|  |  |
| --- | --- |
| Course | Law & Ethics in Forensic Investigation |
| Assignment | Assignment 3 |
| Name of the Student | Maisha Khatoon |
| Student ID | 100899259 |

**Part-1:**

**Question-1**

Under Canadian law, not all material that has been unlawfully searched for or taken is automatically excluded from use as evidence. According to Section 24(2) of the Canadian Charter of Rights and Freedoms, such evidence is admissible. According to this clause, if admitting the evidence would tarnish the reputation of the legal system, it may be eliminated if it was collected in a way that violated the Charter rights of the accused.

There are, however, several exceptions to this rule. If it is determined that the evidence's removal will not affect the fairness of the trial or compromise the integrity of the judicial system, the court may use discretion and allow the evidence. When deciding whether the evidence should be omitted, factors such the gravity of the Charter breach, the impact on the accused's rights, and the effect on public faith in the judicial system are considered.

Reference- <https://laws-lois.justice.gc.ca/eng/Const/page-15.html#h-42>

**Question-2**

In Canada, the "reasonable expectation of privacy" test is used to assess whether a person has a reasonable expectation of privacy with respect to the data kept on their computer. For reasonable expectation of privacy to computers, the Supreme court of Canada has set a method called two-part test such as subjective expectation and objective reasonableness. The subjective expectation is predicated upon an individual’s subjective views and the corresponding measures undertaken to ensure the confidentiality of the information.

Business-issued computers and gadgets may have a lower expectation of privacy, particularly if employers warn workers that their computer activity may be monitored for business reasons. Even at work, workers may demand privacy for personal information like emails and papers.

At home, computers and gadgets are expected to be private. Section 8 of the Canadian Charter of Rights and Freedoms requires a warrant to examine a suspect's personal computer.

Reference- <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/7733/index.do>

**Question-3**

In the Canadian context, it is normally required for the government to get a search warrant to conduct a search and confiscate a suspect's computer. This need is set forth in Section 8 of the Canadian Charter of Rights and Freedoms, which guarantees certain rights and freedoms to everyone inside the country. Searches need a warrant when the person in question has reasonable expectations of privacy in their home or personal space, where the computer is. Besides this, exigent circumstances or permission do not allow warrantless searches.

Some examples of warrantless searches:

* Approval: If a person provides voluntary permission to a search, it may eliminate the need for a warrant. Nevertheless, it is essential that permission be provided willingly and comprehensively, with a clear awareness of the entitlement to decline.
* Incident to Arrest: Under certain conditions, when a suspect is legally apprehended, law enforcement officials may perform a restricted search of the vicinity immediately accessible to the suspect. This search is conducted with the objective of safeguarding the safety of the officers involved and preventing the potential destruction of evidence.
* The Plain View Doctrine allows for the seizure of incriminating information on a computer without a warrant if an officer is legally present in a particular area and visually perceives such material in plain view.

Reference- <http://www.canlii.org/en/on/onca/doc/2017/2017onca385/2017onca385.html>

**Question-4**

Upon the legitimate arrest of a suspect in Canada, it is permissible to confiscate and subsequently search a portable electronic device, subject to certain conditions:

* The electronic device is in the immediate possession of the individual who has been apprehended now of their apprehension.
* The scope of the search is constrained to the evidence pertaining to the crime that led to the arrest or to guarantee the safety of the officer.
* The search is carried out in accordance with the legal procedures associated with the process of arrest.

**Question-5**

Exigent circumstances pertaining to computers refer to emergency events that may require the execution of a search without a warrant. Several instances of cyber dangers include persistent cyber assaults, the potential for remote data deletion, the imminent loss of crucial evidence, the imminent risk of damage, and the presence of life-threatening cybercrimes. In some situations, it may be necessary for law enforcement authorities to promptly intervene to safeguard evidence or mitigate potential damage. Nevertheless, exigent circumstances serve as exemptions to the conventional need of obtaining a search warrant and are subject to rigorous examination by the judicial system to ascertain their compliance with the legal standards of urgency and indispensability.

