PPIT SHEET – **FINALS**

Rayyan Minhaj (20K-0143 | BCS-7F)

----------CASE STUDIES----------

FACEBOOK – CAN ETHICS SCALE IN DIGITAL AGE?

Facebook valued at $750bn in 2021 faced success AND increasing scrutiny. With over 2.8bn users, 7mil advertisers and significant volumes of data, it had to deal with **data privacy, anti-trust, and content moderation issues.** The Cambridge Analytica scandal, acquisitions of potential competitors like Instagram and WhatsApp, and debates on antitrust regulations fueled criticism, raising concerns about governance, user consent, and societal impact.

THE PATH TO USER AS PRODUCT

Facebook's evolution began in 2004 as a Harvard student network, **quickly expanding with venture capitalist investments** and opening to the public in 2006. Facing **competition from Myspace and Twitter**, Facebook introduced the **News Feed** in 2005, later enhancing sharing with the **Share button**. The platform's mobile presence grew in 2007, and by 2011, it focused on smartphone users, capitalizing on addictive engagement. The Facebook Platform in 2007 allowed third-party apps, leading to a robust ecosystem. Microsoft's investment and Facebook Beacon marked strategic moves in 2007. Sheryl Sandberg joined in 2008, steering Facebook towards advertising as a revenue model. **The "Like" button in 2009 and Open Graph API in 2010 expanded user interactions and data accessibility**. Acquisitions of Instagram in 2012 and WhatsApp in 2014 strengthened Facebook's position. By 2018, **Facebook and Google formed a digital duopoly, dominating online advertising.** Facebook's financial success continued, reaching $84 billion in revenues in 2020. However, concerns persisted, with plans for **an Instagram version for children** raising ethical questions.

THE ULTIMATE SURVEILLANCE MACHINE

The misuse of Facebook data, focused on the **Cambridge Analytica scandal**. Researchers initially **used Facebook data for personality prediction**, but later, GSR and Cambridge Analytica **exploited** the platform **to collect and sell data from 87 million users for political advertising**. The revelation led to public outrage, a #DeleteFacebook movement, and scrutiny from industry leaders. **The incident prompted Facebook to implement a six-point plan to enhance data protection**, including reviewing the platform and turning off access for unused apps. The company **also faced criticism for granting device manufacturers, including Chinese firms, access to user data**. In response, Facebook released a **privacy-focused plan in 2019**, aiming to integrate and encrypt communications across its platforms.

PLATFORMS & ANTI-TRUST

The concerns about the **digital duopoly of Facebook and Google**, suggested that they should be **split up or restricted from acquiring potential competitors**. Facebook's **acquisition strategy**, including **copying features from emerging apps and acquiring companies like Instagram and WhatsApp**, has raised **antitrust concerns**. Analysts question whether the U.S. government missed an opportunity to review the Instagram acquisition more closely. In 2019, legal scholar Lina Khan argued that **Facebook, despite offering free services, constituted a monopoly by extracting user data**. Antitrust investigations were initiated by the Federal Trade Commission, state attorneys general, the U.S. Department of Justice, and the European Union. In 2020, a German court ruled Facebook violated antitrust laws, and in December 2020, the U.S. federal government and state attorneys general filed an antitrust lawsuit against Facebook, focusing on its acquisitions and alleged pattern of neutralizing competitors. **Facebook proposed building a potential competitor, but regulators rejected the idea.**

CONTENT MODERATION AND POLITICS: “THE IMPOSSIBLE JOB”

Facebook's struggles with content moderation, included issues like the **Russian interference** in the 2016 U.S. election where 13 military Russian officers and 3 Russian entities **purchased $46,000 worth of Facebook ads** in hopes of tampering with election campaigns and the broader challenge of **managing false campaigns and hate speech**. One study showed that **lies spread faster than the truth** on Twitter. “On average, it took true claims about six times as long as false claims to reach

1,500 people, with false political claims traveling even faster than false claims about other topics, such as science, business, and natural disasters," It mentions the emergence of startups, including **New Knowledge, addressing these concerns**. New Knowledge utilized a team of **former intelligence workers** to develop **AI software that could extract indications of manipulation within user accounts**. It could monitor how bad actors could "plant seeds" in individual accounts and paid advertisements, it could inform companies and social media platform clients that bad influencers were attempting to manipulate their customer base. Clients could then be shown how to prevent such manipulation. In 2018, **criticisms faced by Facebook**, ranging from **allegations of bias** to the **spread of hate speech and fake news**. The Court of Justice of the European Union's 2019 ruled that **Facebook must globally remove hateful content**. Facebook's **response** involves significant efforts, **including increasing content moderation staff, investing in AI, publishing transparency reports, and spending billions on platform safety**. The creation of a "Supreme Court" for content moderation was done. **Despite these measures, the persistent nature of the challenges, such as livestreaming violent acts continued (Christchurch, NZ)**. Facebook's ongoing struggles to maintain a secure online environment are still providing insights into the company's mismanagement of personal data.

