

CAB-240 Risk Report

Contents

[Project Members 3](#_Toc114393014)

[Organisation Establishment: 3](#_Toc114393015)

[Introduction 3](#_Toc114393016)

[Discussion 5](#_Toc114393017)

[Context Establishment 5](#_Toc114393018)

[Hardware 5](#_Toc114393019)

[Software 5](#_Toc114393020)

[Data 6](#_Toc114393021)

[Device Usage 6](#_Toc114393022)

[Risk Assessment 8](#_Toc114393023)

[Security Issue with Device Application 8](#_Toc114393024)

[Security Issue with a Device Operating System 9](#_Toc114393025)

[Security Issue with Device User Behaviour 10](#_Toc114393026)

[Physical Threat to Mobile Devices 11](#_Toc114393027)

[Risk Assessment Summary 12](#_Toc114393028)

[Privacy Impact Analysis 12](#_Toc114393029)

[Name of the Application 13](#_Toc114393030)

[Type of Information that is Collected 13](#_Toc114393031)

[How is the Information Collected 13](#_Toc114393032)

[When is the Information Collected 14](#_Toc114393033)

[How Relevant is the Collected Information in the User’s use of the App 14](#_Toc114393034)

[How is the Information Stored 14](#_Toc114393035)

[How is the Collected Information Used by The Application 14](#_Toc114393036)

[Use of Encryption 15](#_Toc114393037)

[Sharing of Collected Information 15](#_Toc114393038)

[User Access to Collected Information 15](#_Toc114393039)

[Privacy Risk Identification and Analysis 15](#_Toc114393040)

[Which Assets are Most at Risk 15](#_Toc114393041)

[What Sort of Analysis can be Performed 16](#_Toc114393042)

[Limitations / Difficulties of Risk Analysis 16](#_Toc114393043)

[How is this Connected to User Privacy? 16](#_Toc114393044)

[Privacy Impact Analysis Summary 17](#_Toc114393045)

[References 17](#_Toc114393046)

[Appendices 19](#_Toc114393047)

[Appendix 1 19](#_Toc114393048)

[Appendix 2 19](#_Toc114393049)

[Appendix 3 19](#_Toc114393050)

[Appendix 4 19](#_Toc114393051)

[Appendix 5 19](#_Toc114393052)

[Appendix 6 19](#_Toc114393053)

[Appendix 7 19](#_Toc114393054)

# Project Members

|  |  |  |  |
| --- | --- | --- | --- |
| **Team Member** | **Student Name** | **Student Number** | **Last Digit** |
| 1 | Braydan Newman | n11272031 | 1 |
| 2 | Elshan Rahnamay Touhidi | n10937668 | 8 |
| 3 | Quinn Rigby | n11251557 | 7 |

# Organisation Establishment:

**Industry Sector:** Transport

**Employee Type:** Technician

**Mobile Device Type:** Samsung Galaxy S21 FE 128GB

**Device Owned By:** Employee

**Usage Restrictions:** Used for all personal use and for work use

# Introduction

Logical logistics is an organisation in the transport sector that focuses on allowing clients and customers to complete all of their goods transport needs. The organisation enables customers to ship their online purchases and transport vehicles, along with any other goods transportation that they may require.

As a large amount of technology is used within the organisation to help day to day operations run efficiently, the impacts of device security are extraordinary. By looking at the employment position of a technician, the greater impact of the use of technology toward the goals of the organisation can be seen, along with how this use impacts information and general cyber security. The technician’s role within the organisation is to provide support to all online resources that are involved, both on the business and customer sides. This involves website support, shipment booking software support, and the management of all customer and employee data that is handled by the organisation.

The technician contributes to the organisation’s objectives and goals by providing customers with a seamless and smooth experience with booking their goods transport service through the website, along with making sure all crucial business applications are running properly, providing technological support to employees and customers, and managing all sensitive data that is stored by the organisation. This contributes to the objectives of the company as it allows the majority of business operations (apart from the actual goods transport handled by shipment / truck drivers) to run efficiently, allowing users to experience a smooth, quick and hassle-free process for their goods transportation.

Mobile device security is incredibly important in the context of this organisation as the technician employee has access to sensitive information about customer and employee information. Along with this, the technician also has sensitive company information regarding to the running of the business and the logistical chain that operates when a customer wants to utilise their transport services.

The purpose of this report is to outline the security concerns, vulnerabilities and impacts associated with using the Samsung Galaxy S21 FE 128GB mobile phone for both personal and work use. The report will highlight the specifications and usage of the device, a risk assessment of security issues, a privacy impact analysis and recommendations that will improve the security associated with the device’s usage for both work and personal purposes.

Before the report is undertaken several assumptions have been made, and limitations noted about the device, and the scope / level of detail that the report goes into. One assumed limitation of the device that has been made is that the device has the smallest storage option out of its series’ line-up, meaning that as the user utilises the device for both work and personal purposes, there may not be enough storage to handle this amount of data needed to be stored on the device. A limitation to the report, with regards to the overall scope and level of detail is that the report only considers the risk of one application, leaving out the various others that are also utilised by the employee.

# Discussion

## Context Establishment

The Samsung Galaxy S21 FE 128GB is the budget conscience option out of the Samsung S21 device line-up. The device is aimed at being a budget friendly smartphone that still delivers an immense amount of functionality and. While this device is not the flagship of the S21 line-up, it still has noteworthy hardware features and security guarantees.

