Dawson Zhang, Inu Baek Shreyes Ram, Shrihan Bolleni

23andMe

The major tasks related to the assignment, group members responsible for each task (include PPT and Activity related tasks).

- Areas to address in the paper/presentation include:
    - **Introduction/Activity**
        - Paper with 25 sites that you have to create passwords for, with different levels of sensitivity
        - Feel free to reuse if you would like
        - One MFA cover slip you have to cut and paste onto (shows realism of MFA, ask how many would have liked more slips? Shows how this doesn't reflect our reality as not many really use MFA all the time unless required
        - Evaluate (either through looking at data or just a debrief)
        - A classroom survey that also happens to have them put their address in
        - Do an inside man in front of the class and show their house on Zillow on the board
        - "Imagine if instead of your house for the entire class to see, it was your genetic code."
        - Have a demonstration of MFA and reusing passwords
    - **History**: short history of the organization (name, type, industry, customer base, year founded, other key factors that clarify the role of this organization)
        - 23andMe
        - Consumer-facing biotechnology company offering **direct-to-consumer (DTC) genetic testing**
            - Saliva kits -> online reports
        - Personal genomics / consumer testing industry
        - Founded in 2006 by Anne Wojcicki, Linda Avey, and Paul Cusenza
        - Over **12 million** kits sold worldwide
        - Ancestry reports, carrier and genetic health risk reports (some FDA-authorized), raw genotype downloads, and subscription services

        - Went public in 2021 via a SPAC; reached a **multi-billion dollar peak valuation**. Later struggled financially and with reputational issues
- **Problem**: description of the problem, context (historical, economic, social, political, etc.), and Impact of the Problem (on employees, public, corporate reputation, profits, environment, etc.)
    - October 2023: 23andMe reports 6.9 million users had data accessed by hackers using credential stuffing, which takes login credentials of other sites and uses them on 23andMe accounts
    - https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/
    - At the time of the breach, 23andMe had made two-factor authentication optional (raise your hand if you've ever felt annoyed about Duo Security)
    - Exposed Data set:
        - Full name, birth year, location
        - Ancestry and ethnicity percentages
        - Genetic haplogroups
        - Relationship labels
        - Links to public family trees
        - About me bios (for the users that filled this out, which could contain any kind of personal information)
    - The company placed blame on the "reused passwords", not themselves
    - The breach also began months before public disclosure, with initial statements trying to downplay the breach (14k)
    - General Impacts:
        - Genetic, health, and ancestry data of individuals exposed
        - Relatives and family genetic data indirectly exposed (34.9 million if we extrapolate by 5 linked relatives)
        - Consumer trust broken with 23andMe and possibly the entire genetic testing industry
        -
    - Data impacts:
        - Can cause genetic discrimination, where people are treated differently due to their genetic makeup (like making insurance more expensive if someone has genes linked to cancer)

        - Targeted social manipulation using breached information
        - Some leaked data was placed on dark web, ethnically targeting “Ashkenazi Jewish” and “Chinese” users by advertising to them (shows potential for weaponizing genetic data)
    - Company Impacts:
        - 23andMe settled for a 30 million class action lawsuit
        - Fined 2.31 million euros by ICO in June 2025
        - Strategically filed for bankruptcy, making customers feel shaky about whether data will be sold if the company is bought
- **Key players:** key people involved in the company and contributors to the problem
    - **Anne Wojcicki:** Co-founder and former Chief Executive Officer (CEO) of 23andMe. Her leadership, and subsequent resignation as CEO shortly before the company filed for bankruptcy protection (in the aftermath of the data hack and financial losses), make her a key figure in the company's trajectory and response.
    - Other Founders: **Linda Avey and Paul Cusenza** co-founded the company with Wojcicki in 2006.
    - Joe Selsavage: Interim CEO following Anne Wojcicki's resignation.
    - The Threat Actor (**Hacker**):
        - An anonymous hacker operating under the pseudonym "**Golem**" claimed responsibility for leaking and selling the stolen data on a dark web forum.
        - This individual executed a credential stuffing attack.
    - 23andMe's Security Deficiencies (Company's Contribution): Joint investigations by the **Privacy Commissioner of Canada** and the **UK Information Commissioner** found that 23andMe failed to implement appropriate safeguards. These deficiencies are considered a major contributor to the problem:
- **Evaluation of the current strategy**
    - After the 2023 data breach, 23andMe implemented multi-factor authentication, launched an internal investigation, and temporarily disabled its DNA Relatives feature.
        - The company worked with cybersecurity experts and regulators to assess the scope of the breach.
    - The company also started to emphasize ISO data security standards and allowed users to delete their data or samples.

