Elective Proposal

Soumya Singh Chauhan
Assistant Professor
Jindal Global Law School

Title: *Privacy, Surveillance & National Security*

Credits Type: Law
Cross-listed: No
Pre-requisites: N/A

Course Vision

The elective *Privacy, Surveillance & National Security* is designed to respond to the negotiation between individual rights and collective security in an age defined by ubiquitous data and technological governance. Privacy, once regarded primarily as an individual right to be left alone, has evolved into a multidimensional concept—spanning bodily, behavioural, communicational, decisional, and informational domains. In parallel, states have expanded their surveillance capacities, often invoking national security as justification for intrusive data collection and monitoring. These developments have profound consequences for constitutional law, democratic accountability, and the everyday exercise of liberty.

The course is premised on the recognition that privacy and surveillance are not abstract ideas but deeply embedded in India's constitutional structure and lived social realities. Beginning with the *Puttaswamy* decisions, which definitively recognized privacy as a fundamental right under Article 21, students will explore how proportionality, legitimate state interest, and reasonable restrictions shape constitutional adjudication. Against this doctrinal backdrop, the course examines statutory regimes like the Telegraph Act, the Information Technology Act, and the Digital Personal Data Protection Act, alongside contemporary case studies including Aadhaar, Pegasus spyware, and DigiYatra.

From a global perspective, the course situates Indian law within the comparative experience of other jurisdictions. The U.S. debates over the Patriot Act, FISA, and *Carpenter v. United States* illuminate the tension between surveillance and Fourth Amendment privacy. The U.K.'s Investigatory Powers Act reveals a model of legislative expansion of surveillance powers, while the EU's GDPR and AI Act illustrate strong rights-based protections with growing relevance for India's own data governance. By weaving in these comparative dimensions, the course highlights both the uniqueness of India's constitutional model and the universal dilemmas posed by surveillance in democracies.

The vision of this course extends beyond doctrinal study. It emphasizes the interdisciplinary and socio-technical dimensions of privacy, drawing on scholarship in political theory, technology studies, and sociology. Students will critically assess the political economy of datafication, where personal data is commodified, repurposed, and deployed by both corporations and states. In

particular, the course interrogates the problem of "function creep," where data collected for welfare or efficiency is repurposed for surveillance, eroding public trust and undermining democratic accountability.

Pedagogically, the course adopts a dialogic and problem-based approach. Students are not passive recipients of doctrine but active participants in discussions, simulations, and case analyses. By engaging with case studies like Aadhaar and Pegasus, they will explore not only constitutional arguments but also broader normative concerns: the chilling effect of surveillance on dissent, the discriminatory impacts of facial recognition technologies, and the limits of executive discretion in times of crisis. A moot-style exercise on privacy v. national security provides an opportunity for students to apply doctrinal tests, philosophical reasoning, and policy critique in an adversarial setting.

The course vision is also forward-looking. As India advances initiatives like Digital India and DigiYatra, and as AI surveillance technologies become embedded in policing, governance, and mobility, the need for regulatory foresight is urgent. Students will be encouraged to think beyond critique and towards governance design: what oversight structures are necessary? How should accountability be enforced? What regulatory models are normatively desirable and practically feasible?

In essence, this elective seeks to create lawyers and policy thinkers who understand that privacy is not simply about secrecy but about power: who collects, who controls, and who benefits from data. It aims to equip students with the doctrinal, analytical, and advocacy skills to navigate the future of constitutional rights in an era where surveillance is both a tool of governance and a challenge to liberty. By bridging theory, doctrine, and practice, the course aspires to prepare students to intervene meaningfully in debates that will define Indian democracy in the digital age.

Pedagogical Approach

- **Lectures:** Introduce doctrinal foundations, philosophical concepts, and statutory frameworks.
- **Seminar Discussions:** Student-led debates on comparative case law and current controversies.
- **Case Study Analysis:** Aadhaar, Pegasus, DigiYatra, Carpenter v. US, Snowden revelations.
- **Simulations:** Moot-style exercise on privacy v. national security.
- **Research & Writing:** Reflective case analysis and longer research paper assignments.

Weekly Outline (13 Weeks)

Week 1: Introduction – Privacy as a Right (Global & Indian context)

- Concept of privacy as a natural, constitutional, and human right
- Evolution of privacy globally: from *Warren & Brandeis* to the Universal Declaration of Human Rights and ICCPR
- Early Indian jurisprudence: *Kharak Singh v. State of UP* (1962), *Gobind v. State of MP* (1975)

- Comparative starting points: U.S. “penumbras of rights” vs. Indian “ordered liberty”
- Why privacy matters: dignity, autonomy, liberty

Week 2: Constitutional Foundations – Puttaswamy, proportionality, reasonable restrictions
- The nine-judge bench in *Justice K.S. Puttaswamy v. Union of India* (2017)
- Privacy as a fundamental right under Article 21 and as an emanation of multiple rights
- The proportionality test in Indian constitutional law
- Reasonable restrictions on privacy: public order, national security, morality, health
- Judicial balancing of privacy vs. state interest

Week 3: Data Processing and its Purpose – commodification and autonomy
- Data as a new resource: information capitalism and surveillance capitalism
- The political economy of data: who benefits from collection and processing?
- Autonomy, consent, and the illusion of control in digital environments
- Profiling, behavioural advertising, and predictive analytics
- Case illustrations: Cambridge Analytica, Indian voter profiling