### Hardware

The first of these hardware features is the devices’ cameras. The device is equipped with a 12 megapixel (MP) ultra-wide camera, a 12 MP wide angle camera, an 8 MP telephoto camera and a 32 MP selfie camera that boasts stunningly clear photos (Samsung, n.d.).

The system chip onboard the device is a Qualcomm Snapdragon 888 SM8350 (5 nm) chipset that integrates industry-leading innovations in 5G, AI, gaming and photography (Qualcomm, n.d.). The device also utilises an Octa-core, 2840 MHz, Kryo 680 Prime, 64-bit processor allowing users to have a fast and powerful experience with the device (Phone Arena, n.d.). Onboard the device is also an Adreno 660 graphics card (GPU) that allows the phone to display ultra-HD and crisp graphics to the user, enhancing media consumption, gaming and everyday use (Phone Arena, n.d.). The device is also equipped with 6 gigabytes of memory (RAM), enabling the device to seamlessly switch between applications and access data faster (Phone Arena, n.d.).

As alluded to in the name of the device, it also comes with 128 gigabytes of storage (Samsung, n.d.). This allows users to have a large photo album, download various applications, media content and music, without having to sacrifice data in order to free up space for an essential work mandated application. The phone also utilises a 4500 milliampere hour long-lasting battery that can be charged either wirelessly or through the USB-C port (Samsung, n.d). The device also comes with a 6.4-inch, 2340 x 1080-pixel Dynamic AMOLED display that has a refresh rate of 120 hertz, which has HDR support, is scratch resistant, and has an automatic brightness adjuster due to an ambient light sensor (Phone Arena, n.d).

The device has biometric security measures of 2D face unlocks and ultrasonic in-screen fingerprint reader, along with standard password, pin, and android pattern unlock features. The device also has 5G capabilities, along with Bluetooth 5.0, Wi-Fi connectivity, and dual-sim features (Samsung, n.d).

### Software

The Samsung Galaxy S21 FE 128GB device comes out of the box with the Android 11 operating system (OS) (Samsung, n.d). Since the release of the phone however, Android have come out with another iteration of their OS, the Android 12, which is available for this device. Both of these operating systems are supported by Android, backed with a 5-year security update guarantee by Samsung themselves (Android Authority, 2022).

During the work and personal usage of the mobile device, several applications will be accessed and interacted with by the employee. Several of these applications are preloaded by the device OS like messenger and phone, and others are loaded by the organisation including Facebook Workplace, Slack, Microsoft Teams, Microsoft Outlook, Facebook Work Chat, Zoom Virtual Meetings, Google Sheets and the Office 365 Suite of Apps (i.e., word, excel etc…). The rest of the applications used by the employee may include, but are not limited to Instagram, YouTube, Netflix, Stan, Facebook, Twitter, Premier League, Optus Sport, Google Maps, Uber, CommBank, and Bumble. While these applications may not necessarily be on every employee’s mobile device, it is an accurate depiction of the types of applications organisations require employees to have along with the types of applications that the user may have for their personal use.

### Data

As the employee uses the device for both work and personal purposes, a large amount of data will be needed to be stored on the device. This data will include a large amount of work and personal contacts (approximately 500 megabytes (mb)), a large amount of work and personal photos and videos (approximately 30 gigabytes (gb), a moderately sized collection of download music, books and podcasts (approximately 5 gb), a large amount of downloaded media content from streaming services (approximately 30 gb), a fairly large amount of cached data in applications (combined approximately 5gb), a large amount of data stored in work and personal emails (approximately 5gb), and OS and system data (approximately 25gb).

## Device Usage

The employee may use the device for work purposes by answering business related calls, interacting with various work and team specific applications, responding to emails and texts from colleagues and customers, and taking pictures of problems encountered on a day-to-day basis. They also use their device for personal activities which may include browsing social media applications, responding to personal emails and messages, watching videos online, interacting with online banking from their phone, and taking part in online dating.

The usage outlined above shows how the employee interacts with the organisations information assets on a daily basis as they will be managing sensitive information stored by the company, they will be sending and receiving emails and texts that may contain sensitive customer or employee information, company policies or internal communications that are meant to be confidential within the organisation, they will be photographing company property that may contain sensitive information, and they will also have access to shipping timetables, routes and general information.

The information stored in the organisations databases consist of sensitive information relating to both customers and employees, most notably customer email addresses, phone numbers, account passwords and shipping addresses. Along with this, the database will hold information relating to shipping details and employee payment information. All of the data stored within this database is incredibly sensitive and critical in maintaining smooth business operations on a daily basis. If the database was breached in some form of attack or an exploited vulnerability, the sensitive data would lose its confidentiality and customer, employee and business information will be put at risk. Along with this loss in confidentiality, flow on impacts may occur with regards to the integrity and availability of this data. If an attacker were to gain access to the system, they can easily manipulate the recorded data, lock access to the database, or delete the database entirely.

The information that is handled and passed through emails, text messages phone calls and other communications on work applications by the employee may also contain sensitive information about the organisation, other employees and customers. The information transmitted through these communications is incredibly sensitive and relates to customer support information, customer information, employee information and the organisations information. This asset is important within the organisation as it allows employees to share information along with allowing employees to interact with customers and offer support to help provide a satisfactory experience with the organisation. However, unlike the database, the only CIA principle that is going to be impacted is confidentiality, this is because these communications are not a physical resource that can be changed or deleted, only viewed / intercepted. While confidentiality is the only principle affected, it is still important to uphold this principle as the information passed through the communications is sensitive and may put the organisation, employees and (or) customers at risk.

