

UNIT 3

Privacy and Freedom of Expression

(10 Hours) — Cyber Law & Professional Ethics (CACS401)

Please read: These notes are prepared as a study aid and **may contain errors** or out-of-date details, especially section numbers, penalties, dates, case names and statistics. Always cross-check with your prescribed textbook, class lectures, and the official text of any law (Nepal Law Commission website) before relying on them in an exam or in practice.

Syllabus note: "First Amendment Rights" refers to the US Constitution. These notes explain it as a reference model and then relate it to Nepal's own constitutional provisions. Case names and years are given from memory of standard textbooks; verify before citing.

3.1 Privacy Protection and the Law

Information Privacy

Privacy is the right to be left alone and to control one's personal life. The idea was famously described by Warren and Brandeis in 1890 as "the right to be let alone". **Information privacy** is the right to control what personal data is collected about you, how it is used, and who it is shared with. Personal data includes name, address, citizenship or national ID number, phone, email, IP address, location, health and financial records, and browsing history.

Why privacy is at risk today: cheap storage, constant online tracking, data brokers, social media over-sharing, data breaches and government surveillance.

Fair Information Practices (OECD Principles, 1980)

Principle	Meaning
Collection limitation	Collect only necessary data, lawfully and with knowledge or consent.
Data quality	Data must be relevant, accurate and up to date.
Purpose specification	State the purpose of collection at or before the time of collection.
Use limitation	Do not use or disclose data for other purposes without consent or legal authority.
Security safeguards	Protect data against loss, unauthorised access, destruction and modification.
Openness	Be transparent about policies and practices.
Individual participation	People can access and correct their own data.

Principle	Meaning
Accountability	The organisation is responsible for complying with these principles.

Privacy Laws

United States has a sector-based approach with no single general privacy law:

Law	Purpose
Fourth Amendment	Protects against unreasonable searches and seizures by the government.
Fair Credit Reporting Act (1970)	Regulates credit reports and access to them.
Privacy Act (1974)	Limits how federal agencies use personal records.
Family Educational Rights and Privacy Act (FERPA, 1974)	Protects student education records.
Electronic Communications Privacy Act (1986)	Restricts interception and access to electronic communications.
HIPAA (1996)	Protects health information.
Children's Online Privacy Protection Act (COPPA, 1998)	Parental consent for data collection from children under 13.
Gramm-Leach-Bliley Act (1999)	Financial institutions must explain data-sharing practices.
USA PATRIOT Act (2001)	Expanded government surveillance powers after 9/11.
California Consumer Privacy Act (2018)	State law giving consumers rights to know, delete and opt out of sale of data.

European Union: the **General Data Protection Regulation (GDPR)**, applicable since 25 May 2018, gives individuals rights of access, correction, erasure ("right to be forgotten"), data portability and objection; requires a lawful basis (such as consent) for processing; requires breach notification within 72 hours; and allows fines up to 20 million euros or 4% of worldwide annual turnover, whichever is higher. It also applies to non-EU companies that handle EU residents' data.

Nepal:

- **Constitution of Nepal (2015), Article 28** makes the privacy of a person, their residence, property, documents, data, correspondence and character inviolable, except as provided by law.
- **Individual Privacy Act, 2075 (2018)** and its regulations: rules on collection, use and protection of personal information, and on privacy of communications and correspondence.

- **Right to Information Act, 2004 (2007):** balances public access to information with protection of personal information.
- **ETA 2063:** offences for unauthorised access and breach of confidentiality.
- **Muluki Criminal Code, 2074:** covers offences such as unauthorised recording and disclosure of private matters.
- Nepal still lacks a comprehensive GDPR-style data-protection law with an independent regulator (draft proposals exist; check current status).

Court Rulings (Applications)

Case	Key point
Katz v. United States (1967, US)	The Fourth Amendment protects people, not places; established the "reasonable expectation of privacy" test.
Riley v. California (2014, US)	Police generally need a warrant to search the digital contents of a mobile phone.
Carpenter v. United States (2018, US)	Access to historical cell-site location records generally requires a warrant.
Google Spain v. AEPD (2014, EU Court of Justice)	Recognised the "right to be forgotten": individuals can ask search engines to delist outdated or irrelevant results.
Schrems I (2015) and II (2020, EU Court of Justice)	Struck down the EU-US data-transfer frameworks (Safe Harbor, Privacy Shield) for inadequate protection against US surveillance.
K. S. Puttaswamy v. Union of India (2017, India)	Supreme Court of India held privacy to be a fundamental right; a persuasive precedent in South Asia.