**Question-6**

If investigators engaged in a computer search come across or have reason to believe that privileged material, such as attorney-client communications, is present, it is imperative for them to promptly cease the search. It is advisable for individuals to promptly tell their legal representative or the office of the prosecutor, take possession and ensure the security of the computer, and seek legal advice about the appropriate course of action in relation to the confidential material. The scope of the information may be assessed by an impartial third party, and it is imperative to maintain confidentiality and separate sensitive data from the investigating team. In the event of conflicts, investigators have the option to seek a court order as a means of resolving the matter. The appropriate management of confidential data is crucial to prevent legal ramifications and maintain the integrity of the inquiry.

**Question-7**

MLAT stands for Mutual Legal Assistance Treaty. The Mutual Legal Assistance Treaty (MLAT) is an internationally recognized agreement established between nations to facilitate collaborative efforts in legal affairs, with a specific focus on criminal investigations and prosecutions conducted across national borders. The acquisition of evidence, witness testimony, and legal aid across international boundaries is of utmost importance. The use of Mutual Legal Assistance Treaties (MLATs) serves to uphold principles of equitable judicial proceedings, uphold the principles of national sovereignty, and adhere to the norms and regulations of international law. These tools are used for the purpose of collecting evidence, obtaining witness testimonies, making extradition requests, exchanging data, and fostering collaboration with entities such as Interpol. The use of Mutual Legal Assistance Treaties (MLATs) has significant importance in the efforts to fight transnational crimes and provide a framework for equitable and efficient global justice.

**Question-8**

A computer security framework refers to a methodically organized collection of principles and directives used by businesses to effectively govern and augment the security measures implemented on their computer systems and networks. This document outlines optimal methodologies, established guidelines, and systematic protocols aimed at safeguarding information, thwarting unlawful entry, and mitigating hazards pertaining to cybersecurity.

The significance of a computer security framework is in its ability to detect and evaluate potential cybersecurity threats, protect sensitive data, verify adherence to regulatory requirements, and provide uniform security protocols across a company.

The Computer Security Framework is used by organizations to facilitate the development of cybersecurity policies, perform risk assessments, enforce security controls, provide training and awareness programs, and consistently analyze and enhance their cybersecurity processes.

Several computer security frameworks exist, such as the NIST Cybersecurity Framework, ISO/IEC 27001, CIS Controls, COBIT, and sector-specific frameworks as the Cybersecurity Framework for Financial Services. These frameworks provide businesses a methodical and uniform strategy to tackle cybersecurity concerns and safeguard data and systems.

