slide Time: 17:35)



Privacy Online: A Report to Congress

Traditionally, two types of choice/consent regimes have been considered: opt-in or opt-out. Opt-in regimes require affirmative steps by the consumer to allow the collection and/or use of information; opt-out regimes require affirmative steps to prevent the collection and/or use of such information. The distinction lies in the default rule when no affirmative steps are taken by the consumer.⁴³ Choice can also involve more than a binary yes/no option. Entities can, and do, allow consumers to tailor the nature of the information they reveal and the uses to which it will be put.⁴⁴ Thus, for example, consumers can be provided separate choices as to whether they wish to be on a company's general internal mailing list or a marketing list sold to third parties. In order to be effective, any choice regime should provide a simple and easily-accessible way for consumers

Traditionally two types of choices are concerned regimes have been considered. Which is opt in or opt out. Which is to say that look for getting you on to a mailing list, should I just add you to a mailing list? And then say that look, go and opt out? Or should I say, I am going to add you on the mailing list, or if you are interested in the mailing list, please come and sign up here. Two different approaches, fundamentally, they are different. Generally, in terms of

privacy aware solutions, you want to keep it as an opt in solution. You want to put it into the system that users will sign up for being part of.

(Refer Slide Time: 18:28)



to exercise their choice.

In the online environment, choice easily can be exercised by simply clicking a box on the computer screen that indicates a user's decision with respect to the use and/or dissemination of the information being collected. The online environment also presents new possibilities to move beyond the opt-in/opt-out paradigm. For example, consumers could be required to specify their preferences regarding information use before entering a Web site, thus effectively eliminating any need for default rules.⁴⁵

3. ACCESS/PARTICIPATION

Access is the third core principle. It refers to an individual's ability both to access data about him or herself — i.e., to view the data in an entity's files — and to contest that data's accuracy and completeness.⁴⁶ Both are essential to ensuring that data are accurate and complete. To be meaningful, access must encompass timely and inexpensive access to data, a simple means for contesting inaccurate or incomplete data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients.⁴⁷





Highlighted part, I would like you to take a look at it if you're interested. In online environment, choice easily can be exercised by simply clicking a box. So, if you in a Slack users slack would actually tell you there's that radio button there, which will tell you to send you notifications, send you updates on the products.

So, this is a choice that you can make by checking that box or not checking that box. That is what it is saying in the online environment choice easily can be accessed by simply clicking a box on the computer screen that indicates a user's decision. Whether you want to sign up for that mailing list or not, is just in your hands in the decision that you are making.

The third one Access Participation accesses third core principle it refers to an individual's ability both to access data about him or herself that does to view the data and entities files and to contest that data accuracy. Is again going back to OCDs policy also whether you will be able to get access to the information that you shared and if there is something wrong, my data will change. It can you actually contest with the organization saying that what they did is strong.

(Refer Slide Time: 19:55)



4. INTEGRITY/SECURITY

The fourth widely accepted principle is that data be accurate and secure. To assure data integrity, collectors must take reasonable steps, such as using only reputable sources of data and cross-referencing data against multiple sources, providing consumer access to data, and destroying untimely data or converting it to anonymous form.⁴⁰



Security involves both managerial and technical measures to protect against loss and the unauthorized access, destruction, use, or disclosure of the data.⁴¹ Managerial measures include internal organizational measures that limit access to data and ensure that those individuals with access do not utilize the data for unauthorized purposes. Technical security measures to prevent unauthorized access include encryption in the transmission and storage of data, limits on access through use of passwords, and the storage of data on secure servers or computers that are inaccessible by modem.⁴⁰

5. ENFORCEMENT/REDRESS

It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.⁴¹ Absent an enforcement and redress mechanism, a

Integrity and security is very similar to the safe guard security safeguard policy of OECD, which is to give protection to the data. Encryption storage, physical security. Here, it also talks about both managerial and technical measure. Both at the level of technical solutions, and the system level solution should be provided for making sure that the data is protected.