The information contained in the photographs taken by the employee may contain information relating to the organisation’s processes and policies (general information), information about online resources like the business’s website, and customer information through photographing communications to share with other employees. This information that may be contained in the photographs stored on the employee’s device is sensitive as it related to the organisation’s confidential information and customer details. This asset, however, is not critical in achieving the goals of the business or ensuring smooth and efficient business operations as the photographs are not necessary in the operation of the organisation. While the asset is not critical or important in the organisation’s operations, it is still important that the information be kept confidential as it relates to sensitive information. If this data was to be seen by an unauthorised person or party, it may put the organisations data and customers data at risk.

The information asset of shipping information such as routes, timetables and other important details that is kept on the employee’s device is also a sensitive asset. This is a sensitive asset as it contains details of customers addresses, contact information, shipping routes, shipping times, and other information relating to the drivers and organisation. This asset is critical to the organisation as without it they would not be able to provide their service of transporting goods across Australia. If this asset was to be exploited or attacked, information may lose its confidentiality, along with the integrity and availability of the data being lost. This is due to the fact that an attacker may change or delete the shipping routes or times, customer addresses or driver and vehicle assignment details. Therefore, this asset can be seen to be incredibly Important to achieving the goals set out by the organisation in providing customers with an easy, hassle-free goods transfer process.

The applications that might be interacted with the most frequently include, Facebook Workplace, Zoom, Microsoft Outlook, Microsoft Teams, Slack, Instagram, Netflix, Facebook, Optus Sport, CommBank, Bumble and the phone and messenger. These applications are assumed to be used the most frequently used as they are essential for completing work from the device, interacting with social media and content delivery through subscription television and sports services, and interacting with mobile banking. These apps also provide a good mix between the different aspects of the employee’s personal usage of the device as it is spread between social media apps, media consumption apps, a sports consumption app, an online banking app, and an online dating app.

While some applications are used frequently by the employee, several apps including Google Sheets, Stan, Premier League and Uber are used rarely. These applications will get the least amount of usage on the device as most work documents are created and edited using Microsoft Offices Word instead of google sheets, as Netflix is the primary entertainment streaming application and Stan is only utilised for a couple of series’, as Premier League games cannot be viewed on the app with its namesake, but instead on Optus Sport, and as the employee drives their own vehicle and does not need to use Uber except on special occasions.

Even though some applications may be interacted with by the user more frequently than others, similar types of information will be used throughout. The work-related applications consist of information about the organisation including any sensitive customer or employee details that may have been shared with the user through phone calls, emails, photographs, text messages or from having been sent over Slack or Workplace. These applications may also contain login details, private policies of the organisation, shipping timetables and shipping routes, which are required to stay confidential. The information handled by the personal usage applications on the device may consist of the user’s private information including address, contact information, login credentials, banking / payment credentials, the user’s personal contacts and photographs.

## Risk Assessment

The following section of the report summarises recent articles in relation to a security issue associated to a mobile device application, a security issue associated to a mobile device operating system, a security issue associated with mobile device user behaviour, and a physical threat to a mobile device. Included in these summaries is an outline of what the information asset identified is, what the security issue is, what the vulnerability is, and what the security incident / attack is.

### Security Issue with Device Application

**Title:** Hackers can exploit a flaw in Apple's latest update to take full control of your iPhone and Mac

**Author:** Matthew Loh

(Loh, M., 2022) (CVE-2022-32893, 2022).

The article discusses a variability with the apple application safari which is the default web browser on all apple devices. Software needed by safari to run enables maliciously crafted content on a web page to run arbitrary code on the given device. (Refer to appendices 1 and 2 for full articles).

There isn’t a specific information asset involved in this attack the attacker could be going after and doing a wide verity of things Eg.(Privilege escalation, Malware, Spyware). The attacker had to write software that wrote data outside the allocated buffer, and this was allowed due to the bug in WebKitGTK in safari. With arbitrary code execution anything is possible with this attack and is not limited.

This is an external threat involving deliberate human action by the attacker. Writing software with the known bug in mind to write data outside the given buffer allowing potentially harmful code to be executed by another process. This could allow the attacker to gain full access over the device. This can compromise all security goals, Confidentiality, Integrity, and availability depending on how this attack is performed and used.

The vulnerability with this CVE is about improper management of data or “Out-of-Bounds Write” (CWE-787), the more common consequence of the vulnerability is just data corruption, but when done right this can lead to an arbitrary code execution, which in turn could allow the attacker to take over the device fully and from there they can perform any attack they want on the device.

The article describing this vulnerability and the related CVE reports describe the incident in further detail. This Given Security flaw (CVE-2022-32893) was officially realeased to the public on the 24/8/2022 with the flaw having a rating of 8.8 (High) on the severity scale. The flaw affected IOS and iPadIOS and safari versions lower than 15.6 and macOS versions 12.5 and lower. This vulnerability used safari webKitGTK as the attack vector and used maliciously crafted web content which could lead to arbitrary code execution. This exploit is extremely easy to pull off and affected over 1 billion devices, however, it does require user actions to pull off such as navigating to a malicious website but merely opening the link is enough for the attack to be pulled off. The type of attack is a “out-of-bounds write” it which case the program writes data outside the intended buffer space. At the time of writing the CVE is still at a great effect and is not completely solved by apple.

### Security Issue with a Device Operating System

**Title:** Google patched a critical Android 12 security flaw today

**Author:** Doroteya Borisova

(Borisova D., 2022) (OpenCVE, 2022).

