UNIT 4 PRIVACY RELATED WRONGS AND REMEDIES THEREOF

Structure

4.1 INTRODUCTION

There are a number of issues related to privacy related crimes. From a purely academic point of view one of the most important problems is that of classification —when it is privacy related crime and when it is a wrong? This difference is important because it determines which jurisdiction will be applied to the transgression. For cyber crimes, the jurisdiction of criminal court will be attracted while cyber wrongs are civil wrongs and therefore only civil court remedies will be attracted. Since it is relatively new field there are a number of problems with such a classification. For example, in case of fraud, existing legislation generally seems to be a powerful enough instrument under which to prosecute. However problems do arise when trying to apply traditional criminal concepts to acts involving intangible information.[1] This is because of the simple reason that information is not per se not property; thus when a machine has been deceived to obtain property then it is theft, but when a machine has been deceived to obtain a service then it is not a theft[2]. At this point it would do well to note the general computer crimes of fraud, criminal damage, obscenity, forgery, unauthorized access, unauthorized modification of the contents of the computer, etc. are all bogged down by issues of forensics, evidence and the basics of criminal prosecution like burden of proof. A very viable alternative will be the usage of tortious remedies.

Whenever tortious remedies are used then they can be no longer be called crimes instead they will have to go by the nomenclature of 'wrongs'. In this unit we will basically look at privacy related cyber wrongs. Tortious remedies are in any case can be considered more appropriate for most privacy related issues. Defamation, for example, is punished by awarding of damages. There are certain basic ways in which common law remedies are available for the enforcement of privacy rights. One of the ways offered is that statutes may impose a duty to exercise care for the protection of data from intruders in certain express terms given in the legislation. Such a standard of care may also be interpreted by the courts in a tortious action, especially when the statute is silent as regards to the civil liability.[3]

The right of privacy is the government's tortious remedy that attempts to balance two opposing interests, of which one is that all individuals have parts of their lives which should be rightfully be allowed to be kept free from public view; and on the other side there is the issue of significant public value which is there in the dissemination of information and the right to free speech. The contours of existing privacy law are efforts by courts and the society to define the proper balance between right to be free from intrusion into private space of an individual and the right of society to obtain information about issues of public concern.

The common law sources in this regard are basically related to two questions — whether a tort duty to safeguard the security of computerised personal data exists and how ordinary tort principles and fiduciary-duty law can be applied to this purpose.[4]

At this juncture it would be fine to remember that when *Warren* and *Brandeis* were publishing their landmark article which basically established the right of personal privacy as an independent cause of action in tort, they were reacting to new technology, mainly mechanical devices which enabled a number of actors, like the press to overstep in every direction the obvious bounds of propriety and of decency. Presently when we try to conceptualize action against tort wrongs as regards privacy over the Internet and cyberspace, it seems that the very same concerns have raised their heads again, even in a different space and time.

However in India, the constitutional remedies available become more important if anything for the simple reason, that the enforcement is very simple due the convenience of writs. The Supreme Court has in the past read the Right to Privacy in the Right to Life (this has been discussed elsewhere in other Blocks) and that means there exists a constitutional right, and thus one can immediately approach the High Courts in this regard. On the other hand, if one wants to use law of torts then he will have to go the lower civil courts. The enactment of the Information Technology Act (IT Act) has resolved things to a certain extent so that some of the tortious remedies have been incorporated into the provisions of the Act. These provisions are really important for the reason that the courts in India are generally wary of awarding high damages in tort cases. The Section 43 of the IT Act on the other hand allows for the highest amount of compensation that is available in law in India and the buzz is that this amount might be raised even further by the legislators while amending the IT Act.

4.2 OBJECTIVES

After studying this unit, you should be able to:

- differentiate between a privacy related crime and a privacy related wrong;
- define the various kinds of privacy related wrongs; and
- suggest the legal remedies for such privacy related wrongs.

4.3 WHAT ARE PRIVACY RELATED WRONGS?

William Prosser had reviewed the court decisions on privacy cases after the Warren-Brandeis article on privacy and he had opined that the classes of tort actions in relation to privacy matters could be broadly be classified into four heads which are all regarded as different torts. These are –

1. Intrusion upon the plaintiff's seclusion or solitude, or into his private affairs.
2. Public disclosure of embarrassing private facts about the plaintiff.