**Part-2:**

**Question 1**

|  |  |  |  |
| --- | --- | --- | --- |
| Privacy Laws | Canadian | USA | EU |
| Privacy Legislation | The Personal Information Protection and Electronic Documents Act (PIPEDA) serves as the principal federal legislation in Canada that regulates privacy issues inside the private sector. Various provinces may possess distinct privacy laws. | The United States of America currently does not possess a one, all-encompassing federal privacy legislation. Privacy restrictions are tailored to certain sectors, such as the Health Insurance Portability and Accountability Act (HIPAA) which governs health data, and the Gramm-Leach-Bliley Act (GLBA) which pertains to financial data. Certain states have implemented their own privacy legislation, such as the California Consumer Privacy Act (CCPA) and the Virginia Consumer Data Protection Act (CDPA). | The European Union (EU) has implemented the General Data Protection Regulation (GDPR), a comprehensive regulatory framework that encompasses all member nations within the EU. Furthermore, it is worth noting that individual member states has the authority to enact their own national privacy legislation that complements the General Data Protection Regulation (GDPR). |
| Right to Private Action | In the Canadian context, it is often observed that private persons lack the legal entitlement to initiate legal proceedings for privacy breaches under the Personal Information Protection and Electronic Documents Act (PIPEDA). The Office of the Privacy Commissioner of Canada is responsible for the management of complaints and the conduct of investigations pertaining to privacy matters. | In the United States, there is currently no comprehensive statutory provision that guarantees individuals the right to pursue private legal action in cases of privacy infringement. Nevertheless, some state laws, such as the California Consumer Privacy Act (CCPA) and particular legislation applicable to certain sectors, provide consumers the privilege to initiate legal action under specified conditions in the event of data breaches or unlawful access to their personal information. | Within the European Union, people possess the entitlement to pursue legal recourse and initiate private litigations against data controllers and processors in cases of privacy infringements as stipulated by the General Data Protection Regulation (GDPR). Individuals have the option to file complaints with their respective national data protection authority (DPA) in order to seek non-judicial remedies. |
| Breach Notification | Under the Personal Information Protection and Electronic Documents Act (PIPEDA), enterprises are obligated to notify the Privacy Commissioner and affected persons of noteworthy data breaches, contingent upon the level of potential damage. | The United States of America currently does not possess a singular, all-encompassing federal legislation pertaining to breach notification. In contrast, the standards for breach notification differ across states. Numerous states have enacted individual breach reporting laws, exhibiting variations in terms of temporal parameters, extent of coverage, and triggers for notification. | The General Data Protection Regulation (GDPR) stipulates that organizations must notify the appropriate Data Protection Authority (DPA) within 72 hours of becoming aware of a data breach, unless it is determined that the breach is unlikely to pose a harm to the rights and freedoms of persons. Notification to data subjects is required where a breach is anticipated to pose a significant danger to their fundamental rights and freedoms. |
| Privacy Commissioner | The Privacy Commissioner of Canada is an autonomous ombudsman responsible for the oversight of privacy-related issues and the investigation of complaints in accordance with the Personal Information Protection and Electronic Documents Act (PIPEDA). The Commissioner has regulatory authority and could provide recommendations that are not legally obligatory. | The United States of America currently does not possess a centralized government privacy regulatory body. In contrast, privacy enforcement within specialized sectors is managed by other federal organizations, such as the Federal Trade Commission (FTC) and the Department of Health and Human Services (HHS). The Federal Trade Commission (FTC) plays a crucial role in the enforcement of privacy regulations for corporations. | Each member state of the European Union (EU) has its own autonomous Data Protection Authority (DPA), which assumes the responsibility of upholding the General Data Protection Regulation (GDPR) and other privacy legislations specific to the respective country. The European Data Protection Board (EDPB) is responsible for offering advice and ensuring the uniform implementation of the General Data Protection Regulation (GDPR) across the European Union (EU). |
| Cross-Border Data Transfers | The Personal Information Protection and Electronic Documents Act (PIPEDA) permits businesses to engage in the cross-border transmission of personal data, provided that such transfers have a legitimate purpose and are accompanied by appropriate safeguards. The cross-border data transfer regulations of the Personal Information Protection and Electronic Documents Act (PIPEDA) are in accordance with the adequacy judgments made by the European Union (EU). | The United States of America lacks a unified and comprehensive framework for data transport. In the context of EU-US transfers, businesses have the option to use Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), or other procedures that have been officially sanctioned by the European Union (EU). The Schrems II judgement, which was issued recently, has imposed more stringent criteria on the transfer of data from the European Union to the United States. | The General Data Protection Regulation (GDPR) imposes limitations on the transfer of personal data to countries that are situated outside the European Union (EU). The transmission of data to nations that have received an adequacy judgment from the European Union Commission is possible. When companies lack sufficient sufficiency, they have the option to use Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), contingent upon an evaluation of the data protection legislative framework in the jurisdiction of data transfer. Derogations for certain circumstances are also available. |

1. Privacy Legislation

* Practical Advantages: The extensive GDPR of the EU offers a uniform framework for all member states, simplifying compliance procedures for businesses operating in the EU. In contrast, Canada's PIPEDA gives provinces considerable latitude to modify legislation to suit their unique requirements.
* Operational Disadvantages: For businesses operating throughout many areas of Canada, adhering to numerous provincial legislations may be expensive and operationally challenging. A patchwork of laws may develop from the absence of a single federal privacy legislation in the USA, making compliance more difficult for organizations with nationwide operations.
* Societal Advantages: The GDPR's continental reach means that all EU citizens, regardless of where they live inside the EU, are given uniform privacy rights. In Canada, both federal and provincial regulations may be tailored to the requirements and demographics of an area, improving privacy protection for citizens of different regions.

1. Right to private action

* Practical Advantages: In the EU, the right to judicial remedies gives people legal redress for privacy abuses, pushing businesses to give data protection a high priority. In the USA, allowing private activities in certain states gives citizens the ability to uphold their constitutional rights to privacy.
* Operational Disadvantages: The lack of a universal right to private action in Canada may restrict individual redress against privacy infractions and increase dependence on the Privacy Commissioner's enforcement operations.
* Societal Advantages: Because people have greater control over their privacy rights and may hold companies responsible, the availability of private actions in the EU and several US states can help to strengthen social trust.