The article discusses a vulnerability in the mobile OS Android, and the CVE for this security flaw is CVE-2021-39675. The bug used a flaw in the NFC code for privilege escalation with no user interaction giving this a very high CVE rating of 9.8. (Refer to appendices 3 and 4 for full articles).

There isn't a specific type of information involved in this attack, but in combination with a RAT (Remote Access Trojan) this would give it admin levels of control over your android device putting all data stored on the device at risk. The bug affected Version 12 of Android OS early this year with the number of vulnerable devices being upwards of 1 billion.

The threat from this bug doesn't allow an attacker to gain initial access to a vulnerable devise but instead allows a bad actor with minimal privilege to escalate into the equivalent of admin on an android. From here the attacker could do anything they wish from data collection to malware to adding the device to a bot net.

The vulnerability is in code for the NFC found in GKI\_getbuf of gki\_buffer.cc. The type of attack that is used for this is an Out of Bounds Write (CWE-787), and the privilege escalation doesn’t require any user interaction with the devise and can be done remotely.

The article does not describe the attack processes as google never released any information on how to perform the attack but it’s safe to say that it would be performed like most Out of Bounds Write exploits with using some code in android that doesn't handle memories correctly that then gives escalated privilege to the process. The flaw was first published in 11/02/2022 by google, but the possibility that this flaw was used in the wild before google found it is high. The flaw affected over 1 billion devices would wide but since its patch earlier this year, it has now been rendered ineffective.

### Security Issue with Device User Behaviour

**Title:** Oversharing in Social Media, A Biggest Security Risk

**Author:** Anil Rachamalla

(Rachamalla, A., 2022)

The article discusses the security risk that sharing personal information online has on a user. The human need and want to share information about yourself to others in real life or over the internet can cause major security risks. (Refer to appendices 5 and 6 for full articles).

The information involved in these social engineering attacks, where an attacker manipulates a device user for a certain goal, can be anything from passwords to just emails, as to gain access to all your personal information. Social engineering attacks become a lot easier to perform on people when the attacker already knows personal information about you, that you most likely have shared online. The information that could be useful for social engineering could be your pets’ names, family members and a lot of various other personal and family details, as this allows the attacker to get closer to you.

The threat of over sharing personal information about yourself or others online isn't an internal or external threat but comes from the fact that as humans we like to tell others about ourselves and with enough of this information this can become a vulnerability. For a brief example if your password to everything is your dog’s name and you share your dog’s name with someone, they now have your password or something close to it. You are unknowingly compromising your own confidentiality.

The vulnerability with sharing information about yourself is that you are telling people how to attack you and your most vulnerable points. For example, if you tell some you are having trouble with power bill, they can use this information to make a spearfishing attack on you. People have a tendency implicitly trust another person and this can be taken advantage of by an attacker with malicious intent.

Social Engineering and over sharing are happening all the time, and with the information they gain it makes it a lot easier to perform attacks like, Spearfishing, Pretexting, Baiting, and so many more. Whilst over sharing isn't a security vulnerability in itself, it does help facilitate a vast majority of other vulnerabilities.

### Physical Threat to Mobile Devices

**Title:** Eavesdropping User Credentials via GPU Side Channels on Smartphones

**Authors:** Boyuan Yang, Ruirong Chen, Kai Huang, Jun Yang, Wei Gao

(Yang, B., Chen, R., Huang, K., Yang, J., & Gao, W., 2022)

This paper discuses a vulnerability with phone GPU’s and how they display images on the screen. The GPU could be used to infer with high certainty what the user was typing from within another application. (Refer to appendix 7 for full article).

The information at risk with this vulnerability is any typed information like passwords, private information, or even online banking credentials. The vulnerability turns your on-screen keyboard into a key logger, tracking all keystrokes made with the device.

This is an external threat involving deliberate human action by an attacker who is recording the latency of the GPU and correlating that with user inputs and the screen display. There is always ambiguity when it comes to trying to eavesdrop, this has been attempted on CPU’s but due to the GPU solely being used for graphics rendering, the correlation is much higher and has far less ambiguity. The reason typing has such an impact and is easily correlated to latency in the GPU is because of Android over draw and how android renders in layers, some parts are drawn multiple times.

The vulnerability is with how easy it is to spot different keystrokes in the latency of the GPU. This can be done by downloading a malicious application, the app doesn't even need elevated permissions to accomplish the key logging. Due to the app not having to do much, it is super lightweight to run and accurate to over 80%, even with passwords up to 16 characters. With this data the app could ex-filtrate the users sensitive and confidential information to anyone.

The paper describes a theoretical attack flow that is possible with this exploit. To actually use the data collected from the GPU, the data is first passed through a model to make sense of the data and give a key press. These models need to be trained and once done it can be bundled up into APK files that are freely downloadable from the App store. Once on the victim’s device, with the keystroke tracker application running in the background, the attacker can start collecting data from the GPU passing, passing it through the trained model and inferring what key has been pressed. From here the data is sent back to the attackers. The attack has only been performed on certain devices, but theoretically could be exploitable on almost any modern smart phone. The security researcher that came up with the vulnerability has told companies such as google and Qualcomm who make the OS and chips for the devices, and they have since put in mitigation to combat this vulnerability in their device operating system and hardware.