3. Publicity which places the plaintiff in a false light in the public eye.
4. Commercial appropriation of the plaintiff's likeness or name.

A brief study on the application of these torts as applicable in cyberspace is detailed as below:

- ***Tort of Intrusion***

This tort might happen whenever an individual intentionally pries or intrudes upon another individual's private affairs or seclusion in a manner which would strike a reasonable person to be objectionable in case they were the individuals whose affairs were the ones being intruded upon. The initial act of intrusion is itself the cause of tort, not what the person later on does with the information so obtained. Thus in cases of photography/ videotaping there is very little chance of proving that there is an intrusion but in case of the Internet, the scope is very widespread. This is because the intrusion must be into a private place or matter as to which a person would have a reasonable expectation of privacy. Thus this tort consists of three factors—

(i) There was intent to intrude or knowledge that the intrusion would be wrong.

(ii) There was a reasonable expectation of privacy, and

(iii) Intrusion was substantial and highly offensive to a reasonable person.[5]

With regard to online privacy one finds that there are no strict prohibitions imposed for using the personal data voluntarily disclosed in an e-mail and other cyberspace communications. As the channels which are used by ISPs to provide channels of communication might get tapped, there can be no expectation of privacy in the online information that the individual volunteers or allows to be accessed unless the individual is personally using some secure electronic medium.

- ***Public Disclosure of Private Facts***

Whenever there is a public disclosure by an individual of private information about another individual which would generally be considered objectionable by a reasonable individual of ordinary sensibilities and information so revealed was not a matter of public concern can be categorised as a tort in this context. The public disclosure of private facts requires that the facts must be private and that the communication must be to a significant portion of the community. Thus facts which were already in public domain or parted with voluntarily or where consent was obtained will not be attracted by this tort.

- ***False Light Publicity***

Whenever an individual publishes facts about another such that the other individual is represented falsely in the public domain and such that if the individual who is represented thus were to be a reasonable individual then he would be offended, then this wrong is committed. However the exception to this rule laid down by the US Supreme Court is that where the published matter is in the public interest, the plaintiff cannot recover unless it is established that the defendant has acted with actual malice. This tort is generally associated with the tort of defamation and involving making false connections between an individual and immoral, illegal or embarrassing situations which might result in an injury to one's reputation.

- ***Appropriation***

The tort of appropriation occurs when a individual uses another individual's name or likeness without authorization and for the individual's own commercial or business

purposes. The appropriation right generally allows for two theories of recovery — one, in case of celebrities there is focus on a reasonable value of the usage rights and that the other individual should not profit from the unauthorized use; two, in cases of a private individual, damages will be sought on basis of the emotional harm that use of his image has caused to him.[6] This difference exists because in case of a celebrity, the subject's likeness has commercial value, whereas a private individual's does not.

These four are the major wrongs associated with privacy. Other than these there can be some other tort based actions also for the safeguarding of information. In US there has been judicial recognition of a database possessor's duty to safeguard information from intruders.

Please answer the following Self Assessment Question.

Self Assessment Question 1 *Spend 5 Min.*

(a) What are the four main privacy related wrongs?

.....

.....

.....

.....

(b) What is a specific privacy related wrong which has surfaced specifically in the cyber law context?

.....

.....

.....

.....

.....

.....

4.4 TORTIOUS REMEDIES AVAILABLE FOR PROTECTION OF PRIVACY

- ***Tort of Intrusion***

The leading case in this regard was *Katz v. United States* [389 U.S. 347 (1967)] and when the law laid down in it is used with regard to online privacy one finds that there are no strict prohibitions imposed for using the personal information we voluntarily disclose an e-mail and other cyberspace communications. Because the channels which are used by ISPs to provide channels of communication are easily tapped, there can be no expectation of privacy in the online information that the user himself volunteers or allows to be accessed unless the user is himself using some secure system. According to some the unauthorized or unjustified access by an employer of an employee's online communications result in an invasion of privacy, this tort provides probably the best remedy especially because monitoring telephone or e-mail messages without justification or consent would probably outrage the conscience of a reasonable person which is an essential ingredient of this tort. However in *Michael A. Smyth v. Pillsbury Company*

