**A1: ESG Paper: Who, if anybody, should have access to your stored communications?**

**Summary:**   
This paper explores the importance of digital accountability and the evolving tension between privacy and law enforcement needs. Part A reflects on how past social media activity can impact personal and professional credibility, prompting actions to align digital presence with current values. Part B examines the Adrian Pina homicide case, highlighting the need to balance privacy rights with access to critical evidence through a case-by-case judicial oversight model, ensuring trust, safety, and fairness for all stakeholders.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Part A**

**The Online Accountability**

The digital advancement in today’s world especially in social media shapes an image on one’s personal and public narratives. From breaking news to following viral trends the content we post, or share can have a huge impact. For instance, **Justine Sacco**, a PR executive, lost her job after a tweet intended as a joke was declared offensive, leading to a global backlash (Wagner, 2018). This highlights the need to be mindful of our online presence, as even well-intentional or natural posts could be mistaken out of context, potentially damaging your image and reputation in personal and professional space.

**Platform 1: Facebook**

Facebook is a casual space to share interests and opinions. Reflecting on my older posts, I found one from 2021 about politics, shared around the election period. It humorously criticized election promises as a “Monthly Report Card,” suggesting leaders rarely deliver. At the time, it seemed harmless and funny. However, now I see it could be perceived as insensitive or offensive, especially since the ruling party was performing well. As societal norms and political views have shifted, sharing such content today could be inappropriate for someone outside politics or without influence *(refer to the appendix for the screenshot of the post).*

**Why This Could Be a Problem:** The post about politics is highly subjective and can evolve. It might be sensitive to people who support a particular party and can become offensive, especially when it influences the real lives of the people. Political humour can undermine the government’s reforms, sanctions, and schemes as it is a serious topic. Sharing these without the context, particularly from a personal account, risks being mistaken or misinterpreted.

**Action Taken:** To avoid leaving a bad or negative impression on my audience or anyone in general, I decided to delete the shared post. Through this action, I believe I’m reducing the risk of the content resurfacing in a way that could harm me. This action also helps me maintain a more casual and neutral online presence.

**Platform 2: Instagram**  
On Instagram, users engage with trends, hashtags, and challenges, pushing them out of their comfort zones. A few years ago, I joined an “ugly filter” challenge, posting an unflattering photo for fun. It seemed funny then, but now I find it embarrassing and unprofessional. Such posts are termed “cringe” today, exposing me to judgments in a professional setting *(refer to the appendix for the screenshot of the post)*.

**Why it could be a Problem:** The trend I followed might be harmless, but there is a high chance that my employers or colleagues will perceive me in a silly way or negative way. In a professional environment often expect a simpler online presence, a simple post can unintentionally lead me to easy judgment.

**Action:** I decided to archive the post, as it is harmless. Effectively removing it from the public view I can retain the post for my reflection. This approach ensures that I have control over my digital presence without completely deleting my past experiences.

**Part- B**

**Introduction to the Stored Communications Act (SCA)**

The real struggle between protecting privacy and granting law enforcement access to stored communications is crucial to the modern debates over digital rights. Why because the act Stored Communications Act (SCA) was originally designed to safeguard electronic communications stored by third parties. However, as we evolve in the digital advancement in technology and business practices there is a limitation to SCA in addressing criminal investigations.

**The Samuel Pina case:**

In this case, a debate on whether the Supreme Court must uphold the **Stored Communications Act (SCA)** or grant access to the tech companies to private communications. The balance is privacy with justice, as privacy laws enforcement are so different globally. To keep things fair and lawful, judges must approve warrants before law enforcement can access private messages (Wikipedia contributors, 2024). This ensures that the search is legitimate and justified. Countries like the EU enforce strict privacy laws under GDPR with national security exceptions, while the U.S. debates SCA reforms (*General Data Protection Regulation (GDPR) – Legal Text*, 2024). Other countries like China, prioritize state access, often supporting individual privacy with the **Personal Information Protection Law (PIPL)** (*China’s New Data Security and Personal Information Protection Laws: What They Mean for Multinational Companies*, 2021).