## Risk Assessment Summary

Overall, the security issues discussed in the 4 papers and articles posed serious threats against user privacy, many of which may still impact devices that have not yet been patched and protected against them. While all the vulnerabilities have been against users of the devices and not major companies, the risk of mass data breaches are low, however, these technics could still lead to bad actors gaining access to these companies. The threat still posed by these issues leaves millions of people vulnerable to exploitation and with the compounding of multiple of the identified flaws a device could be fully taken over and all data like bank details and secure passwords may be stolen. The consequence of these vulnerabilities has been low due to the swift actions of the manufacturing and software development companies, and by some vulnerabilities still being theoretical, but if circumstances were different, these vulnerabilities may have led to massive data theft, ransomware, and spyware attacks on hundreds of millions of users' worldwide.

## Privacy Impact Analysis

The following section of the report contains a privacy impact analysis undertaken on a privacy policy within an application that may be present onboard an employee such as the one defined within the context establishment that uses their mobile device for both work and personal purposes. The privacy impact analysis contains a summary of a privacy policy for an application, a privacy identification and analysis for the data associated with the application, and a privacy impact summary.

### Name of the Application

Bumble is an online dating application; it displays potential matches to users, giving them the ability to indicate an interest or dis-interest in a person.

### Type of Information that is Collected

According to bumbles privacy policy the first phase of the app collects registration information such as: name, email, username, mobile number, date of birth and other social media accounts login information (Facebook and Instagram accounts).

Generally other information that are collected during use of app and sites of bumble are:

• Network activities such as links, browsing history and interactions with bumble app and sites

• Profile information and content

• Content of messages, photographs, and videos

• Geolocation Information

• Device Information such as IP address and IP sessions

• Cookies

In some situations, there is a number of other information that may be collected such as:

• Sensitive information: “Age, gender identity, marital status, sexual orientation, race, ethnic background, religious views, and medical conditions”. (Bumble - Privacy, 2022)

• Commercial and purchase information including transaction history

• Biometric information

### How is the Information Collected

Information at bumble can be collected at different times and vary on the type of situation, for example in the registration phase the user’s personal information and location will be collected along with network and device information. As the user intends to build their profile, upload pictures and interact with other users via messages, photos, and other means, this sensitive information will all be collected. Sensitive information is collected under user’s explicit consent. Commercial and purchase information is also collected when a transaction occurs during their session. Some personal information such as contact details may be collected through customer support enquiries, surveys, contributions, and success stories conducted by Bumble.

### When is the Information Collected

According to bumbles privacy policy, personal, network, device, and other sensitive information is generally collected during use of the application, however, Bumble might collect information while not using the app where users have given access to their device’s location:

“When you use your mobile, we will collect information about WiFi access points as well as other location information about your longitude and latitude and may save your device’s coordinates to offer certain features to you.” (Bumble - Privacy, 2022)

### How Relevant is the Collected Information in the User’s use of the App

Bumble personalises its contents and features based on the user’s device, location, photos, and character information. According to Bumble’s privacy policy, optional character information is used to facilitate networking opportunities along with device location where it makes interaction with people nearby easier (Bumble - Privacy, 2022).

### How is the Information Stored

According to the app’s privacy policy, Bumble stores information across several servers in the world, “including the US, UK, EU, and (for Users located in Russia) Russia” (Bumble - Privacy, 2022). The hardware that is used to store the collected information is owned by Bumble Group and follows EU approved model clauses. Bumble keeps users’ information as long as the described legal basis allows. Bumbles’ stored information is described under contractual necessity, legitimate and consensual interests. They also retain biometric information for future verification purposes for a period of three years after final interaction with the app.

### How is the Collected Information Used by The Application

As part of anti-fraud and anti-spam procedures, device, personal, and payment information are used to keep users safe. Bumble uses further data such as government ids, verification photos, message content and photographs to ensure safety and prevent fraud. The collected personal and device information is used for marketing, communication, and surveying purposes. According to Bumble’s privacy policy, Bumble reserves the right to access all sorts of information for legal reasons, for instance protecting legal rights, and preventing harm to company and/or third-party providers. The previous ban history is also recorded and used in Bumble Group platforms to prevent users from registering again.

### Use of Encryption

According to the bumble privacy policy, data servers are protected by firewalls and appropriate security actions are taken:

“We pride ourselves on taking all appropriate security measures to help protect your information against loss, misuse and unauthorised access, or disclosure. We use reasonable security measures to safeguard the confidentiality of your personal information such as secured servers using firewalls” (Bumble - Privacy, 2022).

However, in terms of data transmission and storage security, Bumble do not disclose any use of end-to-end encryption or other security method and do not guarantee the security of data transmission:

“We cannot guarantee the security of your personal data while it is being transmitted to our site and any transmission is at your own risk.” (Bumble - Privacy, 2022)

### Sharing of Collected Information

User information is shared with third-party apps for billing, authorization, payment, social media integration, market research and troubleshooting purposes. These service providers include: Bumble Group companies, Facebook, Instagram, Google Play, Twilio, Spotify, Khoros, Kantar and Typeform. Also, Bumble reserves the right to share existent information on a business transaction. According to the disclosure section on Bumble’s privacy policy, information may be shared to prevent any misuse of application or responding to law authorities or other investigation purposes.

### User Access to Collected Information

Depending on the user’s country of residence’s privacy laws, users have the right to access, erase, and restrict personal information. This can be done by emailing the Data Protection Officer (DPO@team.bumble.com) or making contact through the feedback page (https://bumble.com/contact-us). The postal address at The Broadgate Tower Third Floor, 20 Primrose Street, London, United Kingdom, EC2A 2RS is also available for users to contact regarding their data.

