

Online Privacy
Professor Ponnurangam Kumaraguru
Privacy laws and regulations (Part-1)

Welcome back to week 11. I hope you are enjoying the class again. I hope it is making some connection to your otherwise discussions, otherwise interactions with people outside the class; given the topic I am guessing that some of it is making sense in the real world also, you are able to connect to it, you are able to think through some topics that we see in the class. So this is week 11. So, primarily what we are going to cover in week 11 is Privacy Laws and Regulations.

I think it is extremely important to think about have an understanding of the laws and regulations also because I think as technologists we generally end up thinking more of technology and less of laws and regulation. I think, we will not go into detail. What I am going to go through is I am going to give a list of, say dump a list of act and laws around the privacy across the world.

Some discussion around, what is happening around the world, but primarily then focus on our IT Act, India 2000, IT Act, amendments of 2000 and 2008. Then Personal Data Production Bill that is under review and Non-personal Data Framework that has been proposed and lastly GDPR, which is a European Privacy Directive. So those four things I will go in detail but other than that I will keep many things slightly abstract.

(Refer Slide Time: 2:22)

What we have covered until now

- What is Privacy?
- Why study Privacy?
- Fair Information Practices
- Right-To-Privacy
- Contextual Integrity
- Privacy Policy
- Privacy Enhancing Technologies
- Privacy Invasive Technologies
- Social Media Privacy
- Identity resolution
- Privacy nudges
- Cookies
- Ethics / IRB

- Why anonymize - AOL, Netflix
- Methods for anonymization
- Cost of Reading Privacy Policies
- Conducting (User, Lab, and Online) Studies
- Reading research papers
- Voter Privacy Leaks
- Browser Privacy Leaks
- Profiling from publicly available information
- LBSN - Privacy
- Mobile #s publicly available

NPTEL

INTERNET INSTITUTE OF INFORMATION TECHNOLOGY
MADRAS

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDRABAD

Privacy 101

What we have covered until now

- What is Privacy?
- Why study Privacy?
- Fair Information Practices
- Right-To Privacy
- Contextual Integrity
- Privacy Policy
- Privacy Enhancing Technologies
- Privacy Invasive Technologies
- Social Media Privacy
- Identity resolution
- Privacy nudges
- Cookies
- Ethics / IRB

- Why anonymize – AOL, Netflix
- Methods for anonymization
- Cost of Reading Privacy Policies
- Conducting (User, Lab, and Online) Studies
- Reading research papers
- Voter Privacy Leaks
- Browser Privacy Leaks
- Profiling from publicly available information
- LBSN – Privacy

What have we covered until now? We have covered, particularly in the last class we covered this very interesting thing of how to use mobile phones, that is publicly available on how to create privacy awareness among people. We also looked at location-based services. How your check-ins, your tips done on foursquare can be used to find out where you live, where you work, all those kind of information.

And then the rest is until week on 10 we have seen basics of privacy, anonymization techniques all of that. Again, please remember this is an introduction to class, so if I were to say this is privacy 101 class. I am sure if there are students in class who are interested in taking any of these topics, there are specialized courses only on these topics, for example, only anonymization. I know people teach only anonymization techniques.

A different class for example, this week on privacy laws and regulations, I am pretty sure we can teach our one semester course on details of laws and regulations on privacy. Why do we need laws and regulations? So, laws and regulations are generally the top-down approach, which is constitutional rights, Indian Penal Code Act or a law level provides provision for privacy, then it becomes much more easier to implement it. And having a regulation will also be able to restrict, give deterrent for criminals to misuse the data.

Enable people to use the mechanisms in a better way, all of that will happen if it is in the top-down approach, which is what a law regulation is written for the country, everybody should follow it. Income Tax returns income, Income Tax returns has to be filed as in 31st of March and with some relaxation of dates if you are not submitting it is actually a crime. So that is why laws and regulations are extremely important.