**The Adrian Pina Homicide Case:**

The Fourth District Court of Appeal in San Diego ruled that the SCA does not protect Facebook, Snapchat, and Instagram from subpoenas in a homicide case. Adrian Pina, accused of homicide, successfully argued for access to his brother's social media communications for his defense. The court found that the commercial use of user data by these platforms excluded them from SCA protections, challenging social media companies' long-standing practice of using the SCA to reject subpoenas. This case highlights the privacy vs. security debate, with individual privacy at risk when law enforcement seeks critical evidence (Kerr, 2024). **2. Further Analysis of the Arguments**

**For Law Enforcement Access:**

1. **Crucial for Crime-Solving:** In the Adrian Pina case, access to private communications was vital for uncovering the truth and ensuring a fair trial. Encrypted communications and social media privacy can be key evidence in solving crimes.
2. **Addressing the "Going Dark" Problem:** The “going dark” problem refers to cases where necessary information is inaccessible due to legal barriers like the SCA. The Adrian Pina case shows how court intervention can allow platform cooperation under specific conditions (*Social Media Outfits Must Disclose to Court Stored Data, n.d.).*
3. **Judicial Oversight Provides Safeguards:** Court-approved summons in this case required additional data access on legal grounds to ensure justice, preventing indiscriminate data access in critical cases.

**Against Law Enforcement Access:**

1. **Erosion of Privacy Rights:** Opponents argue that weakening the SCA breaks a barrier. If commercial practices disqualify SCA coverage in different platform implementations, it could broaden data access requests, undermining user privacy. Violating user trust could lead to severe consequences.
2. **Risk of Overreach and Misuse:** A global example of law enforcement misuse by broad access to user data is Uganda’s internet shutdown. Oversight expansion could lead to a surveillance state, eroding public trust in government and private parties *(AfricaNews, 2021)(refer to appendix).*
3. **Damage to Tech Companies’ Trust:** User trust is crucial for social media, impacting engagement on the platform. Cases like Adrian Pina challenge this trust, causing fears about data security and potentially leading to financial and reputational damage *(Eveleth et al., 2024).*

**3. Stakeholder Analysis**

|  |  |  |  |
| --- | --- | --- | --- |
| **Stakeholder** | **Interest Level** | **Influence Level** | **Impact** |
| **Law Enforcement** | High | High | (+) Gain critical evidence for cases, (-) Risk of public backlash |
| **Tech Companies** | High | High | (+) Must adapt to legal requirements, (-) Face compliance burdens and reputational risks |
| **Citizens** | High | Medium | (+) Safer communities, (-) Privacy concerns |

*(OpenAI, 2024)*

The Adrian Pina lawsuit has a direct impact on these stakeholders, compelling platforms to choose between complying with court demands and retaining user trust. Law enforcement's ability to obtain evidence is improved, but the foreseeable implications for confidentiality and platform trust are enormous.**4. Recommendations**

**Proposed Solution:**  
To address privacy and law enforcement access, a case-by-case oversight model is proposed, based on the Adrian Pina case approach. Key aspects include:

1. **Court-Approved Warrants:** Ensure tight court monitoring for data requests, making them focused and case-related.

2. **Controlled Access Systems:** Encourage tech companies to create mechanisms for temporary access to specific data while preserving privacy.

3. **Updated SCA Guidelines:** Amend the SCA to clarify when platforms must cooperate with summons, considering their commercial use and the digital ecosystem.

This ensures data protection, legal access, and clarity in data requests.

**Global Perspective:**  
The GDPR, enacted by the European Union, provides a solid structure for balancing privacy and security concerns. GDPR stresses user consent and openness, with limited permits for national security and law enforcement under specific conditions. Implementing comparable concepts in the United States might enhance the SCA and give clarity to digital businesses and law enforcement (*General Data Protection Regulation (GDPR) – Legal Text*, 2024).