## Privacy Risk Identification and Analysis

### Which Assets are Most at Risk

Regarding previous class actions against Bumble about their data breaches, users are concerned if any vulnerabilities still exist (Mozilla, 2021). According to Bumble's privacy policy, the application stores portions of data in Russia, where ACSC has recently warned organisations about criminal cyber threats to critical infrastructure following Russia’s invasion of Ukraine (Cyber.gov.au, 2022). Following a forensic analysis of the Bumble app, “it was possible to identify some of the pictures exchanged in personal conversations within cached files” and private directory of the app provided “valuable information about a user, such as the messages exchanged with others, their matches, data about their linked Facebook account, and configuration settings” (Barros et al., 2022). If a vulnerability is exploited by an attacker due to a lack of security, users’ sensitive information such as sexual preferences, religion, political beliefs, private messages, and pictures could be exposed and result in terminations and (or) arrests depending on the origin of the user. High-ranked political and other government workers are at high risk of being targeted for such attacks. It also increases the possibility of sexual harassment and other harms to users following their personal information breach. Moreover, personal information may be used to extort the organisations’ employees for sensitive and confidential information. In this scenario, the technician can be blackmailed to provide high-profile customers’ personal or payment information.

### What Sort of Analysis can be Performed

Qualitative analysis would be performed to measure potential risks, their likelihood, and their possible outcomes. This will allow people to analyse how a user’s sensitive and payment information breach could be harmful and what the likelihood of it happening in the product cycle is. Treatments and preventing actions will also be studied to reduce risks. Depending on the user’s background and behaviours, the consequences of a security breach can change and studying them closely is preferred as this allows for the measurement of treatments and likelihoods accordingly.

### Limitations / Difficulties of Risk Analysis

Bumble provides both a privacy policy and cookie policy online, although Bumble uses third-party software providers for one or more of their business functions and there are no relevant links to external parties and service providers privacy policies. In terms of security of data transmission and storage, bumble’s privacy policy security and firewall specifications are unclear and lack transparency. Moreover, Bumble Inc., the parent company of Bumble, Badoo, and Fruitz does not disclose how age verification and storage of biometric information works within their applications.

### How is this Connected to User Privacy?

Lack of transparency and increasing number of unnecessary information collections without clear disclosure notice have made concerns around identity theft and mass surveillance. Any unnecessary or unjustified information such as biometric information, political believes and private messages can put users’ privacy and freedom under threat. According to Privacy ACT 1988, biometric information along with religious views, ethnic background, and political beliefs fall under the sensitive information category (Australian Government, 2022). Sensitive information requires a high level of privacy protection and consent to be collected by companies. Bumble claims sensitive information is collected with explicit consent from users, whereas it is arguable that the notice of secondary use of data is not clear while using the application. Moreover, Australian privacy legislation requires companies to “clearly explain how they want to handle your personal information” and “communicate their request in plain English, without legal or industry jargon” (Australian Government, 2022). As mentioned previously, Bumble does not reveal any used encryption or security measures for handling data. Bumble’s privacy policy does not include any information on how Bumble Group meets with Australia privacy legislation; however, they perform under GDPR and California privacy laws and allow users to reach appropriate authorities upon an issue. Overall, Bumble follows the same factors in the Australian Privacy Principles and uses personal information for marketing purposes in regulation with consumer data rights, such as providing information on how data is collected and shared, who accesses the data, how long it is stored for and how users can manage/withdraw consents. (Consumer Data Right, 2020)

## Privacy Impact Analysis Summary

Breach of user’s sensitive information can result in harmful consequences and holds a priority for treatment and regulating unnecessary collection. Sensitive information breach es can result in harm to sexual minorities or result in individuals’ arrest in some regions around the world. With education and more regulations, unjustified data collection can be reduced to very minimal amount. Another priority for treatment is the ability to delete biometric information where they are frequently stored in foreign countries. Biometric information breaches can cause illegal and dangerous activities such as malicious use of fingerprint and face recognition data or mass surveillance (Biometrics and Privacy - Issues and Challenges, 2022). Another priority is to identify and treat vulnerabilities in users’ devices. An information breach can occur from physical or online unauthorized access to users’ devices. In this scenario, target devices are owned by individuals and the organisation cannot provide technical support or monitor high-sensitivity employees’ devices.

# References

Android Authority. (2022, August 16). Samsung Galaxy S21 FE gains August 2022 security patch in the US. <https://www.androidauthority.com/samsung-galaxy-s21-fe-update-3090962/>

Australian Government. (2022, July 10). Privacy Act 1988. Www.legislation.gov.au. <https://www.legislation.gov.au/Details/C2022C00199>

Barros, A., Almeida, R., Melo, T., & Frade, M. (2022). Forensic Analysis of the Bumble Dating App for Android. Forensic Sciences, 2(1), 201–221. <https://doi.org/10.3390/forensicsci2010016>

Biometrics and Privacy - Issues and Challenges. (n.d.). Office of the Victorian Information Commissioner. <https://ovic.vic.gov.au/privacy/biometrics-and-privacy-issues-and-challenges/>

Borisova, D. (2022). Google patched a critical Android 12 security flaw today. Retrieved 16 September 2022, from <https://www.phonearena.com/news/android-12-security-flaw_id138364>

Bumble - Privacy. (2022, June 21). Bumble. <https://bumble.com/en/privacy>

CVE-2021-39675 - OpenCVE. (2022). Retrieved 16 September 2022, from <https://www.opencve.io/cve/CVE-2021-39675>

CVE-2022-32893. (2022). Retrieved 15 September 2022, from <https://cve.report/CVE-2022-32893>

Gilbert, E. (2019 Antitrust and Commitment Issues: Monopolization of the Dating App Industry. New York University Law Review, 94(4), 862-898.