1. Breach Notification

* Practical Advantages: The GDPR's standard 72-hour breach notification period improves efficiency and uniformity within the EU and makes breach reporting for businesses that operate in several member states simpler. States may be able to customize notification requirements to their unique situations thanks to the decentralized system in the USA.
* Operational Disadvantages: Organizations operating across several states may have compliance challenges due to the USA's inconsistent breach reporting rules.
* Societal Advantages: By requiring rapid disclosure of data breaches, the GDPR's stringent breach notification standards increase openness and confidence in society. The amount of openness supplied to impacted persons may vary depending on state legislation in the USA.

1. Privacy Commissioner

* Practical Advantages: Canada's independent privacy commissioner is well-equipped to deal with privacy-related issues and grievances nationwide. In the USA, the existence of several federal entities involved in privacy enforcement may lead to jurisdictional overlap and associated inefficiencies.
* Operational Disadvantages: Because there is no one federal privacy authority in the United States, different enforcement strategies and interpretations may be used.
* Societal Advantages: Independent privacy commissioners in Canada and the EU, as well as individual data protection authorities, assure specialized supervision and uniform implementation of privacy laws, bolstering public trust.

1. Cross-Border Data Transfers

* Practical Advantages: The GDPR's adequacy determinations make cross-border data transfers between the EU and recognized nations simpler and less onerous to comply with. Utilizing SCCs and BCRs in the USA permits data flows between the EU and the USA.
* Operational Disadvantages: The Schrems II decision increased the standards for EU-US data transfers, thereby complicating and raising the cost of operations for firms.
* Societal Advantages: Adequacy rulings in the EU and adherence to certain procedures in the USA support data protection during cross-border transfers, protecting people's right to privacy.

**Question 2**

In data protection, privacy and security are different but typically intertwined.

Privacy is like people have the right to determine how their personal data is collected, utilized, shared, and preserved. It protects sensitive and personal data from illegal access, allows people to make informed data usage decisions, and prevents data abuse. Privacy is a human right and important to trust between people and organizations.

On the other hand, Security protects data, systems, and information against unauthorized access, misuse, theft, or damage. Technical, administrative, and physical controls protect data and assure its confidentiality, integrity, and availability. Encryption, firewalls, access restrictions, authentication, and cybersecurity are security measures.

Because appropriate security measures are necessary to safeguard an individual's privacy, privacy and security are closely related. Data security reduces the possibility of breaches or illegal access, which might result in privacy violations. Strong security measures make sure that personal data cannot be accessed, changed, or shared without permission, preserving its confidentiality and integrity.

Privacy or security is subjective and context dependent. Privacy and security pose unique challenges:

Privacy Issues:

* Rapid technological advancements: new data collection and processing methods make privacy issues difficult to manage.
* Cross-Border Data Flows: In a globalized society, maintaining privacy and complying with foreign privacy standards may be difficult.
* Balancing corporate Interests: Businesses acquire and utilize data for many reasons, and balancing corporate interests and privacy rights may be difficult.

Security issues:

* Constant Threats: Cyber threats and assaults evolve, making it difficult to keep ahead of vulnerabilities and secure data.
* Human Error: Weak passwords, misconfigurations, and accidental data disclosure cause many security breaches.
* Resource Limits: Smaller firms may struggle to fund comprehensive security measures.

Data protection requires privacy and security. Both demand continual work, alertness, and a proactive attitude to protecting data and respecting people' rights, but the problems differ. To comply with rules and preserve user confidence, organizations must constantly evaluate and enhance their privacy and security procedures.

**Question 3**

<https://decisions.ipc.on.ca/ipc-cipvp/phipa/en/item/468594/index.do>

a) Summary-The investigation report of the Privacy Commissioner that was chosen is the one that can be found by clicking on the above-mentioned link. Within the scope of this report is an inquiry conducted in accordance with the Personal Health Information Protection Act (PHIPA) in the province of Ontario, Canada.

b) Discussion- The Privacy Commissioner of Ontario is looking into a complaint that was filed under the Personal Health Information Protection Act (PHIPA). This act is what controls the privacy of individuals' personal health information in the Ontario health care system. It is very probable that the study addresses concerns about the acquisition, use, and disclosure of patients' personal health information by organizations and providers of medical treatment.