(Refer Slide Time: 5:09)

 Privacy laws around the world 

Privacy laws and regulations vary widely throughout the world

US has mostly sector-specific laws, with relatively minimal protections

Federal Trade Commission has jurisdiction over fraud and deceptive practices

Federal Communications Commission regulates telecommunications

European Data Protection Directive requires all European Union countries to adopt similar comprehensive privacy laws that recognize privacy as fundamental human right

Privacy commissions in each country (some countries have national and state commissions)

GDPR
General Data Protection Regulation <https://edps-info.eu/>

PDP Bill

Handwritten notes: FTC, FCC, US/Europe



 Privacy laws and regulations vary widely throughout the world 

US has mostly sector-specific laws, with relatively minimal protections

Federal Trade Commission has jurisdiction over fraud and deceptive practices

Federal Communications Commission regulates telecommunications

European Data Protection Directive requires all European Union countries to adopt similar comprehensive privacy laws that recognize privacy as fundamental human right

Privacy commissions in each country (some countries have national and state commissions)

GDPR
General Data Protection Regulation <https://edps-info.eu/>

PDP Bill

Handwritten notes: US/Europe, ↓ sectoral



3 Some US privacy laws



So, let us look at privacy laws around the world. Now let us like take a whirlwind tour of what privacy is across the world and then we will focus it on only in India. Privacy laws, privacy laws around the world gives, so US, so two very clear distinction between US and Europe you will see. The way that they think about privacy laws itself is very different. US takes very much like a sectoral specific, which is for a few slides later.

The slide if you see every law is for a particular sector. It is a credit card, financial, communication, information, it is specifically written for a particular sector, whereas Europe does it at a generic and a directive level. They would say that look this is what we define privacy as. This is how it should be implemented and leave the implementation for the every sector, every organization to take it and implement it in their work.

I mean, you can discuss pros and cons of each of them, sectoral specific because in sectoral specific, meaning if, I mean, for organizations which are involved they have to actually understand, for example, let us take if TCS and Wipro are involved in projects with the US, just imagine the different sectors if they are implementing projects, they have to know different acts very well, laws very well.

Whereas European directive is just one, either you do it in Telecom or you do it in financial sector, everything is just the same but the advantages of sectoral is that it can be very detailed, the act can be very detailed the implementation becomes slightly easier because it is very detailed, you have all details necessary for implementing the act or a act. So, that is why, so that is the clear distinction between US and Europe.

I mean there must be some reasons why US and Europe decided to go in these two different directions. So US mostly sector specific laws with relatively minimal protections, Federal Trade Commission, FTC, we have mentioned FTC in the class quite a few times as jurisdictions over fraud and deceptive practices. Federal Communications commission regulates telecommunication.

So this is another organization called FCC, this is an organization called FTC. European directives requires all European countries to adapt similar comprehensive privacy laws that recognize privacy as fundamental human rights, that is the GDPR requirement now. So they have privacy commissions in each country who help, I mean, which is a team, which helps in implementing this at a government level.

GDPR, we look at GDPR in detail, so we can skip it here and then PDP Bill; that is the Indian version of privacy protection. That is the US and Europe side.

(Refer Slide Time: 9:31)

The slide lists the following US privacy laws with their respective URLs:

- Fair Credit Reporting Act, 1971
<http://www.ftc.gov/os/statutes/031224fcra.pdf>
- Privacy Act, 1974
<http://www.usdoj.gov/oip/privstat.htm>
- Right to Financial Privacy Act, 1978
<http://www.fdic.gov/regulations/laws/rules/6500-2550.html>
- Cable TV Privacy Act, 1984
http://epic.org/privacy/cable_tv/ctpa.html
- Video Privacy Protection Act, 1988
<http://www4.law.cornell.edu/uscode/18/2710.html>
<http://epic.org/privacy/vppa/>
- Family Educational Right to Privacy Act, 1993
<http://www.ed.gov/policy/gen/reg/ferpa/index.html>
- Electronic Communications Privacy Act, 1994
<http://www4.law.cornell.edu/uscode/18/2701.html>
- Freedom of Information Act, 1966, 1991, 1996
<http://www.usdoj.gov/oip/index.html>

The slide also features the NPTEL logo on the top left and the International Institute of Information Technology logo on the top right. A video feed of a presenter is visible in the bottom right corner.