[914 F. supp. 97 (E.D. Pa. 1996)] the court held that no reasonable person would hold such monitoring of e-mail systems, to be highly offensive intrusion upon an employee's privacy considering its workplace e-mail and there are other considerations like company's own interests like inappropriate or unprofessional comments. *See* Michael L. Rustad, Sandra R. Paulsson, Monitoring Employee E-mail and Internet Usage: Avoiding the Omniscient Electronic Sweatshop: Insights from Europe, 7 U. Pa. J. Lab. & Emp. L. 829 for further reference.

- ***False Light Publicity***

It is interesting to note that this tort has not been used much for enforcing privacy rights in cyberspace even though cyber defamation is not unheard of, it is often classified as a crime rather than a wrong.

- ***Public Disclosure of Private Facts***

In the cyber context this often does not apply to information parted online as in most instances parties have to click-contract the consent to the ISPs/companies operating online. This information then remains stored in their online database and can be used for a number of purposes. See Gerald R. Ferrera et. all, *Cyber Law* (Ohio: West-Thomson learning, 2001) page 192 for further reference.

- ***Appropriation***

Now many problems arise in considering online spaces like online newsletters, websites as news disseminators (news disseminators are allowed under the First amendment, which states that "…. Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances", exception of incidental use to publicize and to make public their own communications).

In *Howard Stern v Delphi Services Corporation* [165 Misc. 2d 21, 626 N.Y.S. 2d 694 (N.Y. Sup Ct. 1995)] a very similar problem arose. Stern had announced his candidature for Governor of the State of New York, and then an ad appeared for Delphi services online bulletin board which was supposed to discuss this candidature. Stern contested that the image used for the advertisement was used without taking his permission. The court held that the online bulletin board is a news disseminator and usage of the name and photograph of Stern is permitted as it is allowed for them to inform the public of the nature of their service and therefore it will be covered by the exception of incidental use.

- ***Database Possessor's Duty of Care***

In this regard, two landmark cases offer guidance: *Palsgraf v Long Island Railroad Co.* [(162 N.E. 99 (NY 1928)] and *Kline v 1500 Massachusetts Avenue Apartment Corp* [439 F.2d 477 (D.C. Cir. 1970)]. These cases are the pillars of American tort law and set down the basic rule of duty— The risk reasonably to be perceived defines the duty to be obeyed and risk imports in relation associated thereon it is risk to another or to others within the range of apprehension. The question is whether, from the standpoint of database possessors, there is a 'risk reasonably to be perceived' to data subjects if data is not protected from unauthorized intrusion. In most situations (where hackers can access data via the Internet), the answer is yes. The risk is entirely foreseeable and a threat to the interests of data subjects is 'within the range of apprehension'.

Therefore the first impression at least seems to state that the basic rule in *Palsgraf* suggests that database possessors should often have a duty to exercise reasonable care to protect data from intruders. In *Palsgraf* there was no threat of criminal intimidation. This situation is covered by court's decision in *Kline* where the landlord was supposed to take precautions and cautions which are available to him in order to take care of the common areas in a property when there was generally a threat of usage of criminal force in those areas.

The subjects whose personal information has been collected are in no position to put protective mechanisms in place to protect the information that has been collected from them earlier. In fact the possessor of data is the only one in the situation who can adopt certain safeguards against the risk that the intruders may cause harm, which puts him in the position of Kline's landlord. Like the landlord he can charge for the information from the subjects whose information he is trying to protect. Here the catch is the relationship which the plaintiff and the defendant share. This is because of the fact that duty often depends upon more than foresee ability of harm and opportunity to take precautions—it depends sometimes on a special linkage between the party who owes the duty and the one who receives its benefit. For liability on basis of a charge of negligence, there should be a relationship which in law leads to a responsibility upon the parties. Thus such a duty of care as regards data seems to be very high in cases in which both parties are in business with each other. So how does this principle fare in cases in which the privacy of personal information is the main issue not business secrets.

