

Structured Summary of Topic 4: What is the Role of Nation States on the Internet

December 10, 2025

Ankara University

Lecture Notes: Digital Governance, Privacy, and the Geopolitics of Data

1. The Geopolitics of Innovation and Regulation

The lecture begins by framing the global digital landscape through a popular adage that describes the distinct roles of major world powers: "**America innovates, China imitates, Europe regulates.**".

- **The US Model:** Driven by massive private corporations (Google, Meta, Amazon), the US ecosystem focuses on rapid innovation and market dominance. However, this has led to the creation of monopolies that are difficult to control.
- **The European Model:** Europe has positioned itself as the global regulator. Lacking the "Big Tech" giants of the US or China, the EU focuses on protecting citizen rights through legal frameworks like **GDPR (General Data Protection Regulation)**.
- **The Tension:** There is a constant conflict between governments trying to enforce laws (taxes, privacy) and tech companies finding ways to bypass them. Governments attempt to tax these corporations, but big tech often uses legal loopholes to avoid paying their fair share.

2. Antitrust and the Google Monopoly Case

A significant portion of the lecture discusses the legal battle against monopolies, specifically the recent US court ruling regarding Google.

- **The Ruling:** In September, a US court officially declared Google a **monopoly** in the search engine market. This is a historic decision, marking the first time in the digital age that an American court has explicitly labeled one of its own tech giants as a monopoly.
- **The Implication:** This challenges the assumption that digital markets are free and competitive. Google dominates 90% of the search market. While alternatives like *Perplexity AI* exist, the default behavior for billions of users is to "Google it." This dominance allows Google to set the rules of the internet economy without facing real competition.
- **Government Intervention:** The lecture argues that governments act as a necessary brake on corporate power. Without regulation (antitrust laws), companies naturally

tend toward monopoly, stifling innovation and consumer choice. Breaking up these monopolies (e.g., separating Google's search business from its other services) is a potential, though difficult, solution.

3. Data Privacy and the Cambridge Analytica Scandal

The lecture uses the **Cambridge Analytica** scandal (2016) as the primary case study for why data privacy matters.

- **The Mechanism:** Cambridge Analytica was a British consulting firm that harvested the personal data of millions of Facebook users without their consent. They used this data to build "psychographic profiles" of voters.
- **The Application:**
 - **2016 US Election:** The firm used these profiles to identify "swing voters" in key states. They then targeted these individuals with personalized political advertisements (often fake news or manipulative content) to sway their votes toward Donald Trump.
 - **Brexit:** Similar tactics were allegedly used to influence the Brexit vote in the UK.
- **The Lesson:** This proved that personal data is not just about showing better shoe advertisements; it is a political weapon. By manipulating the information flow to individuals based on their psychological vulnerabilities, data companies can alter the course of democratic elections.

4. GDPR and the Right to Privacy

In response to these threats, legal frameworks like GDPR (and its Turkish equivalent, **KVKK**) have been established.

- **Consent and Transparency:** GDPR mandates that companies must explicitly ask for consent to collect data. This is why we constantly see "cookie banners" and pop-ups asking for permission. Companies must declare *why* they are collecting data and *how* it will be used.
- **The "Invisible Hand" Failure:** The lecture notes that the free market (Adam Smith's "Invisible Hand") failed to protect privacy. Companies did not self-regulate because exploiting data was too profitable. Therefore, the "visible hand" of the government was required to impose limits.
- **The Cost of "Free":** Users must understand that "free" services are never truly free. If you are not paying for the product (Gmail, WhatsApp, Instagram), **you are the product**. Your data is the currency used to pay for the service.

5. Algorithmic Profiling and the "Target" Case

The lecture revisits the **Target pregnancy prediction** case to illustrate the power of algorithmic profiling.

- **Predictive Analytics:** Target's algorithm analyzed shopping habits (e.g., buying unscented lotion, specific vitamins) to assign a "pregnancy score" to female customers.

- **The Consequence:** The store sent coupons for baby products to a teenage girl before she had told her family she was pregnant. The algorithm inferred a private biological fact purely from commercial data points.
- **The Broader Context:** This logic applies everywhere.
 - **Spotify/Netflix:** They analyze your listening/watching history not just to recommend songs, but to keep you on the platform longer. They create a "filter bubble" where you only see what you already like, potentially narrowing your worldview.
 - **Credit Scores:** Banks use similar data to determine if you are "worthy" of a loan.
- **No Place to Hide:** The argument "I have nothing to hide" is flawed. In a digital society, you cannot live without leaving a data trail. Even if you don't post on social media, your credit card usage, location data, and network connections create a profile that can be exploited.

6. Digital Ethics: A Warning for Students

The lecture concludes with a practical warning about digital ethics and liability, specifically regarding academic integrity.

- **Sharing Exam Papers:** Sharing photos of exam papers or answers on social media (WhatsApp groups, Instagram) is a violation of intellectual property and privacy.
- **Legal Liability:** If a student shares an exam paper, they are liable. The university or the professor can take legal action. It is a reminder that the digital world is subject to real-world laws regarding copyright and privacy.
- **Final Thought:** We must be conscious "data citizens." We need to be aware of what we share, who owns it, and how it might be used against us or others in the future.