Let us look at the US, even though I looked at it quickly, if you look at the US Privacy Acts. So, the first one is Fair Credit Reporting Act, only looking at credit cards, credits system, different aspects of credit system, how information should be collected. So, in general I think all of them will fit the concepts that we have seen before, which is fair information practices, concerned, limitation of collection, limitation principle.

How the information will be used, how long will the information be kept? All of that is just the same, but the sectoral implementations are different. Privacy Act, a broader version of the

privacy expectations, right to financial Privacy Act, which is getting into banking, getting into your financial information of the citizens. There is also Cable TV Privacy Act. Cable TV, Internet, TV, so the TV as a communication was a very strong earlier.

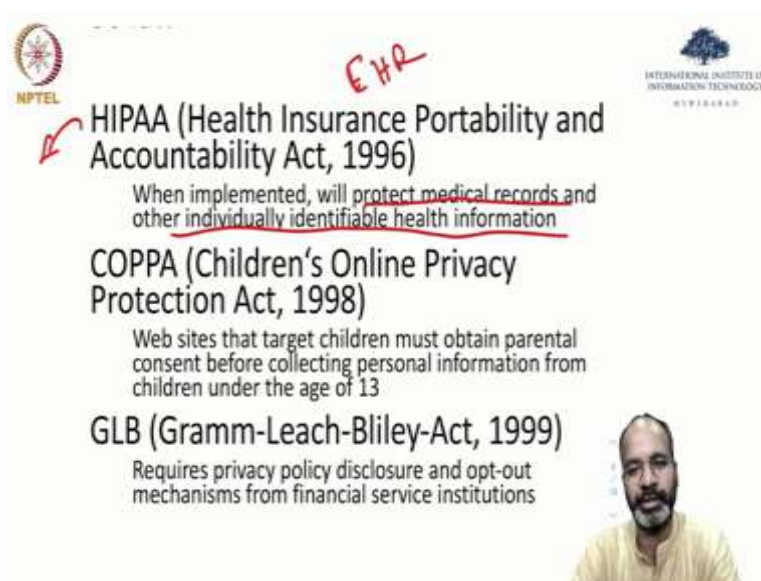
So that is the act, Privacy Act that is written, which is what ads can be presented, what information can you collect, can you know, can the TV channel know what programs you are actually watching for longer, if they know about it what can they do about it, do with that information, all that is discussed in this Cable TV Privacy Act.

Video Privacy Protection Act, again aspects of the TV Act itself. FERPA is for Family Education Right to Privacy Act. This is an interesting act because this allows you as a student control who gets access to your education details. For example, here in India the institute can send a letter home with your grades potentially, whereas in the US that is not possible unless and until you get explicit concern from the students saying the parents can know the grades, it is not possible to send these grades.

So that is what this Family Education Right to Privacy Act gives protection for who to get access to students grades will be controlled by, not just grades, any information about the student I guess, how well they are performing in school, are they having any depression issues, are they having any financial issues inside the campus, all of that is controlled by this act, meaning the citizen gets protection through this act.

Electronic Communications which are, see electronic communications, video, cable TV, all of this if you just think about it 15 - 20 years, 30 years before was necessary because those were the ways of communication. A Freedom of Information Act, this is again giving protection for citizens, it has had multiple versions and the entire gamut of this privacy acts in the US protects the US citizens.