3.2 Key Privacy and Anonymity Issues

Consumer Profiling

Consumer profiling means collecting data about people's behaviour (purchases, search queries, location, social media activity) to build detailed profiles used for targeted advertising, pricing, credit and even political messaging. Tools: **cookies** (small files stored by the browser), tracking pixels, device fingerprints, mobile app SDKs, loyalty cards and **data brokers** who sell or combine data.

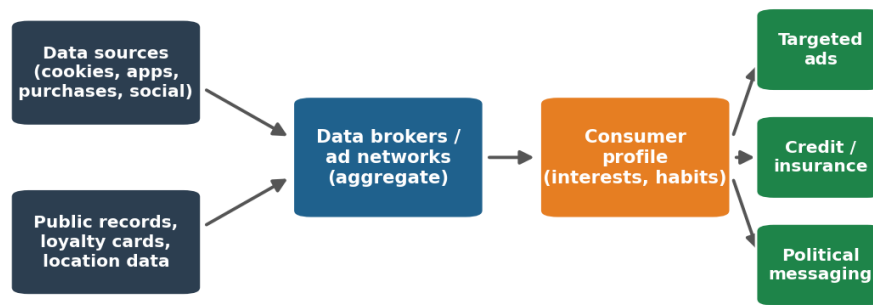


Figure 3.1: How consumer profiles are built and used

- **Opt-in:** data is collected only after the person agrees. **Opt-out:** data is collected unless the person objects. Privacy advocates prefer opt-in.
- **Benefits:** relevant ads, personalised services, free apps. **Risks:** loss of control, discrimination, manipulation, data breaches.
- **Good practice:** clear privacy policies, consent management, data minimisation, ability to delete data.

Electronic Discovery (E-Discovery)

Electronic discovery is the process of collecting, preserving and producing **electronically stored information (ESI)**, such as emails, chats, files, databases and backups, as evidence in a lawsuit or investigation. Issues: enormous data volume and cost; the duty to issue a **litigation hold** (stop deleting relevant data when a lawsuit is likely); privacy of personal data mixed in; and the need for an organisation-wide **document retention policy**. Destroying ESI after a dispute is foreseeable can lead to penalties.

Workplace Monitoring

Employers monitor email, web use, phone calls, keystrokes, CCTV and GPS location to improve security and productivity, prevent leaks and harassment, and limit legal liability. Employees expect privacy. Balanced approach:

- Publish a clear monitoring policy and get employee acknowledgement (transparency).
- Monitor only what is necessary and proportionate; avoid private spaces such as restrooms.
- Protect the collected data and limit who can see it.
- Remember that company-owned equipment usually carries a lower expectation of privacy than personal devices.

Surveillance

Surveillance is systematic monitoring of people or places, by governments (CCTV, facial recognition, interception of communications) or companies. It can prevent crime and terrorism but may chill free speech and be abused. Examples: the 2013 Snowden disclosures about mass surveillance by the US NSA, and spyware such as Pegasus reportedly used to target journalists and activists. Democratic safeguards include legal authorisation (warrants), proportionality, oversight and transparency.

Anonymity

Anonymity means acting without revealing one's identity. Tools: anonymous remailers, VPNs, Tor, pseudonyms. Supporters: protects whistle-blowers, journalists' sources, dissidents and abuse victims. Opponents: enables harassment, fraud, defamation, piracy and terrorism. Courts often require a plaintiff to show a real case before forcing a website to reveal an anonymous user ("John Doe" lawsuits).

Example 3.1: Workplace Monitoring Dilemma

A company installs software that records screenshots of employees' screens every five minutes without telling them. Employees are also using company laptops for banking. Is this acceptable?

Solution

Monitoring for security is legitimate, but **secret**, constant recording is disproportionate and violates transparency and fair information principles; it may also breach privacy laws (e.g., Article 28 of the Constitution of Nepal and the Privacy Act). The company should adopt a written policy, tell employees, limit monitoring to work-related activity, and secure the data. Employees should avoid sensitive personal activity on company devices.

3.3 Freedom of Expression

First Amendment Rights (United States)

The First Amendment of the US Constitution prohibits Congress from making laws that abridge freedom of speech, of the press, of religion, of peaceful assembly and the right to petition the government. It protects even unpopular opinions, but it is **not absolute**. Generally **not protected**: obscenity, child pornography, defamation (false statements harming reputation), incitement to imminent lawless action, true threats, and fighting words. Also, the amendment restricts the **government**, not private companies. A social network can lawfully remove posts under its own rules.