(Refer Slide Time: 22:32)



through use of passwords, and the storage of data on secure servers or computers that are inaccessible by modem.⁴⁰

5. ENFORCEMENT/REDRESS

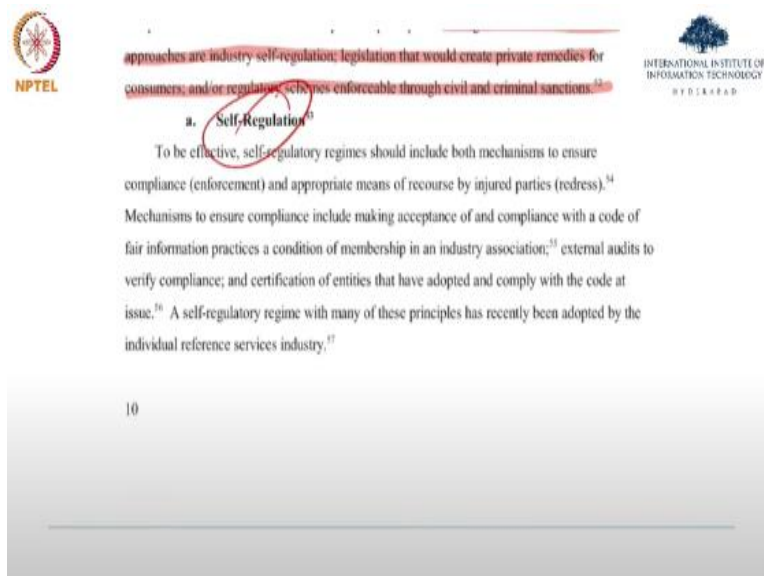
It is generally agreed that the core principles of privacy protection can only be effective if there is a mechanism in place to enforce them.⁴¹ Absent an enforcement and redress mechanism, a fair information practice code is merely suggestive rather than prescriptive, and does not ensure compliance with core fair information practice principles. Among the alternative enforcement approaches are industry self-regulation; legislation that would create private remedies for consumers; and/or regulatory schemes enforceable through civil and criminal sanctions.⁴²

a. Self-Regulation⁴³

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress).⁴⁴ Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association;⁴⁵ external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue.⁴⁶ A self-regulatory regime with many of these principles has recently been adopted by the

Enforcement and redress among the alternative enforcement. So, this basically is a bar the approaches that are provided for if something goes wrong, which is the accountability that we saw in OACD. If something goes wrong, who should have who should you go to? What provisions do we have? What should the company do about it, all of that is written in this enforcement, remedies, enforcement redress.

(Refer Slide Time: 21:04)



The slide features the NPTEL logo on the left and the International Institute of Information Technology Hyderabad logo on the right. The main text discusses industry self-regulation and private remedies. A red circle highlights the section title 'a. Self-Regulation'. The text explains that self-regulatory regimes should include enforcement mechanisms and redress for injured parties. It lists several mechanisms: acceptance of a code of fair information practices as a membership condition, external audits, and certification of compliance. A reference to the individual reference services industry is also included.

approaches are industry self-regulation, legislation that would create private remedies for consumers, and/or regulatory schemes enforceable through civil and criminal sanctions.⁵³