(Refer Slide Time: 13:20)



NPTEL logo on the left and International Institute of Information Technology Hyderabad logo on the right. The slide lists three acts:

- HIPAA (Health Insurance Portability and Accountability Act, 1996)** - Handwritten "EHR" in red above it. A red arrow points to the text: "When implemented, will protect medical records and other individually identifiable health information".
- COPPA (Children's Online Privacy Protection Act, 1998)** - Text: "Web sites that target children must obtain parental consent before collecting personal information from children under the age of 13".
- GLB (Gramm-Leach-Bliley-Act, 1999)** - Text: "Requires privacy policy disclosure and opt-out mechanisms from financial service institutions".

A small video feed of a man is visible in the bottom right corner.



NPTEL logo on the left and International Institute of Information Technology Hyderabad logo on the right. The slide lists several acts with red circles around their titles and URLs:

- Fair Credit Reporting Act, 1971** - URL: <https://www.ftc.gov/os/statutes/031224fcra.pdf>
- Privacy Act, 1974** - URL: <http://www.usdoj.gov/oip/privstat.htm>
- Right to Financial Privacy Act, 1978** - URL: <http://www.fdic.gov/regulations/laws/rules/6500-2550.html>
- Cable TV Privacy Act, 1984** - URL: http://epic.org/privacy/cable_tv/ctpa.html
- Video Privacy Protection Act, 1988** - URL: <http://www4.law.cornell.edu/uscode/18/2710.html> and <http://epic.org/privacy/vppa/>
- Family Educational Right to Privacy Act, 1993** - URL: <http://www.ed.gov/policy/gen/reg/ferpa/index.html> - Handwritten "FERPA" in red to the right.
- Electronic Communications Privacy Act, 1994** - URL: <http://www4.law.cornell.edu/uscode/18/2701.html>
- Freedom of Information Act, 1966, 1991, 1996** - URL: <http://www.usdoj.gov/oip/index.html>

A small video feed of a man is visible in the bottom right corner.

Just to take a slightly longer explanation of a few other acts in the US, which is HIPAA. HIPAA is a very popular, so FERPA, so this is called FERPA. FERPA, HIPAA are all slightly popular acts in the US. HIPAA is about, everything about your visits to the hospital, who gets access to your medical records, for example, I as a patient go to the hospital, give my, meet a doctor, physician and some regular checkups, some discussion, some medication is given, I come back.

Next time when I go to the hospital this physician is not there, whereas another physician is going to get access to the data of mine, for that also they need approval from me saying that I am allowing the hospital to have access to the data for a different physician because the

physician one, primary physician is not around. There are many things like this, one example is what I am giving you, otherwise who gets access to the data.

For example, I said which physician, how long should they have access to data, if I move from hospital to hospital what information is shared from hospital to hospital, all of this is controlled by HIPAA Act, which is called Health Insurance Portability and Accountability Act. It will protect medical records and other individual identifiable health information. India also we have been talking about electronic, EHR.

Electronic Health Records and transfer of these records between hospitals all that is going on and very recently there has been a huge discussion around setting up national level infrastructure for these kind of transfer between hospitals, patients' details all that. COPPA is another act which looks at only children's online privacy.

Again it was passed in 1998, you can see the relevance then very, very relevant because of the needs of where more children were getting online and this would protect what information can the organizations collect if the children is a minor. Do they need parental control? What parental control is allowed, what is not allowed? Even under parental control what information can child be able to see?

So if you think, if you look at YouTube and all, if you are less than 13 they do not give you access to anything other than cartoons, anything other than very basic cartoon and then if you have, your parental control gives you access to some more videos some more content on YouTube, so that kind of protection what YouTube is implementing would fall under COPPA. GLB is very similar to the financial one that we saw, financial privacy here.

Here it is a modified version, advanced version of the Financial Act. GLB is again what bank can use my personal information for, can they transfer the information between banks, can they sell their own products to me, can they do advertisement, all of that is controlled by GLB. Gramm-Leech-Bliley Act and again requires privacy, policy disclosure and opt-out mechanisms of financial service institutions.