The following topics are covered in depth in the reports issued by the Privacy Commissioner:

Breach of Privacy It is quite probable that an investigation will be conducted in the report to determine whether there was a violation of the individual's privacy rights under PHIPA. This might involve incorrect management of sensitive data, unlawful access to personal health information, or inappropriate sharing of information.

Compliance with PHIPA: The purpose of the inquiry was to determine whether the health care provider or organization in question complies with the mandates that are spelled out in PHIPA. This contains regulations relating to obtaining permission, protecting personal health information, and engaging in appropriate procedures about dissemination.

Enforcement Actions: Depending on the findings, the Privacy Commissioner may suggest enforcement actions or remedies to resolve the identified privacy infractions. These might include fines, remedial measures, or policy changes.

c) Critique- Reports from privacy commissioners are essential for upholding privacy rules and protecting people's personal data. They encourage compliance with applicable privacy laws and hold corporations responsible for their data management procedures.

The length of time required for investigations and the eventual settlement of cases is one possible criticism of the report. Individuals' private rights may be severely jeopardized by privacy violations, thus quick action is often required to safeguard them. Investigation and resolution delays might make it more difficult for people to get timely redress and could reduce public confidence in the privacy enforcement process.

Additionally, the efficiency of the suggested enforcement methods could come under examination. The legislative structure of the area and the resources available for enforcement may determine the Privacy Commissioner's capacity to impose fines or other remedies. To guarantee effective enforcement of privacy legislation, the Privacy Commissioner's office must have enough power, resources, and support from relevant parties.

The investigation reports of the Privacy Commissioner are fundamental for upholding accountability, openness, and adherence to privacy legislation. They support the continual improvement of privacy safeguards in the relevant jurisdiction by assisting companies in improving their data practices and by assisting with the identification of privacy concerns.

**Question 4**

A project, effort, or system that includes the gathering, using, or management of personal information may go through a privacy impact assessment (PIA), which is a methodical procedure used to identify and evaluate the possible privacy risks and implications. A PIA's main objective is to make sure that privacy concerns are included into the project's planning and execution, assisting companies in recognizing and proactively addressing any possible privacy problems.

How to Conduct a PIA:

* Start the PIA by determining the project or system that needs one and the parameters of the evaluation.
* Data Mapping: Identify the categories of personal data that are being gathered, handled, and kept, as well as their sources and receivers.
* Assess the project's possible privacy concerns by considering elements including data sensitivity, the goal of data processing, and the scope of data collecting.
* Verify that the project complies with all applicable privacy laws and regulations.
* Privacy protections: To reduce possible dangers and defend people's privacy, choose and put into practice the best privacy protections.
* Engage stakeholders, especially those whose data will be handled, to get their opinions and resolve any issues.
* Documentation: Keep a record of the PIA procedure, results, and any suggestions for mitigating risks.

When should PIAs be performed:

When implementing new programs, initiatives, or projects that handle the processing of personal data, PIAs must be carried out. They are particularly important in the following circumstances:

* Anytime a new system or project that deals with personal data is created.
* When significant modifications are made to current procedures or systems that influence privacy.
* When personal data will be shared with other parties or utilized for new purposes.
* Data sharing initiatives: When personal information is given to partners or groups outside the company.
* Projects containing sensitive data or extensive data processing fall under the category of high-risk processing.

Results and Recommendations of a PIA:

A well executed PIA may uncover a variety of conclusions, suggestions, and hazards, including:

* Privacy issues: The project's weaknesses and possible privacy issues are identified.
* Legal Compliance: Evaluation of how well the project complies with all relevant privacy laws and rules.
* Data Protection Gaps: The location of potential weak spots in privacy measures.
* Privacy protections: best practices and recommendations for adopting privacy protections.
* Data minimization: Determining if the amount of data acquired is sufficient for the intended goal.
* Gathering input from stakeholders, including data subjects, and responding to their issues.
* Consent and Transparency: Suggestions for enhancing consent and getting people's informed consent.
* Impact on People: Evaluation of how the project could affect people's freedoms and rights to privacy.

Organizations may analyze and reduce privacy risks using PIAs, which also help to assure the ethical and responsible treatment of personal data. They are compliant with regulatory standards and industry best practices while promoting openness, accountability, and trust with data subjects.