



OFFICE OF THE INFORMATION
AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

Report A-2020-019

September 16, 2020

Memorial University of Newfoundland

Summary:

The Complainant requested from Memorial University of Newfoundland (“Memorial”) information relating to the Linux file server, a list of employees with administrator privileges, and the Computer System Administration Policy. Memorial provided access to some of the records, but withheld some records pursuant to section 31 (disclosure harmful to law enforcement) of the *Access to Information and Protection of Privacy Act, 2015* (“ATIPPA, 2015”) as disclosure would reveal the arrangements for the security of a computer system. Memorial advised that some of the Linux file information was outside its custody and control and that the Computer System Administration Policy no longer existed. The Complainant alleged that Memorial inappropriately withheld the information under section 31. The Complainant also challenged Memorial’s position that it did not have custody or control of some of the records, and alleged that Memorial failed in its duty to assist him by failing to conduct a reasonable search for records. The Commissioner found that the settings and configuration of the Linux server were exempt from disclosure under section 31(1)(l) but recommended that Memorial University of Newfoundland disclose to the Complainant the list of individuals with administrative privileges.

Statutes Cited:

[Access to Information and Protection of Privacy Act, 2015](#), S.N.L. 2015, c. A-1.2, sections 13, 31.

Authorities Relied On:

[Canada \(Information Commissioner\) v. Canada \(Commissioner of the Royal Canadian Mounted Police\), 2003 SCC 8](#); “[Guide to General Server Security](#)”, National Institute of Standards and Technology; NL OIPC Reports [A-2020-006](#); [A-2009-007](#); [A-2010-008](#); [A-2019-030](#).

I BACKGROUND

- [1] In September 2019, during an upgrade process, the files stored on the Complainant's office computer, a Memorial University ("Memorial") asset assigned to the Complainant, were moved temporarily to a drive on another server at Memorial University. The Complainant became suspicious that someone may have accessed sensitive personal files which had been stored on that computer. The Complainant had previously made a request to Memorial for records relating to Memorial's computer file system under the *Access to Information and Protection of Privacy Act, 2015* ("ATIPPA, 2015") which resulted in the issuance of Report A-2020-006. This Report flows from the same series of events.
- [2] The Complainant filed the access request under *ATIPPA, 2015* which is the subject of this Report as follows:
1. *The type and configuration of the Linux file server to which the [named file] folder was migrated between September 6 and September 12, 2019.*
 2. *Settings for log level, vfs objects, full audit of the Samba suite on the Linux file server to which the [named file] folder was migrated between September 6 and September 12, 2019.*
 3. *The list of individuals with administrator privileges to view, copy, delete and change files and folders on the Linux file to which the [named file] folder was migrated between September 6 and September 12, 2019.*
 4. *The Computer System Administration Policy.*
- [3] Memorial provided the Complainant with some information about the type of file server, but refused access to the configuration of the server and to the list of individuals with administrator privileges pursuant to section 31 (disclosure harmful to law enforcement) as disclosure would "reveal the arrangements for the security of a computer system". Memorial also advised the Complainant that records containing the settings were not in the custody or control of Memorial.
- [4] Memorial also informed the Complainant that there is no "Computer System Administration Policy" and that all of Memorial's approved policies are located on Memorial's website.

- [5] The Complainant was not satisfied with Memorial's response and filed a complaint with this Office.
- [6] As informal resolution was unsuccessful, the complaint proceeded to formal investigation in accordance with section 44(4) of *ATIPPA, 2015*.

II PUBLIC BODY'S POSITION

- [7] Memorial provided the Complainant with the type of server in its final response to the request. During its search, Memorial located a record responsive to the request for configuration. Memorial asserts that in order to protect its information assets and infrastructure, it withheld the configuration document pursuant to section 31(1)(l). It is Memorial's position that disclosure of such information "provides an attacker with information that allows them to understand how a server/application is setup, what is enabled/disabled, versions of operating systems/software, etc."
- [8] Memorial states that even within the University, server configuration information is held as confidential and only System Administrators should have access to this type of information: "Disclosing this to the public provides an attacker with intelligence on how to navigate and attack an environment, exploit known vulnerabilities, etc."
- [9] Memorial puts forth a similar argument for withholding the names of the individuals with administrator privileges pursuant to section 31(1)(l):

Cyber threats are advancing and social engineering attacks are more sophisticated than ever. In order to protect the University's Information asset/infrastructure, we cannot release the names of the individuals who have escalated administrative access. Releasing such information places the University at an escalated risk, for example making the individuals subject to targeted social engineering attacks or impersonation attacks.