POTENTIAL FORCES FOR CHANGE

The multifaceted landscape surrounding Facebook focused on the responses and considerations of both **internal and external stakeholders** in the face of significant challenges, particularly the **Cambridge Analytica scandal and escalating regulatory concerns**.

A key aspect was the ongoing debate surrounding **Facebook's business model**. **Some stakeholders propose a shift to a subscription-based approach**, aiming to align user interests more closely with the platform. However, the feasibility of such a transition raised questions, as compensating for the substantial advertising revenue (reported at $40 billion in 2017) would be essential for sustained growth.

The dissent within Facebook's ranks, featuring notable figures like Sandy Parakilas, who **expressed doubts about the company's prioritization of data collection over privacy**. Andrew Bosworth's **controversial memo emphasizing growth at all costs**, Alex Stamos's **push for greater disclosure on interference**, Elliot Schrage's **critique of underinvestment in protections**, and Chris Cox's **call for a shift in the company's approach** all underscore internal tensions.

The passage sheds light on **societal perceptions**, drawing attention to a UK survey where two-thirds of respondents **expressed concerns** about **inadequate regulation, transparency, and inappropriate user data sales by online companies**. Over half felt these companies **exploited user loneliness**, while a third **viewed social media negatively**. Calls for stronger government regulation (64%) coexist with a lack of trust in the government (36%).

Psychographic profiles and their potential invasiveness with **users feeling vulnerable** due to the **intimate nature of this data**. Concerns about **informed consent**, especially given the **complexity** of Facebook's **terms of service**, were raised. Legal actions in Germany and the passage of the GDPR in the EU further illustrate the global challenges related to privacy and data sharing.

Various regulatory approaches are explored, from **fines and the Honest Ads Act to implementing data protection legislation**. The potential adoption of GDPR-like regulations in the U.S. is considered, despite **concerns about its impact on smaller players**. The passage also introduces the idea of creating a **Digital Protection Agency** and highlights debates around antitrust issues, with suggestions to break up Facebook into multiple companies.

Investors, particularly large institutional ones like BlackRock, Vanguard, and State Street **held 20% of Facebook together**. The **Cambridge Analytica scandal** led to a **significant drop** in Facebook's market capitalization, prompting **increased scrutiny** from shareholders. Proxy advisory services consistently gave Facebook **poor marks** on governance, compensation, and shareholder rights.

The impact on advertisers and app developers emphasized the **shift away from traditional media platforms** toward digital advertising on Facebook. Brands are noted for **pressuring social media for better user protections**, although actual spending cuts post-Cambridge Analytica were limited. The digital duopoly's dominance, especially in the context of psychographic marketing, is acknowledged as a challenging dynamic for advertisers.

TIME TO HIT RESET

The aftermath of the challenges faced by Facebook, notably the Cambridge Analytica scandal led to subsequent **scrutiny from regulators and the public**. Mark Zuckerberg and Sheryl Sandberg expressed openness to regulation, and despite an initial stock gain after the Congressional testimony, Facebook **faced a significant drop in its market value** in July 2018 due to missed earnings projections, public perception issues, and stagnant user growth.

Despite the setback, Facebook's **stock price eventually recovered**, reaching an all-time high in June 2018. The company reported growth in revenue, EBITDA, and user engagement, especially with the integration of Instagram and WhatsApp. However, challenges persisted, including the announcement of the LIBRA cryptocurrency, met with withdrawal intentions from high-profile partners.

Questions about the management style of Sandberg and the turnover in her team were raised and whether Facebook's mission aligns with how social media is actually being used and if Zuckerberg and Sandberg are reevaluating priorities to restore user trust and privacy protection. The growing call for regulations globally and locally, coupled with the influx of new users and the influence on them, poses challenges and opportunities for Facebook's leadership. The passage concludes by prompting consideration of how Zuckerberg and Sandberg will navigate these complexities and what their legacy will be.