In the absence of a business relationship, in most situations WHERE a person gets access to personal information there is a voluntary assumption of duty by the possessor of such information. For example, in most cases of financial service providers, like banks, there is a privacy policy which clearly states that such information will be carefully used and protected and never be used for any purposes than that it was supplied for in the first instance. The same logic applies for almost all websites which collect information. All such practices give rise to a reasonable duty of care to be exercised and in case this duty is not exercised it shall be treated as a wrong against the person and shall be actionable in law.

In negligence cases whenever an undertaking has been given, the economic losses will not be compensated according to the Restatement of Torts in the US [Restatement (Second) of Torts 652A-E (1997)], rather only the losses on the basis of personal injury or injury to property resulting from the lack of care being exercised shall be covered. Thus the economic losses from the identity theft cannot be recovered. The principle of law in this regard is robbed of most of its sting, but then this always has been a limitation of tort law or law based on wrongs committed. This is the borderline of tort and contract law; the economic loss rule ensures that a limit is placed on claims especially in a case in which the wrong committed could have had affected a potentially economically beneficial contract or similar business. For further details, please refer to Vincent R. Johnson, Cyber security, Identity Theft, and the Limits of Tort Liability, 57 S.C. L. Rev. 255.

"Hackers and other data intruders are subject to criminal and civil liability. Victims may sue, sometimes successfully, under a variety of tort theories, including conversion, trespass to chattels, and intrusion upon private affairs, as well as under the civil liability provisions of the federal Computer Fraud and Abuse Act."[7] The law of tort wrongs is the basic law and the fact that it can be metamorphosed to deal with new technologies is a testament to its potency. In fact newer torts are being proposed to deal with new

cyberspace issues. For example, a new tort of negligent enablement which will hold software vendors accountable for defective products and services that pave the way for third party *cyber criminals* who exploit known vulnerabilities is being proposed[8]. In Patrick v Union State Bank, 681 So. 2d 1364, 1371-72 (Ala. 1996) a variation of the negligent enablement was defined as "negligent enablement of imposter fraud is a narrowly framed cause of action that applies when the victim's identity theft losses result from a financial institution's negligence in assisting or furthering an identity thief's efforts at stealing the victim's identity" (The Negligent Enablement of Imposter Fraud: A Common-Sense Common Law Claim by Heather M. Howard). This tort would help in providing relief for credit card frauds etc which have become a recurrent nuisance and cause of great loss both to the individuals and financial organizations. This continual evolvement makes this law very useful in redressing many of the wrongs which may be committed in cyberspace especially with respect to privacy as privacy traditionally has been a sphere where tort law has provided efficacious remedies.

Please answer the following Self Assessment Question.

Self Assessment Question 2 *Spend 4 Min.*

Which privacy related wrongs have been examined and adjudicated upon in a court of law?

.....

.....

.....

.....

.....

.....

.....

4.5 IT ACT AND DAMAGES AVAILABLE UNDER IT

Section 43 of the IT Act states that anyone who accesses the computer, computer system or computer network without permission of its owner or the person/entity in charge and copies, deletes, downloads, damages, disrupts data or computer system or network, then the actual damage caused to the victim would be immense and therefore this provision tries to provide for monetary relief for such aggrieved parties.

Like other torts, some of the actions that are provided in the section also have criminal liability attached to them. There are eight different conditions in which this section might get attracted and the most important issue is that in all the situations, the person must have committed the action without the permission of the owner of the computer system or network. However, one disadvantage of using this provision is that it is mostly related to offences which are similar to hacking i.e. unauthorized intrusions into a computer system. On the other hand the other provisions in the same act deal with a number of fraudulent transactions and they have severe fines along with imprisonment provisions, but in those provisions, the affected person does not obtain any monetary relief as the fines do not provide any financial compensation and therefore this Section becomes important for proving a civil remedy for wrongs committed under the IT Act.

Please answer the following Self Assessment Question.

Self Assessment Question 3 *Spend 3 Min.*

What are the damages available for the privacy related wrongs in India?