(Refer Slide Time: 18:00)






Membership

US companies self-certify adherence to requirements
Dept. of Commerce maintains signatory list
<http://www.export.gov/safeharbor/>

Signatories must provide

- notice of data collected, purposes, and recipients
- choice of opt-out of 3rd-party transfers, opt-in for sensitive data
- access rights to delete or edit inaccurate information
- security for storage of collected data
- enforcement mechanisms for individual complaints

Approved July 26, 2000 by EU
reserves right to renegotiate if remedies for EU citizens prove to be inadequate




Membership

US companies self-certify adherence to requirements
Dept. of Commerce maintains signatory list
<http://www.export.gov/safeharbor/>

Signatories must provide

- ~~notice of data collected, purposes, and recipients~~
- ~~choice of opt-out of 3rd-party transfers, opt-in for sensitive data~~
- ~~access rights to delete or edit inaccurate information~~
- ~~security for storage of collected data~~
- ~~enforcement mechanisms for individual complaints~~

Approved July 26, 2000 by EU
reserves right to renegotiate if remedies for EU citizens prove to be inadequate



Some US privacy laws

- Fair Credit Reporting Act, 1971
<http://www.ftc.gov/os/statutes/031224fcra.pdf>
- Privacy Act, 1974
<http://www.usdoj.gov/oip/privstat.htm>
- Right to Financial Privacy Act, 1978
<http://www.fdic.gov/regulations/laws/rules/6500-2550.html>
- Cable TV Privacy Act, 1984
http://epic.org/privacy/cable_tv/ctpa.html
- Video Privacy Protection Act, 1988
<http://www4.law.cornell.edu/uscode/18/2710.html>
- Family Educational Right to Privacy Act, 1993
<http://www.ed.gov/policy/elseq/ferpa/index.html>

Handwritten annotations: 'Sectoral' (top), 'FERPA' (next to the 1993 law), and various red circles and arrows highlighting parts of the list.

Safe harbor is another interesting concept that has come between the US and the Europe, where I mean, if data is moving from, so Europe because of this very strong. I mean, we talked about US and Europe having sectoral and directives, Europe generally has ended up having very stronger privacy expectations compared to the US at least.

And therefore, when the data is moving from US to Europe for any of the cross-border transactions, cross-border business reasons, then Europe wanted to have some level of control over the expectations of privacy, because it is coming from the US where the privacy expectations are slightly lesser compared to the Europe, so therefore if information of European citizens goes into the US and it gets misused, what protection can they get.

I think it is the same thing when it is coming to India, both Europe and US data are coming to you India for offshored business, so there also again protection is given. In India until now the primary way a protection has been given is through the contractual law and so in the contract it is written saying that, I as a company, as in Wipro, Infosys will protect the data, blah blah, in these forms. Because there is no overarching expectations of privacy there.

But some of these organizations have implemented these expectations and they also have certifications for these implementations, everything to show that they are protecting the data well, so the companies can actually give them the business and they will, the engineers who are involved in it, the team which is involved in accessing this data understand the privacy, everything, so US companies self-certify. So, how does the safe harbor work?

The companies actually self-certify, the US companies self-certify adherence to requirements, Department of Commerce maintains a signatory list, who are all the companies that are saying that, look we will protect the data if it comes from Europe with a high standards. Must provide notice of data collected, purposes and recipients, choice of opt-out of third-party transfers, opt-in for sensitive data, access rights to delete or edit inaccurate information.

Security for storage of collected data, enforcement mechanism for individual complaints, so again these are just a version of fair information practices that we saw earlier in the course. So this is a 2000 approved Safe Harbor Act. Reserves right to renegotiate if remedies of Europe citizens prove to be inadequate. I think these are, I mean, if the business needs more privacy, then they can actually renegotiate is what is explicitly stated here.

(Refer Slide Time: 21:35)

The slide is titled "Data protection in India" and features logos for NPTEL and the International Institute of Information Technology. The main text reads: "The customer data from foreign countries can be protected through" followed by a list of laws: Indian Contract Act, 1872 (circled in red), Indian Penal code, 1960, Special Relief Act, 1963, Consumer Protection Act, 1986, IT ACT 2000 (amendments 2008), Possible Tort law, and PDP Bill. A small video inset of a man is visible in the bottom right corner.