----------X----------X----------X----------
-

HOW INDIA PLANS TO PROTECT CONSUMER DATA

The Indian government wants to set a legislate called **Personal Data Protection bill (DPB)** to **control the collection, processing, storage, transfer, protection, and disclosure of personal data** of Indian residents. It will attract numerous global players who must comply with DPB. Previously, India has followed the EU bill (GDPR) to allow global companies to operate within India under certain conditions but with the **DPB, India will be able to carry additional provisions beyond the EU regulations**. India being a nation state, it treats its citizen's data as a **national asset** and hence upholds the responsibility of storing and safeguarding it within national boundaries, along with reserving the rights to use the data in its defense and strategic interests.

Some features of the DPB which will force companies to change their business models, practices, and principles in hopes **of increasing data protection regulation** include:

1. PRIVACY AS A FUNDAMENTAL RIGHT

In 2017, the Supreme Court of India recognized **privacy as a constitutional right for Indian citizens**. The DPB aims to safeguard this right by **regulating the collection, security, storage, sale, and exploitation of private data generated by citizens in the digital realm**. The proposed regulations could impact the business models of digital firms **that provide free services but rely on profits from selling and exploiting user data**. These companies may need to reassess their strategies if the new regulations make **data collection and exploitation less profitable.**

2. USER CONSENT

Under the DPB, digital companies **will require explicit user consent** before collecting data which should state why that data is being collected (**purpose**). This consent should be **asked at every stage of data processing**. The problem is that companies use user data to generate **new information from that data** for ex. Uber analyzing traffic patterns and Amazon assessing feedback. Sometimes, **raw data is sent to third-party** processors for analysis, creating new information when combined with data from other sources. This redefines digital companies as **"data fiduciaries"** under the DPB, **requiring them to take on the responsibility of obtaining user permission for both initial collection and subsequent processing of data**.

3. OWNERSHIP OF PERSONAL DATA

DBP proposes that **data provider is the owner of their personal data**. This places a burden on digital companies. In the physical world, property owners can ask to have their properties returned whereas in digital world, **companies will have to figure out how to comply with the erasure and deletion of all their personal information**. Digital companies will also have to think outside of their own ecosystem **if they have provided the data to any third party.**

4. THREE CLASSES OF DATA

The Data Protection Bill (DPB) identifies **3 classes of data** with **specific regulations** for each: **sensitive data** (involving financials, health, sexual orientation, genetics, transgender status, caste, and religious belief), **critical data** (government-deemed exceptionally important, such as military or national security data), and a **general category encompassing other data**. DPB mandates that **sensitive and critical data must be stored in India**, with **sensitive data allowed for processing abroad but requiring storage in India**. **Critical data cannot leave the country. There are no restrictions for general data**. This shift from the current global cyber environment could impose additional costs on digital companies, potentially leading to suboptimal storage and processing capacities, and contributing to the concept of a "splinternet" or the fragmentation of global digital supply chains.

4. DATA SOVEREIGNTIY

DPB reserves the right to **access locally stored data to protect national interests**. This implies that DPB would **treat citizens' data as a national asset**, **no different than control over citizens' physical properties**. In this respect, DPB differs from GDPR, which imposes no locational storage requirements or preferential access to data for protecting national interests. Currently, digital companies practically own the data if they can address the privacy concerns and meet the user-acceptance requirements. One implication of the new policy is that when the government demands its citizens' data, in case of foreign attacks and surveillance, digital companies would have to abide and assist the Indian government's defense policy.

5. NATIONAL INTERESTS

The Data Protection Bill (DPB), while prioritizing citizens' privacy, **exempts government agencies from certain provisions. DPB does not apply to government agencies processing personal data for reasons related to national security**, **detection of unlawful activity or fraud, and epidemic or medical emergencies**. This means that public sector entities can obtain personal data from individuals without their consent in these situations. Furthermore, **the government can direct digital companies to provide non-personal or anonymized data for research or planning purposes**. Critics express concerns about potential **misuse** of such data for **political surveillance,** and there are debates over the effectiveness of anonymization. Compliance with these requirements may prompt digital companies to revise their policies, **similar to past controversies such as Apple's refusal to unlock an iPhone for an FBI investigation**, raising questions about whether such refusals would be possible under DPB.

6. VERIFICATION TAG

DPB requires that all digital **companies must identify their users and tag them into three categories to reduce trolling** (e.g., an anonymous user or a bot trying to incite violence by posting incendiary comments): **Users who have verified their registration and display real names**; **users who have a verified registration but have kept their names anonymous**; **and users that have not verified registration**. This would be a first regulation of its kind in global social media. This implies that **digital companies must put in place procedures for collecting and verifying the real identities of their users**. Note that **Facebook has more that 100 million fake account**s and faces the dilemma of continuing as is, attempt to verify them, or delete those accounts.