- [10] Social engineering is the act of tricking someone into divulging information or taking action, usually through technology. The idea behind social engineering is to take advantage of a potential victim's natural tendencies and emotional reactions. For example, a social

engineer, can attack by posing as a technical support person to trick an employee into divulging their login credentials.

[11] With regard to the request for settings, Memorial submits that the “settings” do not fall under the category of “record” as set out in section 2(y) of *ATIPPA, 2015*:

(y) "record" means a record of information in any form, and includes a dataset, information that is machine readable, written, photographed, recorded or stored in any manner, but does not include a computer program or a mechanism that produced records on any storage medium;

[12] Memorial states that “appliance settings” are a computer program, part of the inner workings of the operating system that make the program work. Memorial does not believe a record could even be produced of the settings.

[13] Alternatively, Memorial also submits that the settings for the server are not in the University’s custody and control. Using the definition of custody and control in the University’s Information Request policy and the criteria in Ontario Order MO-2750, Memorial states that the server is a prepackaged application purchased from IBM, who configures the backend server. The settings are the technical backend in support of the vendor application and, therefore, are not a core function of the institution. Memorial does not have physical possession of the settings, nor are they held by an officer or employee of Memorial. Memorial does not have a right to possession of these settings, nor does it have the authority to regulate the content or use of the settings. They assert Memorial would have to engage with the server provider to even alter these settings.

[14] Finally, Memorial advised the Complainant that the “Computer System Administration Policy” does not exist. Memorial notes that there was a historical reference to the “Computer Systems Administration Policy” in one of Memorial’s current policies (Limitation of Liability with Respect to Computing Facilities). Memorial submits that in 2006, the University undertook a review of all policies. The Computer System Administration Policy was not carried forward at that time, is no longer in force, and was unable to be located.

[15] Memorial will request that the historical reference be removed from the current policy.

III COMPLAINANT'S POSITION

[16] The Complainant argues that Memorial has custody or control of the settings of the file server. He states that the settings relate to the operation of Memorial's Information Technology services. The server is located in the datacenter on campus and all Memorial's servers are administered by IT services. The Complainant maintains that the settings are specific to a particular server and result from conscious choices of the system administrators. As such, the Complainant asserts that Memorial has custody or control of the records.

[17] With regards to the type and configuration of the Linux file server, the Complainant claims that the disclosure would not reveal security arrangement of a computer system. The Complainant references OIPC Reports A-2009-007 and A-2010-008, which found that no evidence or explanation had been put forth to demonstrate how the disclosure of information would reveal arrangements for the security of the property or system. The Complainant alleges that, as in these previous Reports, Memorial has also not provided any demonstrable evidence in this situation either.

[18] The Complainant submits that Memorial's argument regarding the release of the names of the System Administrators pursuant to section 31(1)(l) has no merit. He cites *Canada (Information Commissioner) v. Canada (Commissioner of the Royal Canadian Mounted Police)*, 2003 SCC 8 as an analogous situation, noting that the Supreme Court of Canada found that disclosure of information relating to the position or functions of law enforcement would not make them vulnerable to 'social engineering' or harm.

[19] In addition, the Complainant asserts that Memorial has disclosed the names of individuals with administrative privileges on previous occasions, including to him, noting two specific employees in particular. The Complainant argues that there is no evidence that this disclosure has made these individuals vulnerable to attempts at social engineering.

[20] The Complainant submits that Memorial failed to meet its duty to assist him in his request because it failed to locate the Computer System Administration Policy. The Complainant points out that Memorial's claim that the record does not exist is "refuted by the material fact that the Computer System Administration Policy is cited or referred to in a number of official university records." The Complainant notes that one specific policy referencing the Computer System Administration Policy has been in effect since March 6, 2018.

[21] He asserts that "this policy, to all appearances, outlines procedures for accessing the contents of user accounts, including their files stored in the domain (the P: drive)." The Complainant wishes to determine whether the individual who he claims accessed his files on September 13, 2019 acted in full conformity with the policy. He states that the fact that the policy is not posted is not material. He further notes that no other policy cited in the response from Memorial pertains to administration of university file and email servers.

IV DECISION

Settings and Configuration of the Linux Server

[22] Settings are a crucial part of an operating system – in this case, the operating program of the Linux server. Although the settings can be accessed through a computer or set of computers to view, they are considered the "logic behind the scenes" that make the service work – in essence, a core component of the computer program.

[23] The configuration of files means the arrangement or set-up of hardware or software that make up a computer system. Operating systems can be configured to each organization or person's requirements.