So, let us look at India now. So this looks at Europe and the US, this is primarily the US which is US privacy laws list, HIPAA, COPPA, GLB, all that, Safe Harbor between US and Europe. Now let us look at India. India the, as of now there is no specific explicit privacy law, but there are many places where we get actually our privacy protections written.

Indian, so I mentioned about earlier the Infosys and Wipro do business using this Contractual Act provision. Indian Penal Code provides some provision, Special Relief Act, Customer Protection Act, IT Act 2000 amendment in 2008, some Tort laws which is a broader way by which India has laws specified, PDP Bill that I mentioned earlier. Constitution also has some reference to, wave reference to privacy.

(Refer Slide Time: 22:50)

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDRABAD

IT Act 2000

के-27] सं विधान, राजपत्र, मूल 8, 2000 / संकेत 19, 1922
No. 27] NEW DELHI, FRIDAY, JUNE 9, 2000 / JYAISTHA 15, 1922

इस भाग में किए हुए संकेत दो नहीं हैं जिससे कि यह आदेश अलग-अलग के रूप में रखा जा सके।
Separate paging is given to this Part in order that it may be filed as a separate compilation.

MINISTRY OF LAW, JUSTICE AND COMPANY
AFFAIRS (Legislative Department)

New Delhi, the 9th June, 2000/Jyestha 15, 1922 (Saka)
The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:—
THE INFORMATION TECHNOLOGY ACT, 2000
(No. 21 of 2000)

[9th June, 2000]
An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate

<http://www.mca.gov.in/section80/2000/2000020001.pdf>

So that is what is a general overview of laws around the world. Now let us specifically look at IT Act, as I said let us go into detail of IT Act. What is it, what does it provide, what provisions does it have.

(Refer Slide Time: 23:18)

NPTEL

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY
HYDRABAD

संकेत १९-१९२२-१३०६४/२००० REGISTERED NO. DL-13064/2000

भारत का राजपत्र
The Gazette of India

असाधारण
EXTRAORDINARY
भाग II—खण्ड 1
PART II—Section 1
प्रकाशित की शक्ति
PUBLISHED BY AUTHORITY

AFFAIRS (Legislative Department)
 New Delhi, the 9th June, 2000 (Jyaishta 19, 1922 (Saka))

The following Act of Parliament received the assent of the President on the 9th June, 2000, and is hereby published for general information:—

THE INFORMATION TECHNOLOGY ACT, 2000
 (No. 21 OF 2000)


[9th June, 2000]

An Act to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

WHEREAS the General Assembly of the United Nations by resolution A/RES/51/162, dated the 30th January, 1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade Law;

AND WHEREAS the said resolution recommends *inter alia* that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information;

AND WHEREAS it is considered necessary to give effect to the said resolution and



records.


BE it enacted by Parliament in the Fifty-first Year of the Republic of India as follows:—

CHAPTER I
PRELIMINARY

1. Short title, extent, commencement and application

(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person.



So, I am going to walk through the actual bill itself, so this is the actual bill that has been passed for and review now it is the... So the definition of an act - An Act to provide legal recognition for transactions carried out by means of electronic data interchange. So, please, remember this that the IT Act.

So, it is at the information technology level, not at the privacy level. Interchange and other means of electronic communication commonly referred as "electronic commerce", which involves the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with government agencies and further to amend the Indian Penal Code, blah blah. So it is basically targeting the electronic version of the documents, e-commerce as the basis.

So, again it goes into the detail of what are the definitions of the terms. That is how every Act would be written, so you will see an amendment's document also like that, GDPR also like that. So I will jump on to showing only what is in the context of privacy, that is how our interests are for this course, at least. All right, so these are all again definitions of what is generally this act is for. Let us jump to where privacy is, there are like a couple of references to privacy in this act, so let us see only them.