7. COMPLIANCE AND ENFORCEMENT

DPB proposes steep **penalties for noncompliance**. In case of **a data breach or inaction** by the fiduciary upon data breach or a minor violation, the penalties could reach $ 700,000 or 2% of a company's global revenues, whichever is higher. For **major violations, such as data shared without consent**, the penalties would double. These penalties, which are based on multinationals' global income, and potential **jail sentences for officers of digital companies**, imply that DPB regulations cannot be taken lightly. Its provisions must be complied with in order to do business in India.

8. TAXING DIGITAL COMPANIES

As we note in a previous article, multinational digital companies can easily transfer their income to tax havens and avoid paying taxes to local governments,

with no fear of confiscation of their properties. **Physical control over data and fear of enforcement penalties might give the Indian government additional leverage to collect taxes and dues from digital companies**. This would lower the likelihood that digital companies can get away with paying little or no taxes to the local governments.

9. OTHER ISSUES

The DPB applies to all businesses that collect personal data, not just digital businesses. For example, John Deere collects and processes data obtained from its farm equipment. Whether DPB applies to tractors with sensors, whether the collected data belongs to the farmers, and how the benefits of farm data are shared becomes a debatable point.

----------X----------X----------X----------

DOLCE & GABBANA: RACISM, STEREOTYPE, OR BEING FUNNY

In 2018, D&G came under heavy scrutiny and boycott after some controversial advertisement videos and racist personal messages by Stefano Gabbana himself went viral.

THE CONTROVERSIAL VIDEOS

Dolce & Gabbana (D&G) faced controversy **over three 40-second videos** promoting "The Great Show" as a tribute to China. The videos, **depicting an Asian model struggling to eat Italian food with chopsticks, were perceived as patronizing and racist**. Social media outrage ensued, with some considering the videos **intentionally provocative for profit**. D&G's official apology and removal of the videos did not quell the controversy. Stefano Gabbana's Instagram response, alleging **hacking**, **added to the backlash** as he appeared to make **derogatory remarks about China**. D&G's claims of hacking were met with **skepticism**, with many finding their apologies insincere, suggesting a **pattern of making offensive remarks and issuing inadequate apologies.**

COMPANY BACKGROUND

Dolce & Gabbana (D&G), established in 1985, had gained international prominence as a **luxury fashion house** producing high-end clothing, accessories, and beauty products. Owned by the D&G Group, the company was divided into **three divisions**: production, distribution, and licenses. Founders **Domenico Dolce** and **Stefano Gabbana** played key roles in the brand's creative direction and global strategies. The duo, with roots in small clothing businesses, founded D&G after a successful runway debut in 1985. Over the years, the company expanded its product lines, collaborated with the Onward Kashiyama Group for distribution in Japan, and launched fragrances, eyewear, and children's collections. D&G's success was fueled by its use of Italian cultural elements, and Madonna's friendship notably contributed to its international fame. As of 2018, the brand continued its global expansion, opening a flagship store in Miami.

CONTROVERSIAL MARKETING STRATEGIES

Dolce & Gabbana (D&G) has a history of **controversial marketing strategies**, often involving **negative advertising and offensive campaigns**. The brand, **not constrained by the need to appease investors, retains direct control** and has been criticized for making politically incorrect statements. D&G's wealthy clientele, perceived as distant from everyday citizens, may contribute to its perceived insensitivity. The brand has **faced backlash for incidents** such as labeling a shoe as a "slave sandal" in 2016 and portraying poor working-class citizens as "normal" in a 2017 Beijing campaign. Despite canceling "The Great Show" in 2018 amid **accusations of racism**, D&G's controversies have sparked discussions about racism and cultural sensitivity in the fashion industry. Some argue that the issue is rooted in a "cult of personality" within the fashion power structure, where celebrity designers with massive followings contribute to the industry's controversies and are amplified by social media.

BOYCOTT FROM CHINESE CUSTOMERS

D&G faced a **significant boycott** from Chinese customers after the controversial videos. Chinese-French model Estelle Chen **withdrew from D&G's planned show in Shanghai**, denouncing the brand's actions **as racist and accusing the designers of**

prioritizing money over China. Other **brand ambassadors, models, and agency** China Bentley announced their boycott, with some even **burning D&G products in protest**. The backlash extended beyond individuals, with major Chinese e-commerce platforms, including Alibaba's Taobao and JD.com, **ceasing to carry D&G products**. Smaller platforms in China and even global platforms like Yoox Net-A-Porter Group joined the boycott. The criticism also affected D&G in European and North American markets, with **consumers denouncing the brand on social media** and **returning items to department stores**. The **model** in the ads **faced personal backlash**, with accusations of makeup manipulation and derogatory comments about her appearance.