Levin, D. (2022). Face the Facts, or Is the Face Fact?: Biometric Privacy in Publicly Available Data. Fordham Intellectual Property, Media & Entertainment Law Journal, 32(4), 1010-1069.

Loh, M. (2022). Hackers can exploit a flaw in Apple's latest update to take full control of your iPhone and Mac. Retrieved 15 September 2022, from <https://www.insider.com/apple-security-update-flaw-hackers-control-iphones-2022-8>

Mozilla. (2021, February). \*Privacy Not Included review: Bumble. Mozilla Foundation; Mozilla Foundation. <https://foundation.mozilla.org/en/privacynotincluded/bumble/#:~:text=In%20November%202020%2C%20researchers%20found>

O’Gara, C. (2019, August 15). What Are the Consequences of a Biometric Data Breach? Www.secureworld.io. <https://www.secureworld.io/industry-news/biometric-data-breach-consequences>

Phone Arena. (n.d.). Samsung Galaxy S21 FE specs. <https://www.phonearena.com/phones/Samsung-Galaxy-S21-FE_id11702>

Qualcomm. (n.d.). Qualcomm snapdragon 888 5G mobile platform | Qualcomm. Wireless Technology & Innovation | Mobile Technology | Qualcomm. <https://www.qualcomm.com/products/application/smartphones/snapdragon-8-series-mobile-platforms/snapdragon-888-5g-mobile-platform>

Rachamalla, A. (2022). Oversharing in Social Media, A Biggest Security Risk - End Now Foundation. Retrieved 16 September 2022, from <https://www.endnowfoundation.org/oversharing-in-social-media-a-biggest-security-risk/>

Rizzi, C. (2022, January 10). Bumble Data Breach: Class Action Alleges Dating App Was Negligent in Handling Vast Amounts of User Info. Www.classaction.org. <https://www.classaction.org/blog/bumble-data-breach-class-action-alleges-dating-app-was-negligent-in-handling-vast-amounts-of-user-info>

Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure | Cyber.gov.au. (2022, May 17). Www.cyber.gov.au. <https://www.cyber.gov.au/acsc/view-all-content/advisories/russian-state-sponsored-and-criminal-cyber-threats-critical-infrastructure>

Samsung. (n.d.). Galaxy s21 FE 5g. Samsung au. <https://www.samsung.com/au/smartphones/galaxy-s21-5g/galaxy-s21-fe-5g/>

Stardust, Z., Gillett, R., & Albury, K. (2022). Surveillance does not equal safety: Police, data and consent on dating apps. Crime, Media, Culture. <https://doi.org/10.1177/17416590221111827>

Yang, B., Chen, R., Huang, K., Yang, J., & Gao, W. (2022). Eavesdropping User Credentials via GPU Side Channels on Smartphones. Pittsburgh: University of Pittsburgh. Retrieved from <https://sites.pitt.edu/~weigao/publications/asplos22.pdf>

# Appendices

Below are the appendices that have been referred to throughout the report.