Week 4: Data Protection Frameworks – GDPR, DPDPA, U.S. state laws
- The emergence of global privacy regimes: OECD Guidelines to GDPR
- Key GDPR principles: consent, data minimisation, portability, right to be forgotten
- India’s Digital Personal Data Protection Act, 2023 – provisions, critiques, enforcement gaps
- U.S. state-level frameworks: CCPA, CPRA, Virginia Privacy Act
- Convergence and divergence across jurisdictions

Week 5: Indian Constitutional Context – Puttaswamy I & II, statutory schemes
- *Puttaswamy I* (2017): recognition of privacy as a fundamental right
- *Puttaswamy II* (2018 – Aadhaar case): proportionality, legitimate state interest, dissenting opinions
- Statutory schemes: Aadhaar Act, IT Act 2000 & Rules, Telegraph Act
- The tension between welfare schemes and surveillance frameworks
- Doctrinal debates: proportionality vs. reasonableness

Week 6: Comparative Data Frameworks – GDPR, Data Governance Act, international influences
- The EU as a global standard-setter in privacy regulation
- Data Governance Act – access, re-use, and the role of intermediaries
- Data adequacy, cross-border transfer rules, and extraterritorial application
- Lessons for India: enforcement independence, role of regulators
- Comparative reflections: Canada (PIPEDA), Australia (Privacy Act), Brazil (LGPD)

Week 7: Repurposing of Data – “function creep” and legitimacy
- Concept of function creep: when data collected for one purpose is reused for another
- Examples: Aadhaar initially for welfare, later for KYC/financial surveillance
- Legitimate state interest vs. illegitimate expansion of state power
- Risks: erosion of trust, chilling effect, normalisation of surveillance

- Legal standards and safeguards for repurposing data

Week 8: State Surveillance in India – Telegraph Act, IT Act, institutional controls

- Types and theories of privacy
- Colonial legacies: Indian Telegraph Act, 1885
- The Information Technology Act, 2000 and its surveillance rules
- Absence of a dedicated surveillance law in India
- Role of executive authorisation and lack of judicial oversight
- Oversight mechanisms: ex-ante vs. ex-post, independent controls vs. executive control

Week 9: Case Studies – Pegasus spyware, Aadhaar database, DigiYatra

- Pegasus spyware: constitutional implications, Supreme Court's technical committee
- Aadhaar: welfare vs. surveillance, authentication and exclusion concerns
- DigiYatra: biometric governance of mobility, facial recognition challenges
- Common themes: transparency, consent, accountability, and redress mechanisms
- Implications for behavioural, decisional, and associational privacy

Week 10: National Security Doctrine – jurisprudential and policy frameworks

- National security as a ground for restricting rights
- Indian case law: *ADM Jabalpur*, *PUCL v. Union of India* (telephone tapping), preventive detention cases
- Policy frameworks: National Security Act, UAPA, Armed Forces (Special Powers) Act
- Doctrinal justifications: reason of state, compelling interest, rights of many
- The dangers of executive supremacy in national security decisions

Week 11: Comparative Perspectives – USA (FISA, Patriot Act, Carpenter), UK (Investigatory Powers Act), EU (GDPR/AI Act)

- U.S. surveillance frameworks: FISA, Patriot Act, NSA programs revealed by Snowden
- *Carpenter v. United States* (2018) and the evolution of 4th Amendment privacy
- UK: Investigatory Powers Act – "Snooper's Charter"
- EU: balancing fundamental rights with security; GDPR and AI Act implications
- Comparative synthesis: oversight, safeguards, and proportionality

Week 12: Technology & Bias – AI surveillance, facial recognition, inequality

- Algorithmic governance: predictive policing, AI in surveillance
- Bias in facial recognition technologies – race, caste, and gender
- The myth of technological neutrality in state surveillance systems
- Social implications: exclusion, discrimination, and deepening inequalities
- Policy challenges: accountability, transparency, explainability in AI systems

Week 13: Synthesis – Privacy v. National Security

<u>Intended Learning Outcomes:</u>

1. Understand and articulate theories and typologies of privacy.

2. Critically analyse constitutional and statutory frameworks governing privacy and surveillance in India.
3. Compare Indian approaches with global jurisprudence and policy frameworks.
4. Evaluate the legitimacy and proportionality of state surveillance measures.
5. Assess the socio-technical impacts of surveillance, including inequality and bias.
6. Develop advocacy skills through moot simulations and reflective writing.

Essential Readings (10):

1. *Justice K.S. Puttaswamy v. Union of India* (2017, 2018).
2. Digital Personal Data Protection Act, 2023 (India).
3. Daniel J. Solove, *Understanding Privacy* (selected chapters).
4. Pamela J. Wisniewski & Xinru Page, *Privacy Theories and Frameworks* (2022).
5. Jim E. Thatcher & Craig M. Dalton, *What Are Our Data, and What Are They Worth?* (2022).
6. Chris Jay Hoofnagle, Bart van der Sloot & Frederik Zuiderveen Borgesius, *The GDPR: What It Is and What It Means* (2019).
7. Bhavani Thuraisingham, *Data Mining, National Security, Privacy and Civil Liberties* (2022).
8. Jude Blanchette, *Ideological Security as National Security* (2020).
9. *Carpenter v. United States* (2018).
10. Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification* (2018).