**Shortcomings:**   
1. To reduce the risk of abuse, consider implementing transparency policies, such as disclosure on summons.   
2. To eradicate uncertainty in SCA protections, modify them on a regular basis to reflect new technologies and business practices.

**Impact Analysis.**

**How the Recommendations Help Stakeholders:**

• **Law Enforcement:** Access critical evidence for serious crimes, as in the Adrian Pina case, without blanket surveillance.

• **Tech Companies:** Maintain user trust by adhering to legal obligations and limiting overreach.

• **Citizens:** Benefit from increased public safety and privacy protections through judicial oversight and transparency.

These recommendations balance justice and privacy, ensuring fairness while updating outdated privacy regulations like the SCA, building on the Adrian Pina case precedent. **Conclusion**

The Adrian Pina homicide case tests the limits of the SCA and necessitates a rethinking of how privacy and security may coexist in the digital era. By implementing a case-by-case judicial monitoring mechanism and reforming regulatory structures, we might guarantee that both privacy rights and law enforcement requirements are successfully addressed.

References:

AfricaNews. (2021, January 13). *Uganda cuts internet hours before election*. Africanews. <https://www.africanews.com/2021/01/13/uganda-cuts-internet-hours-before-election//>

*China’s new data security and personal information protection laws: What they mean for multinational companies*. (2021, November 3). Insights | Skadden, Arps, Slate, Meagher & Flom LLP. <https://www.skadden.com/insights/publications/2021/11/chinas-new-data-security-and-personal-information-protection-laws#:~:text=The%20DSL%20requires%20companies%20doing,revocation%20of%20its%20business%20licenses>.

Eveleth, D. M., Stone, R. W., & Baker-Eveleth, L. J. (2024). Social media users trust in their most frequently used social media site. *Online Journal of Communication and Media Technologies*, *14*(4), e202445. <https://doi.org/10.30935/ojcmt/14796>

*General Data Protection Regulation (GDPR) – legal text*. (2024, April 22). General Data Protection Regulation (GDPR). <https://gdpr-info.eu/#:~:text=Welcome%20to%20gdpr%2Dinfo.eu,us%20by%20sharing%20the%20project>.

Kerr, O. S. (2024, August 14). A ruling that eliminates important privacy rights in many stored internet Contents—And the legal challenge to it. *Reason.com*. <https://reason.com/volokh/2024/08/14/a-ruling-that-eliminates-important-privacy-rights-in-many-stored-internet-contents-and-the-legal-challenge-to-it/>

Miller, C. (2024, July 31). California Appellate Court Opens 'New World of Possibilities' With Social Media Subpoena Decision. *The Recorder*. <https://www.law.com/therecorder/2024/07/26/california-appellate-court-opens-new-world-of-possibilities-with-social-media-subpoena-decision/?slreturn=20241129162425>

OpenAI. (2024). Response on privacy laws and law enforcement access. <https://chatgpt.com/>

*Social media outfits must disclose to court stored data*. (n.d.). <http://www.metnews.com/articles/2024/storeddata_072424.htm>

Wagner, K. (2018, January 19). Justine Sacco, the PR exec who was fired from IAC for her tweets, has landed back at IAC’s Match Group. *Vox*. <https://www.vox.com/2018/1/19/16911074/justine-sacco-iac-match-group-return-tweet>

Waldo, J., Lin, H., & Millett, L. I. (2007). Engaging privacy and information technology in a digital age. In *National Academies Press eBooks*. <https://doi.org/10.17226/11896>

Wikipedia contributors. (2024, July 31). *Stored Communications Act*. Wikipedia. <https://en.wikipedia.org/wiki/Stored_Communications_Act>

Appendix

Screenshot of the Post

1. Facebook: 2. Instagram:

A screenshot of a child

Description automatically generatedA close-up of a document

Description automatically generated

1. Uganda Internet showdown tweets:

A screenshot of a social media post

Description automatically generatedA screenshot of a social media post

Description automatically generated

1. ChatGPT

A screenshot of a computer

Description automatically generatedA screenshot of a computer screen

Description automatically generated