Exam, Legal Aspects of Information Security

Your grade will be influenced by how well your answer is organized, on the micro-level as well as on the macro- level. Clarity is a virtue.

Where possible, state your sources. When referring to sources, you do not have to put down the full references, but they should be identifiable.

- Examples: "Article 6 of the GDPR"…." Or "the *Smith v. Sweden* case from the European Court of Human Rights is an interesting example of…"

Time is scarce and **word count is limited to 2500**. It may be necessary for you to first try to identify the most pressing issues to be dealt with. For full credit on the question, it is not necessary that all issues are dealt with in detail.

The following grading scale is used:

- Fail (F, FX)(below 50 points)
- Sufficient (E)(50-59 points)
- Satisfactory (D)(60-69)
- Good (C)(70-79 points)
- Very Good (B)(80-89 points)
- Excellent (A)(90-100 points)

Students will be graded on the basis of facts, focus and form as follows:

- Facts - ability to demonstrate knowledge of the issue(s).
- Focus - ability to analyze the issue(s).
- Form - ability to present a well-structured and formulated answer.

You are not permitted to use any generative AI tools, including ChatGPT.

Question 1:

Since 2015, Boomin, located in Stockholm (Sweden), has provided Boom, a photo storage and organization application, to consumers. Boom is available as both an iOS and Android mobile application ("app"), as well as in a web and desktop format. Globally, approximately 12 million consumers have installed Boom. Boom allows consumers to upload photos and videos to Boom's cloud servers from sources such as the user's mobile device, computer, or accounts with social media services, such as Facebook or Instagram, or cloud-based storage services, such as Dropbox or One Drive. By storing photos and videos on Boom's servers, consumers can free up storage space on their devices. Boom uses automated features to organize users' photos and videos into albums by location and date.

In February 2020, Boomin launched its "Friends" feature, which operates on both the iOS and Android versions of the Boom app. The Friends feature uses face recognition to group users' photos by faces of the people who appear in the photos. The user can choose to apply "tags" to identify by name (e.g., "Jane") or alias (e.g., "Mom") the individuals who appear in their photos. These tags are not available to other Boom users. When Boomin launched the Friends feature, it enabled face recognition by default for all users of the Boom mobile app. Boomin did not provide users of the Boom mobile app an option to turn off or disable the feature.

Boomin offers users who no longer wish to use Boom the ability to deactivate their Boom accounts. When a user chooses to deactivate their Boom account, Boomin displays a message that tells the user: "We're sorry to see you go! If you choose to deactivate your account, you will permanently lose access to [##] photos and [##] albums." (The message specifies the numbers of photos and albums stored in the user's Boom account.) The message includes a button for the user to click to deactivate their account.

If the user clicks the "Deactivate My Account" button, Boomin then displays a second message stating: "Are you sure? You will lose access to your account and we can't undo this." That message includes buttons that present the user with the choice to "CANCEL" or "DELETE."

Boomin's Privacy Policy also states:

> "If you wish to deactivate your account or request that we no longer use your information to provide you any services or certain services, such as our Friends feature or our face recognition services. Please understand that we may need to retain and use your information for a certain period of time to comply with our legal obligations, resolve disputes, and enforce our agreements. Consistent with these requirements, we will try to delete your information as soon as possible upon request."

Contrary to the statements Boomin did not, in fact, ever delete the photos or videos of any users who had deactivated their accounts and instead retained them indefinitely. Boomin also consistently failed to log sufficient information to adequately assess cybersecurity events; properly configure vulnerability testing and scope penetration testing of the network and web application; or even comply with its own written security policies.

In or around March 2023, a hacker exploited security vulnerabilities in Boomin's system. The hacker found photos and video stored in a database connected to Boomin's network. The hacker exported this information over the Internet to outside computers.

On April 11, 2023, Boomin received notice of a security incident involving an intrusion into its network. An individual stated that he "believe[s] hackers have access to your customer [database]. The data is currently for sale in certain circles."

Part 1A (20 points):

You work in the legal department at Boomin. Prepare a memo detailing the legal issues raised in this scenario and how you will respond, if at all.

Part 1B (20 points):

Hans is a customer of Boomin who purchased services from August 2016 - December 2022. In May 2023, he was shocked to receive a notification from Anonymous Hacker that his personal data would be shared on the Dark Web unless he paid a sum of 2000 EURO. This is especially true since he deleted his account in December 2022 and believed that all his personal data had been removed from the website.

Upset and aggrieved, Hans has turned to his local Data Protection Authority in Sweden, the Swedish Authority for Privacy Protection (IMY), seeking redress against Boomin. You work at IMY. Decide whether to impose fines and if so, on what basis.

Question 2:

Over the past decade, technological advances have drastically evolved our daily engagement with technology. The COVID-19 pandemic also jump-started many organizations' need to adapt (and for some, to establish) their internal and external digital infrastructure to transition to remote work or to adapt a brick-and-mortar business to e-commerce.

Part 2A (20 points):

As we further integrate into the digital world, the risk of encountering cybersecurity threats grows due to vulnerabilities stemming from aging internet platforms and deliberate attacks. There is a growing community of start-ups and small and medium-sized enterprises (SMEs) offering innovative cybersecurity technology to address these threats.

You work for a start-up entitled Cyber Innovation where you develop new and inventive systems and processes to counteract cybersecurity threats. Cyber Innovation's main innovation is Standpoint, a network security monitoring and correlation system that provides a three-dimensional (3D) visualization of network traffic overlaid with security alerts and other relevant discrete data. This innovative software gives security professionals the ability to see and interact with data spatially, eliminating the need to scroll through massive spreadsheets of technical data.

What intellectual property strategies exist to safeguard Cyber Innovation's products and services such as Standpoint?

Part 2B (20 points):

Hans is the CEO of a medium size company called Happykey located in Stockholm, Sweden. Most Happykey employees enjoy working at home and Hans would like to support them to do so. However, Hans is worried about some of the disadvantages of remote work. While Happykey has been focusing on its digital transformation the last few years, it is still utilizing processes that have manual, printed, or face-to-face components. One such process includes document signing.

Hans is interested in using e-signatures, but he is unsure if they are secure and legally valid, especially when it comes to critical documents like contracts, tax forms, and invoices.

You work in the legal department. Advise Hans on this matter.

Question 3 (20 points):

Elsa is a malign actor who decides to employ a deepfake audio to attack Stockholm Bank for financial gain. She conducts research on the dark web and obtains the name, address, social security number, and bank account number of Marcus. Elsa identifies Marcus' TikTok and Instagram social media profiles. She utilizes the videos posted on social media platforms to train the model and create a deepfake audio of her target Marcus. Elsa researches Stockholm Bank for the verification policy and determines there's a voice authentication system. Next, she calls the financial institution and passes voice authentication. She is routed to a bank representative and then utilizes Marcus' proprietary information obtained via the dark web. Elsa tells the bank representative that she was unable to access her account online and needs to reset her password. She was provided a temporary password to access the online account. Elsa gains access to her target's financial accounts. Elsa wires funds from the target's account to overseas accounts.

As this scenario highlights, the relationship between AI, data protection, cybercrime and information security is highly complex. Please discuss. In particular, how does/should/will the law respond to events such as those described above?