[24] Section 8(1) establishes a right of access to "a record in the custody or under the control of a public body" and section 2(y) states that:

a "record" means a record of information in any form, and includes a dataset, information that is machine readable, written, photographed, recorded or stored in any manner, but does not include a computer program or a mechanism that produced records on any storage medium

[25] The definition of record explicitly notes that computer programs are not considered to be records under *ATIPPA, 2015*. As settings make up part of a computer program, this Office therefore finds that the Complainant does not have a right of access to the settings of the server.

[26] Regarding the decision to withhold the configuration document, the configuration document specifically lays out what controls, processes, and protocols are enabled within Memorial's server. Section 31(1)(l) provides:

31. (1) The head of a public body may refuse to disclose information to an applicant where the disclosure could reasonably be expected to

(l) reveal the arrangements for the security of property or a system, including a building, a vehicle, a computer system or a communications system;

[27] Further, the National Institute of Standards and Technology (NIST) sets out standards and recommendations for technological programs, developments, and policies. In its "Guide to General Server Security, NIST SP 800-123", NIST advises:

Organizations should commit to the ongoing process of maintaining the security of servers to ensure continued security. Maintaining a secure server requires constant effort, resources, and vigilance from an organization. [...] Maintaining the security of a server will usually involve the following actions:

Configuring, protecting, and analyzing log files on an ongoing and frequent basis

Backing up critical information frequently

Establishing and following procedures for recovering from compromise

Testing and applying patches in a timely manner

Testing security periodically

[28] Under "5.2 Configuring Access Controls", NIST recommends:

The proper setting of access controls can help prevent the disclosure of sensitive or restricted information that is not intended for public dissemination.

Typical files to which access should be controlled are as follows:

Application software and configuration files

Files related directly to security mechanisms:

- Password hash files and other files used in authentication

- Files containing authorization information used in controlling access

*– Cryptographic key material used in confidentiality, integrity, and non-repudiation services
Server log and system audit files
System software and configuration files
Server content files.*

[29] To disclose the settings or configuration of the server as requested by the Complainant would in essence reveal the security arrangements of the computer system, therefore both are exempt from disclosure under section 31(1)(l).

System Administrator Names

[30] Regarding Memorial's submissions relating to social engineering or the use of system administrator identities by threat actors with malicious intent, this Office does not find that there is sufficient evidence to support the probability that the employees or the institution will be exposed to harm. This Office recognizes that Memorial faces a significant number of cybersecurity threats on a daily basis. However, the knowledge of the names of the individuals with administrative privileges alone does not heighten those threats or make these individuals more vulnerable to impersonations. In fact, as privileged account holders, these individuals should have higher than normal protections related to their accounts to ensure the safety of their work and systems that they oversee. This Office does not find that disclosure of the names of system administrators would reveal system arrangements of a computer system pursuant to section 31(1)(l).

Computer System Administration Policy

[31] While the Complainant believes that the Policy that he requested covers certain subjects, that is speculation. The Appropriate Use of Computing Resources policy and the Electronic Data Security policy are two examples of relevant Memorial policies regarding account access by those other than the user, and these policies are available online.

[32] Further, Memorial provided sufficient explanation regarding the lack of responsive records regarding the Computer System Administration Policy. Memorial engaged several employees from the Office of the Chief Information Officer and other Departments to search for this specific policy. The scope of search included email, electronic files and file shares, file

cabinets, paper and hand written notes, in-person consultations, and searching Memorial's website.


[33] The fact that the policy is referenced in a newer policy is not evidence that the policy currently exists. The length of time since this policy has been in place, combined with the fact that Memorial's retention period has also passed, satisfies this Office that a reasonable search was conducted. As we have found that a reasonable search has been conducted, this Office also finds that Memorial fulfilled its duty to the Complainant in responding to the request.

V RECOMMENDATIONS

[34] Under the authority of section 47 of *ATIPPA, 2015*, I recommend that Memorial University of Newfoundland disclose to the Complainant the list of individuals with administrative privileges. I further recommend that Memorial continue to withhold records relating to the configuration and settings of the Linux file server.

[35] As set out in section 49(1)(b) of *ATIPPA, 2015*, the head of Memorial University must give written notice of his or her decision with respect to these recommendations to the Commissioner and any person who was sent a copy of this Report within 10 business days of receiving this Report.

[36] Dated at St. John's, in the Province of Newfoundland and Labrador, this 16th day of September 2020.



Michael Harvey
Information and Privacy Commissioner
Newfoundland and Labrador