        - Despite these steps, the response was largely reactive, with weak prevention measures and limited transparency about third-party data access.
            - Users and regulators criticized the company for failing to implement proactive safeguards before the attack.
        - 23andMe also faced backlash for blaming users for poor password practices instead of taking full responsibility for systemic weaknesses.
        - The company's ongoing bankruptcy and restructuring efforts raise concerns about data ownership and protection under new management.
        - The company's strategy focused heavily on public relations rather than structural reform, issuing statements to reassure users but making few tangible changes to core security infrastructure or data-sharing policies.
        - Overall, 23andMe's current strategy has struggled to rebuild public trust and confidence in its handling of sensitive genetic information.
    - **Recommendations:** Create and expand on at least 3 recommendations that the organization should take to restore its previous success. The recommendations should be realistic and applicable.
        - Transparency (deals, explicitly stating what the data will be used for, and making it more accessible, make sure they know what their data will be used for)
            - Revise the sharing and consent policy, help customers understand how partners can see your data, make opt-in not opt-out
            - Make videos or interactive tools that lay out how their data can be used
                - **90% of consumers expect brands to act authentically and transparently.** In one brand-authenticity study, 90 % of respondents said they expect transparency from brands. ZipDo+1
                - **70% of consumers say they're more likely to trust brands that demonstrate transparency.** Gitnux+1
                - **58% of consumers believe brands hit by data breaches are no longer trustworthy,**

and about 70% would stop shopping with a brand after a security incident. Security Magazine+1

- **34% of consumers lose loyalty when brands misuse or mishandle personal data.** In one loyalty survey, 34% identified data misuse as a reason for losing loyalty. SAP Emarsys

- **Ethical loyalty (consumers staying with brands for values alignment) was ~30% in 2024.** This suggests that transparency and values are now meaningful drivers of loyal behaviour.

- **Adopt Clear, Opt-In Consent and Real-Time Data Dashboards**
  Transition from complex, opt-out privacy settings to an explicit opt-in framework. Implement a user-facing dashboard that provides real-time visibility into how genetic data is collected, processed, and shared. The dashboard should include partner access logs, consent status, and one-click options to revoke data sharing. This system reinforces user control and mitigates legal and reputational risks.

- **Publish Routine Transparency Reports and Maintain a Public Partner Registry**
  Establish quarterly transparency reports detailing all third-party data requests, research collaborations, and law enforcement inquiries. Complement these reports with a continuously updated public registry identifying every organization with data-sharing permissions. This initiative aligns with best practices from industry leaders like Apple and Microsoft, where routine transparency reporting has measurably improved stakeholder confidence and brand integrity.

- **Enhance Consumer Education through Interactive Communication Tools**
  Develop concise, plain-language educational content — including short videos and interactive visuals — that explain how customer data flows through 23andMe's systems. According to Label Insight (2022), 94% of consumers remain loyal to brands that provide complete transparency. By demystifying data use, 23andMe can transform

transparency into a competitive advantage and a foundation for long-term trust.

-
    - Create a mandatory two-factor authentication and hire an IT consultant for further security measures
        - Hire third party
    - Start a marketing and ethics campaign that brings 23andMe to the forefront of data security regarding genetic data, making customers feel like the genetic industry is trustworthy again
        - Advocate for stronger genetic privacy policy
        - Take accountability
- **Conclusion**.
    - Takeaways for the company
    - Takeaways for YOU (the audience)
        - Link back to the activity and have full circle moment
- **Reference List - APA format**
    - https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/
    - https://www.priv.gc.ca/en/opc-news/news-and-announcements/2025/bg_23andme_250617/
    - https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2025/06/23andme-fined-for-failing-to-protect-uk-users-genetic-data
    - https://oag.ca.gov/system/files/CA%20AG%20-%20CA%20Notification%20Letters.pdf
    - https://www.reuters.com/legal/government/23andme-seeks-approval-larger-50-million-data-breach-settlement-2025-09-05/
    - https://seceon.com/23andme-data-breach-a-wake-up-call-for-consumer-privacy-and-corporate-accountability/
    - https://www.theguardian.com/technology/2024/feb/15/23andme-hack-data-genetic-data-selling-response
    - https://www.darkowl.com/blog-content/23andme-suffers-data-breach/
    - https://heydata.eu/en/magazine/lessons-from-the-23and-me-data-breach-data-privacy-in-an-interconnected-world
    - https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2025/pipeda-2025-001/
    - https://www.bitdefender.com/en-us/blog/hotforsecurity/millions-of-new-23andme-genetic-data-profiles-leak-on-cybercrime-forum
- **PPT**
- Work schedule of deadlines to stay on track.

    - Week 0
        - Start work plan
    - Week 1
        - Complete work plan
        - Complete PPT
    - Week 2
        - Finalize PPT and Outline
        - Focus the majority on rehearsing the presentation
        - Run through the activity for fluidity
    - Week 3 (Presentation on Tuesday)
        - Last run through and polishing meeting (Monday)
- Group Guidelines - at least 5
    1. Make sure to stay on top of individual work and complete it by the deadlines
    2. Make sure to show up to group meetings
    3. If you can't make it to a meeting or you're unable to finish an assignment on time, make sure to inform the group ahead of time
    4. Ensure that everyone is exerting the same effort and is held to the same standard throughout the project
    5. Respect everyone's ideas and be encouraging and constructive so we can build on each other's thinking.