(Refer Slide Time: 25:03)

he may consider necessary.

30. Certifying Authority to follow certain procedures.

Every Certifying Authority shall, —

- (a) make use of hardware, software and procedures that are secure from intrusion and misuse;
- (b) provide a reasonable level of reliability in its services which are reasonably suited to the performance of intended functions;
- (c) adhere to security procedures to ensure that the secrecy and privacy of the digital signatures are assured; and
- (d) observe such other standards as may be specified by regulations.

31. Certifying Authority to ensure compliance of the Act, etc.

Every Certifying Authority shall ensure that every person employed or otherwise engaged by it complies, in the course of his employment or engagement, with the provisions of this Act, rules, regulations and orders made thereunder.

32. Display of licence.

Every Certifying Authority shall display its licence at a conspicuous place of the premises in which it carries on its business.

33. Surrender of licence.

- (1) Every Certifying Authority whose licence is suspended or revoked shall immediately after such suspension or revocation, surrender the licence to the Controller.
- (2) Where any Certifying Authority fails to surrender a licence under sub-section (1), the

So here is the first one. So it is shown under certifying authority to follow certain procedures. Certifying authority is the authority which gives you certificates, digital certificates that you can use in your web services. So, what does it say? For privacy adhere to specific procedures to ensure that the secrecy and privacy of the digital signatures are assured. It is something that the certifying authority to make sure that the digital signatures information is not otherwise available to anybody.

(Refer Slide Time: 25:55)

71. Penalty for misrepresentation.
Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any licence or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

72. Penalty for breach of confidentiality and privacy.
Save as otherwise provided in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

73. Penalty for publishing Digital Signature Certificate false in certain particulars.
(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—
(a) the Certifying Authority listed in the certificate has not issued it; or
(b) the subscriber listed in the certificate has not accepted it; or
(c) the certificate has been revoked or suspended,
unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh

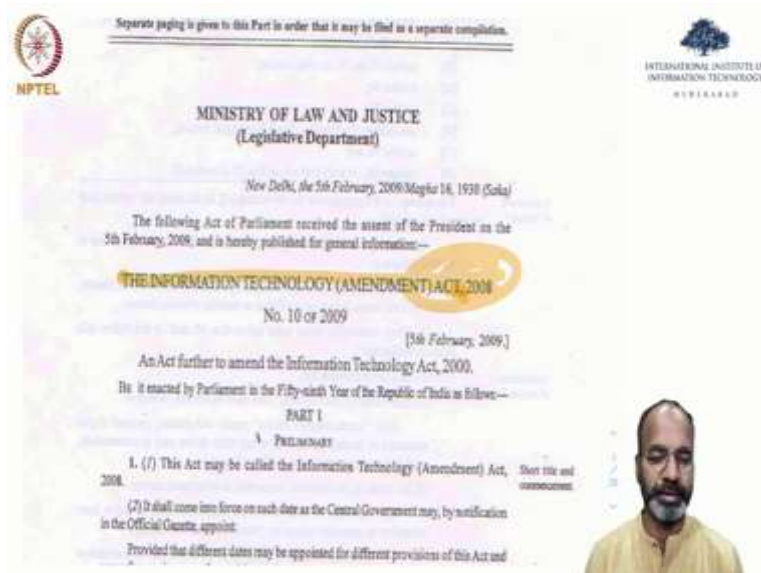
The slide also features the NPTEL logo on the left and the International Institute of Information Technology logo on the right. A video inset in the bottom right corner shows a man speaking.

Next reference is slightly longer, so this is penalty for breach of confidentiality and privacy. What it says is - Save as otherwise provided in this Act or any other law for the time being in force, any person who in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or fine which may extend to one lakh rupees, or with both.