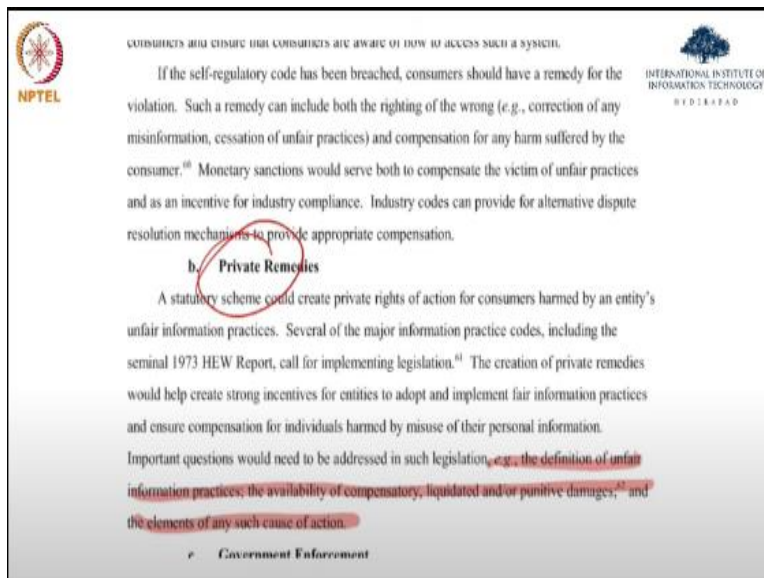
a. Self-Regulation⁵⁴

To be effective, self-regulatory regimes should include both mechanisms to ensure compliance (enforcement) and appropriate means of recourse by injured parties (redress).⁵⁴ Mechanisms to ensure compliance include making acceptance of and compliance with a code of fair information practices a condition of membership in an industry association;⁵⁵ external audits to verify compliance; and certification of entities that have adopted and comply with the code at issue.⁵⁶ A self-regulatory regime with many of these principles has recently been adopted by the individual reference services industry.⁵⁷

10

Self-regulation. So, there are multiple methods for self-regulation is, companies all put together say that, this is what we will follow.

(Refer Slide Time: 21:13)



The slide features the NPTEL logo on the left and the International Institute of Information Technology Hyderabad logo on the right. The main text discusses private remedies for consumers. A red circle highlights the section title 'b. Private Remedies'. The text explains that a statutory scheme could create private rights of action for consumers harmed by unfair information practices. It references the seminal 1973 HEW Report and discusses the need for legislation to address questions like the definition of unfair information practices and the availability of damages.



CONSUMERS WILL ENSURE THAT CONSUMERS ARE AWARE OF HOW TO ACCESS SUCH A SYSTEM.

If the self-regulatory code has been breached, consumers should have a remedy for the violation. Such a remedy can include both the righting of the wrong (e.g., correction of any misinformation, cessation of unfair practices) and compensation for any harm suffered by the consumer.⁶⁸ Monetary sanctions would serve both to compensate the victim of unfair practices and as an incentive for industry compliance. Industry codes can provide for alternative dispute resolution mechanisms to provide appropriate compensation.

b. Private Remedies

A statutory scheme could create private rights of action for consumers harmed by an entity's unfair information practices. Several of the major information practice codes, including the seminal 1973 HEW Report, call for implementing legislation.⁶¹ The creation of private remedies would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information. Important questions would need to be addressed in such legislation, e.g., the definition of unfair information practices; the availability of compensatory, liquidated and/or punitive damages;⁶² and the elements of any such cause of action.

e. Government Enforcement

would help create strong incentives for entities to adopt and implement fair information practices and ensure compensation for individuals harmed by misuse of their personal information.

Important questions would need to be addressed in such legislation, e.g., the definition of unfair information practices, the availability of compensatory, liquidated and/or punitive damages,⁶³ and the elements of any such cause of action.



e. Government Enforcement

Finally, government enforcement of fair information practices, by means of civil or criminal penalties, is a third means of enforcement. Fair information practice codes have called for some government enforcement, leaving open the question of the scope and extent of such powers.⁶⁴ Whether enforcement is civil or criminal likely will depend on the nature of the data at issue and the violation committed.⁶⁵

11

These are the policies, that is private remedies, which is, again, a set of guidelines that companies come up with, which is that they would follow. Third one is, of course, the government enforcement saying, government is putting a rule saying you cannot do you need to have a privacy policy and the privacy policy should be definitely followed, otherwise, you will have legal ramifications.

(Refer Slide Time: 21:50)





monitor their children's interactions and to help protect their children from the risks of inappropriate online interactions.

2. ACCESS/PARTICIPATION AND INTEGRITY/SECURITY

Since parents may not be fully aware of what personal information a site has collected from their child, the access/participation principle is a particularly important one with respect to information collected from children. To provide informed consent to the retention and/or use of information collected from their children, parents need to be given access to the information collected from their children, particularly if any of the information is collected prior to providing notice to the parent. The principle of integrity, which addresses the accuracy of the data, is also

13



And this is a longer document, if interested, please go take a look at it. But otherwise, that is what is OECD principles and FTC guidelines, which allows users to understand how their information is being used for practices that the companies have. That is the end of week 1. So, the week one generally, what did we look at? We looked at what the definition of privacy

is, we will come back to some of these again, in different forms, but not looking at so theoretically, as we did today, as we did in this week.

So, we saw what privacy is well, what are the privacy attitudes in awareness, privacy in this is states have privacy. Then FTC principles FTC guidelines OECD guidelines. That is week 1. Look forward to having you in week two class. Thank you.