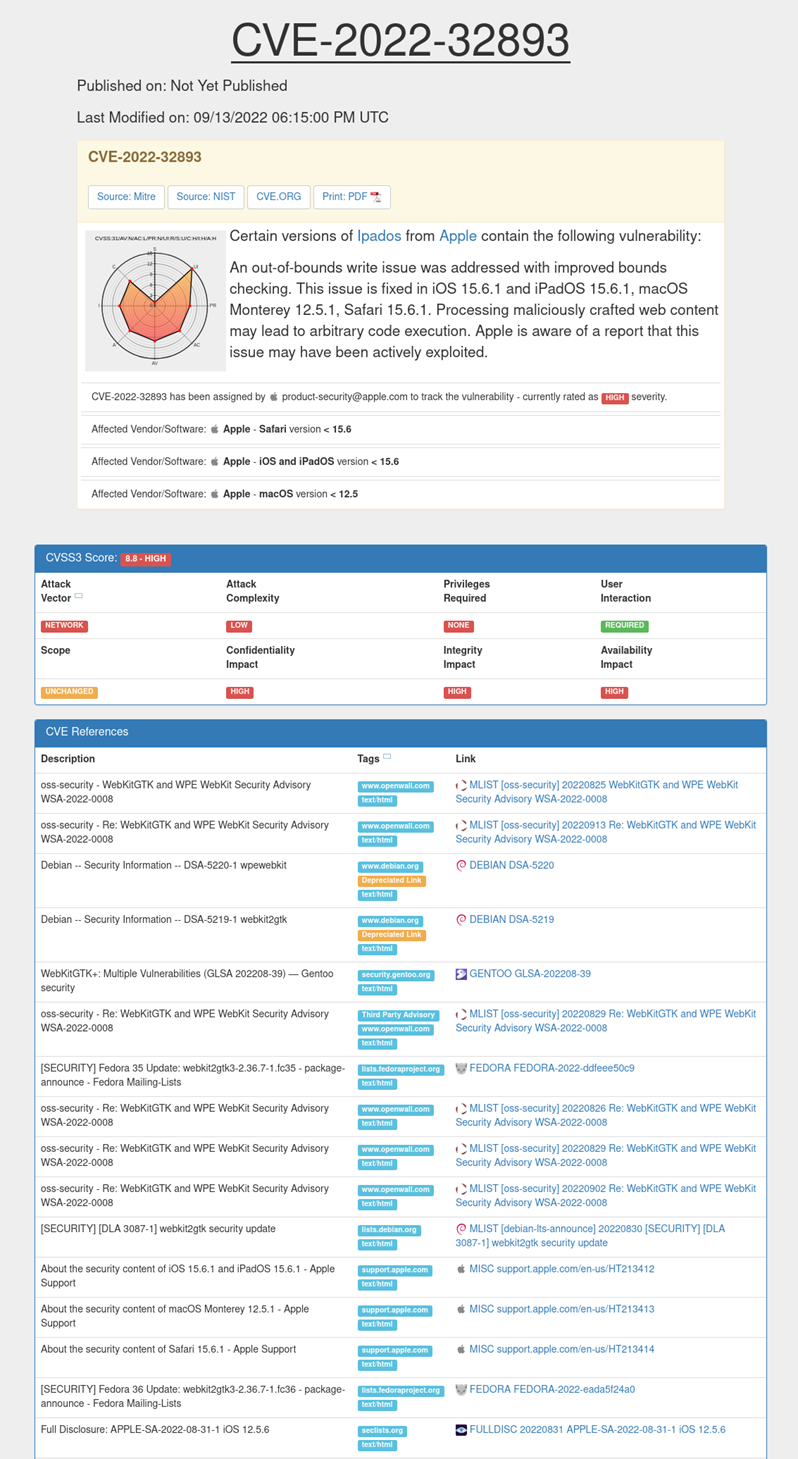
## Appendix 1

Text

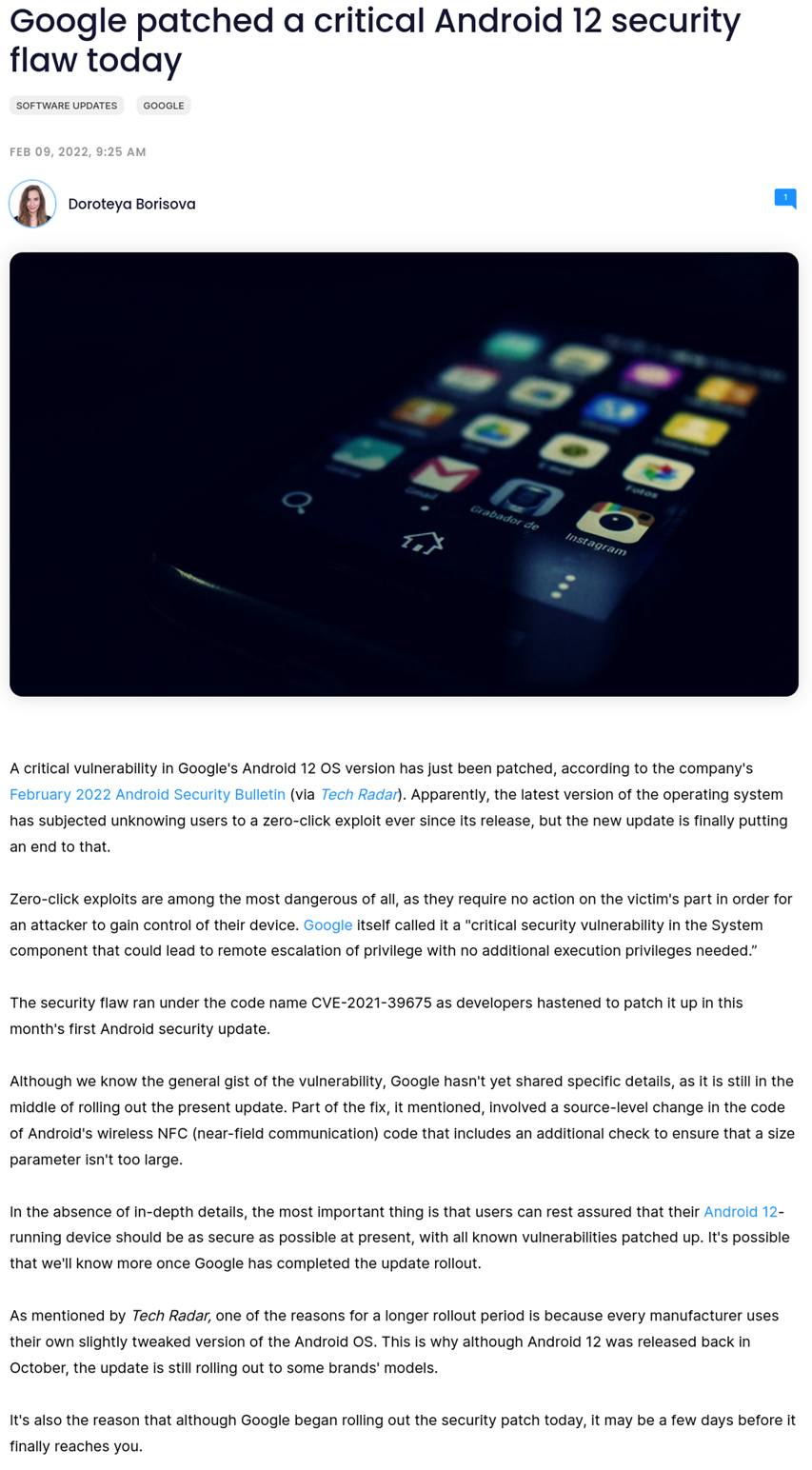
Description automatically generated

## 

## Appendix 2



## Appendix 3



## Appendix 4

## Appendix 5

## Appendix 6

## Appendix 7

A screenshot of a computer

Description automatically generated with medium confidence