.....

.....

.....

.....

.....

.....

Let us now summarize the points covered in this unit.

4.6 SUMMARY

- There are a number of issues related to privacy related crimes. From a purely academic point of view one of the most important problems is that of classification —when is it a privacy related crime and when is it a wrong?
- For cyber crimes, the jurisdiction of criminal court will be attracted while cyber wrongs are civil wrongs and therefore only civil court remedies will be attracted. Since it is relatively new field there are a number of problems with such a classification.
- There are certain basic ways in which common law remedies are available for the enforcement of privacy rights. One of the ways offered is that statutes may impose a duty to exercise care for the protection of data from intruders in certain express terms given in the legislation.
- Classes of tort actions in relation to privacy matters can be broadly be classified into four heads:
  - Tort of Intrusion
  - Public Disclosure of Private Facts
  - False Light Publicity
  - Appropriation
- Tort of Intrusion: No strict prohibitions imposed for using the personal information we voluntarily disclose in an e-mail and other cyberspace communications. This tort provides probably the best remedy especially because monitoring telephone or e-mail messages without justification or consent would probably outrage the conscience of a reasonable person which is an essential ingredient of this tort.
- False Light Publicity: This tort has not been used much for enforcing privacy rights in cyberspace even though cyber defamation is not unheard of, it is often classified as a crime rather than a wrong.
- Public Disclosure of Private Facts: It does not apply to information parted online as in most instances parties have to click-contract the consent to the ISPs/companies operating online. This information then remains stored in their online databases and can be used for a number of purposes.

- Appropriation: Many problems arise while considering online spaces like online newsletters, websites as news disseminators. In *Howard Stern v Delphi Services Corporation*, the court held that the online bulletin board is a news disseminator and usage of the name and photograph of Stern is permitted as it is allowed for them to inform the public of the nature of their service and therefore it will be covered by the exception of incidental use.
- Database Possessor's Duty of Care: Palsgraf v Long Island Railroad Co. and Kline v. 1500 Massachusetts Avenue Apartment Corp are the cases which are the pillars of American tort law and set down the basic rule of duty.
- In negligence cases whenever an undertaking has been given, the economic losses will not be compensated according to the Restatement of Torts in the US.

4.7 TERMINAL QUESTIONS

1. What is the difference between a wrong and a crime?
2. What are the tort remedies available for protection of privacy?
3. Can tort law be used to ensure protection of information that has been stored in databases? (Especially when consent has been given when information was acquired.)
4. How far does the IT act provide viable civil remedy for privacy related wrongs?

4.8 ANSWERS AND HINTS

Self Assessment Questions

1. (a) Four main privacy related wrongs are:
   (a) Tort of Intrusion
   (b) Public Disclosure of Private Facts
   (c) False Light Publicity
   (d) Appropriation
   (b) Database possessor's duty of care is a specific privacy related wrong which has surfaced specifically in the cyber law context.
2. Tort of intrusion and appropriation
3. Under section 43 of the IT Act, the monetary relief is provided to the aggrieved party. However, as is the case with the other torts, some of the actions provided under this section also attract criminal liability.

Terminal Questions

1. Refer to section 4.1 of the unit.
2. Refer to section 4.4 of the unit.
3. Refer to section 4.4 of the unit.
4. Refer to section 4.5 of the unit.

4.9 REFERENCES AND SUGGESTED READINGS

1. Chris Reed, John Angel. Computer Law. New Delhi: Universal Law Publishing, 2002: 279.

2. Ibid.

3. Vincent R. Johnson. "Cyber Security, Identity Theft, and the Limits of Tort Liability". S.C.L. Rev 57: 255.

4. Ibid.

5. William L. Prosser. "Privacy". Cal. L. Rev 48 (1960): 393.

6. Joseph Siprut. "Privacy through Anonymity: An Economic Argument for Expanding the Right of Privacy in Public Places". Pepp. L. Rev 33 : 311.

7. Supra n 3.

8. Michael L. Rustad, Thomas H. Koenig. "The Tort of Negligent Enablement of Cybercrime". Berkeley Tech. L.J 20:1553.