FINANCIAL COSTS

The controversy surrounding D&G is expected to have **significant financial repercussions**. D&G stores in Shanghai were **vandalized**, and considering China's enormous consumer base, the **backlash from millions could have substantial consequences**. Chinese consumers accounted for nearly **one-third of global luxury goods spending** in 2017, representing a substantial portion of D&G's estimated **profits** of €1.3 billion in 2018, with **30% attributed to China**. Women's Wear Daily estimated **potential losses for D&G at €400 million**, excluding additional impacts from canceling the show and potential Western consumer boycotts. Brand Finance **estimated that 20% of D&G's brand value could be eroded**. As Chinese consumers played a significant role in luxury spending, D&G's setback contrasted with other brands actively courting the Chinese market with culturally sensitive approaches. The controversy was viewed as a **crisis**, and experts emphasized the need for global brands to be attuned to local sensitivities for successful recovery.

CONCLUSION

In conclusion, there had been **no significant change in Dolce & Gabbana's (D&G) behavior or marketing following the cancellation of the Shanghai show**. The brand's response included **a video apology** and **messages on social media platforms**, **attributing inflammatory messages and videos to supposed hacks**. Despite these efforts, the **damage** to D&G's reputation was **substantial**, especially given **the size and importance of the Chinese luxury market**, which experts predicted could significantly impact the brand's profits. The question remained about what mitigation strategies or actions D&G could undertake to repair the harm caused to its reputation.

----------X----------X----------X----------
-

CAN FACEBOOK EVER BE FIXED?

Facebook, notorious for **privacy scandals and data leaks**, faces criticism as CEO Mark Zuckerberg proposes **four new ideas to regulate the internet**. Despite the company's history of privacy shortcomings, Zuckerberg's **proposals are deemed superficial in comparison to the scale of the problems Facebook confronts**. The **consistent pattern of privacy issues contrasts with the company's public assertions that it is committed to making amends**, prompting scrutiny of Zuckerberg's latest attempt at change. The article questions the **sincerity** and **effectiveness** of the **proposed solutions** in addressing Facebook's persistent challenges in **data collection**, **storage**, and **analysis**.

Mark Zuckerberg's **four proposals** for regulating the internet include.

- a call for governments to **define harmful content** online.
- expanding **laws on political advertising** beyond elections.
- **standardizing global privacy regulations** like the General Data Protection Regulation (GDPR).
- **advocating for data portability** to enable users to **move their data between services** easily.

However, critics argue that many of **these proposals are already in practice or are being mandated by regulators worldwide**. For instance, GDPR already requires data portability in the EU, and major regulations in countries like Germany, China, and Australia are addressing harmful content. Zuckerberg's proposals may **lack a sense of sacrifice or genuine atonement for past data-related mistakes** and could **potentially benefit Facebook in the long run.**

Three major predicaments stemming from **Facebook's interests** that **diverge** from its **users' interests**.

- First, Facebook's business model relies on **user engagement and monetizing gathered data through targeted advertising**. Users often don't fully grasp the scale of data they provide, while Facebook promotes a sense of social connection and community.
- Second, Facebook's **immense scale**, with 2.32bn monthly users and a very small employee count (1 employee for 65,000 users), makes **effective governance and protection challenging**, leading to inevitable **failures** in areas like **cybersecurity and privacy.**
- Lastly, a **cultural problem within Facebook**, marked by **consistent privacy missteps**, suggests a **lack of prioritization for user security and privacy.** Unforced errors erode user trust, hindering the company's ability to address its core issues.

Its globally acknowledged that **Facebook is not solely responsible for the current digital discomfort**, as many tech **giants face similar issues**. It highlights how the adoption of digital technologies happened quickly without a full understanding of their downsides and risks.

The **suggested solutions involve crafting new legislation to enhance privacy and security standards for all software systems, slowing down the adoption of digital technology**. Limiting the power of companies like Facebook by **restricting data collection** and **service aggregation** is proposed, possibly involving the physical separation of different services. The long-term evolution of **Facebook's business model should prioritize trust** by making user privacy and data security as **crucial as monetization.**

However, in the short term, **Facebook is distant from achieving these goals**. Despite appeals to governments, the company is **yet to fully grasp the depth of the problems**. The ongoing struggle between Facebook and its users to **redefine their relationship may persist until governments intervene more forcefully**. Zuckerberg's **recent proposals are seen as another episode in this prolonged struggle** for reframing the user-company bargain.

----------X----------X----------X----------