Freedom of Expression in Nepal and International Law

- **Constitution of Nepal (2015), Article 17:** guarantees freedom of opinion and expression, but allows reasonable restrictions by law in areas such as the sovereignty and integrity of Nepal, harmonious relations among communities, decency, morality, defamation, contempt of court and incitement to an offence. **Article 19** protects the right to communication (no censorship of publications or broadcasts).
- **UDHR Article 19** and **ICCPR Article 19:** everyone has the right to seek, receive and impart information, subject to necessary and proportionate restrictions.
- **ETA 2063, Section 47** and the Criminal Code's defamation provisions are the main legal limits online in Nepal.

Note: In September 2025 Nepal's government ordered the blocking of many social-media platforms for failing to register, and large protests followed; the order was later withdrawn. It is a widely discussed example of the tension between regulation and free expression. Read current sources for details.

Key Issues in Freedom of Expression

Issue	Explanation
Controlling access to information online	Filtering and blocking (e.g., filters in schools and libraries; the US Children's Internet Protection Act, 2000); concerns of over-blocking legitimate content.
Anonymous expression	Protects unpopular speakers but complicates accountability.
Defamation and hate speech	False statements damage reputation (libel is written, slander is spoken); hate speech incites hostility against groups. Online posts spread quickly and are hard to remove.
Obscene and illegal content	Child sexual abuse material is illegal everywhere; obscenity standards vary by culture.
Intermediary liability	In the US, Section 230 of the Communications Decency Act (1996) generally protects platforms from liability for user content; other countries impose takedown duties.
Fake news and misinformation	Difficult to regulate without restricting legitimate speech; platforms use fact-checking and moderation.
Cyberbullying and harassment	Repeated harmful online behaviour, sometimes with severe consequences for victims; often illegal.
Sexting	Sharing sexual images, especially by minors, is unsafe and may be illegal.

3.4 Social Networking Ethical Issues

A **social networking platform** (Facebook, Instagram, TikTok, X, LinkedIn, YouTube) lets users create profiles and share content and connect. Advantages include communication, business promotion, education and social movements. The ethical issues are:

- **Cyberbullying, cyberstalking and harassment** of individuals.
- **Sexual predators** and grooming of minors; exposure of children to harmful content.
- **Posting of inappropriate or private content** that can damage reputation permanently; employers and colleges often screen profiles.
- **Privacy and data misuse** by platforms and third parties (Cambridge Analytica, 2018).
- **Fake profiles, impersonation and fake reviews** (astroturfing) that mislead users.
- **Misinformation, hate speech and manipulation** of public opinion.
- **Addiction and mental health effects**, especially among teenagers.
- **Business use**: social advertising, employee posts about their employer, and social shopping raise disclosure and trust issues.

Ways to reduce harm: strong privacy settings, think before posting, report and block abusers, digital literacy education, age-appropriate design, transparent moderation and appeals, company social-media policies, and laws against harassment and impersonation.

Example 3.2: Employee Social Media Post

An employee posts a comment on a personal account calling her manager incompetent and revealing an unreleased product. Should the company discipline her?

Solution

Two separate matters: (1) criticism of a manager is opinion and may be protected in principle, but (2) revealing an **unreleased product** breaches confidentiality/trade-secret duties and likely her contract. The company should rely on a clear social-media policy, apply consistent proportionate action, and avoid punishing lawful personal opinion.

3.5 Important Short Questions (Exam Practice)

- Define information privacy. Explain the OECD fair information principles.
- Explain consumer profiling and its risks. Distinguish opt-in and opt-out.
- What is e-discovery? What is a litigation hold?
- Discuss workplace monitoring: its reasons and ethical limits.

- Explain freedom of expression under the Constitution of Nepal. What restrictions are allowed?
- Discuss ethical issues of social networking and how to address them.

Key Takeaways

- ✓ Information privacy = control over personal data; guided by fair information principles.
- ✓ US laws are sectoral; the EU GDPR is comprehensive; Nepal relies on Article 28 and the Individual Privacy Act, 2075.
- ✓ Profiling, e-discovery, workplace monitoring and surveillance all need transparency and proportionality.
- ✓ Anonymity protects the vulnerable but can shield wrongdoers.
- ✓ Freedom of expression is a key right but subject to limits (defamation, hate, obscenity, incitement).
- ✓ Nepal: Article 17 protects expression; ETA Section 47 is the most debated limit.
- ✓ Social networks create ethical issues: bullying, misinformation, privacy loss and reputation damage.

— *End of Unit 3* —