So this is essentially saying, what is the take away from this paragraph? The paragraph basically says that, look if you have access to some information and if you are making it public without the, if you are giving it away to others without my concern, if my data is shared you are punishable. You could be punished. So that is what this paragraph is arguing. So that is the places where privacy has a reference in the IT Act.

IT Act again, IT Act is a very broad act that Indian government want to have and therefore, the reference to privacy has been very, very low. So this, when this started in 2000, the bill was presented in 2000, earlier before 2000 and the Act was created in 2000, and 2000, till 2008 people were looking at it and then they wanted amendments. So, amendments were made in 2008.

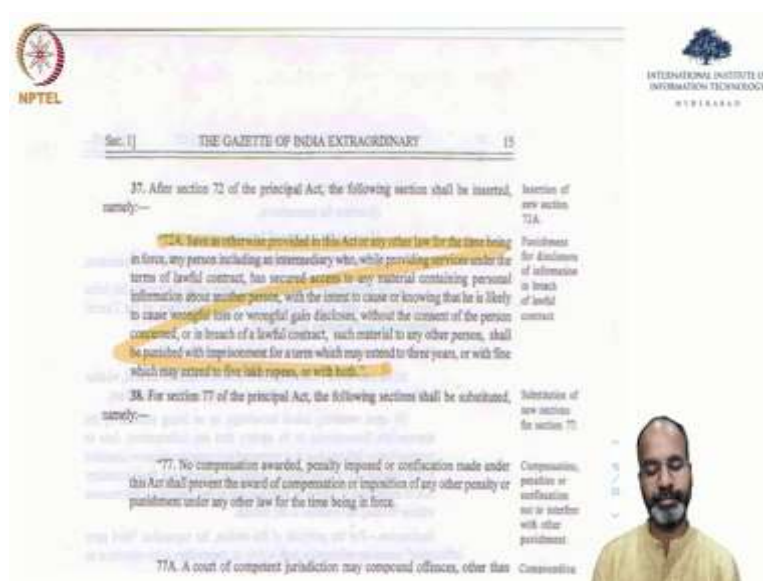
(Refer Slide Time: 27:51)



Now let us look at amendments. So this is the, so what does an amendment mean? There is already an Act, what changes do you want in that Act is what is presented in an amendment. So, if you look at it here, it says Information Technology Amendment Act, 2008. So this basically is talking only about the amendments.

Again some, only some parts we will be interested in, so let us look at that part, those parts. And I would highly encourage if you are interested in any of these topics, otherwise I would highly recommend you to go through these documents yourselves and come back to discuss any of the specifics if you are interested in.

(Refer Slide Time: 28:46)



So the amendments had one big change, this paragraph explains that, which is Section 72a. Save as otherwise provided in this Act or any other law for the time being in force, any person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause a wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a law contract, such material to any other person, shall be punished with imprisonment for a term maybe extend up to three years, or fine which may extend to five lakhs, or with both.

So, one change that happened in amendment is earlier it was, I think, what we saw earlier, it said two years and two lakhs, I think, the fine was. Now they made it three years and five lakhs and while reading if you look at it this is again very, very legalish in that sense, it is hard to actually understand some of these things directly. You definitely need an expert in terms of interpreting all of this, but the crux of it is anybody who has access to information and unlawfully makes it available for others can be punished, section 72a.

So, that is what, the general things that you want to remember is what got updated, section 72a, is one of the parts for privacy which got amended, meaning there are many other amendments that happen in this amendment document, but this is the reference to privacy for us. Please again as I said these documents are so heavy and if, also this is a privacy one-on-one class, therefore, if you are interested in legal side, feel free to read the documents, come back, we can discuss it, more detail also.

We should also remember some of the definitions, some of the definitions. We just saw one definition, one word here, intermediary. So, I think if you think about data itself, data is a processor, it is a company which gets access to our data and then does something with the data, makes inferences and does business around, it is processor. So, there are many, intermediary could be somebody who has access to this information, they are not the user, they are not the final processor also, intermediary could be some company again having access to the information.