Protection de la vie privée en contexte de télétravail et de retour au travail : à quoi porter attention?

Sébastien Gambs
Chaire de recherche du Canada sur l'analyse respectueuse de la vie privée et éthique des données massives
Université du Québec à Montréal (UQAM)

gambs.sebastien@uqam.ca

25 septembre 2020

Plan de la présentation

1. Enjeux généraux de la vie privée (Sébastien)
2. Sécurité informatique en télétravail (Marc-Olivier)
3. Traçage et surveillance dans le cadre du télétravail (Sébastien)
4. Surveillance et retour au travail (Marc-Olivier)

Enjeux généraux de la vie privée (partie 1)

Respect de la vie privée

- Le respect de la vie privée est un droit fondamental de tout individu :
  - Déclaration universelle des droits de l'homme à l'assemblée des nations unies (article 12), 1948.
  - Loi sur la protection des données personnelles dans le secteur privé, Québec (actuellement en processus de révision sous le nom de loi 64).
  - Règlement européen sur la protection des données, RGPD (voté en 2016, devenu effectif en mai 2018).

- Risques : collecte et utilisation des traces numériques et des données personnelles à des fins frauduleuses.

Principes fondamentaux de la protection de la vie privée -1

Minimisation des données :

- Seule l'information nécessaire pour une finalité particulière devrait être collectée/utilisée (et pas plus).
- Difficile à juger dans un contexte de télétravail ou de retour au travail où l'employeur va justifier la collecte par rapport à la mesure de la productivité, la protection de la propriété intellectuelle ou encore assurer la santé pour ses employés.

Souveraineté des données :

- Les données liées à un individu lui appartiennent, il devrait pouvoir contrôler comment elles sont disséminées, utilisées et dans quel but.
- Difficile à réaliser dans un monde ubiquitaire.

Principes fondamentaux de la protection de la vie privée - 2

- Transparence : le système ne doit pas être considéré comme une boîte noire dans laquelle l'individu doit avoir une confiance aveugle.
- Exemple : consultation et inspection de son propre profil.
- Consentement libre et éclairé : avant de collecter les données personnelles d'un individu, il faut lui demander son autorisation et lui expliquer comment elles seront utilisées.
- Imputabilité : l'entité qui héberge les données personnelles doit les sécuriser au meilleur de ses moyens, et le cas échéant peut être tenue responsable (par exemple devant un juge) d'un bris de vie privée si elle manque à ses obligations.

Bouleversement des habitudes en contexte de pandémie

- Bouleversement abrupt des habitudes de travail (à la fois pour le télétravail et le retour au travail) qui amènent les employeurs à déployer de nouvelles technologies pour s'adapter au contexte.
- Exemple (La Presse, 15 septembre 2020) :

  > *[. . .] À Jean de la Mennais, un établissement privé de la Rive-Sud, si un jeune a des symptômes de COVID-19, il suit ses cours à distance. Des caméras ont été installées dans les classes pour que les profs puissent se filmer en enseignant. [. . .]*

- Plus de frontière claire entre la maison et le travail, pression d'ouvrir l'accès à son domicile pour garder son emploi.

Risques émergents pour la vie privée et la sécurité

- Contexte urgence ⇒
  manque de directives et régulations pour encadre les nouvelles pratiques ⇒
  risques importants pour la vie privée des employés

- Exemples de risques :
  - Augmentation des risques de sécurité.
  - Traçage et surveillance des employés, parfois à leur insu.
  - Collecte et partage d'informations personnelles, incluant des nouvelles informations telles que les données de santé.

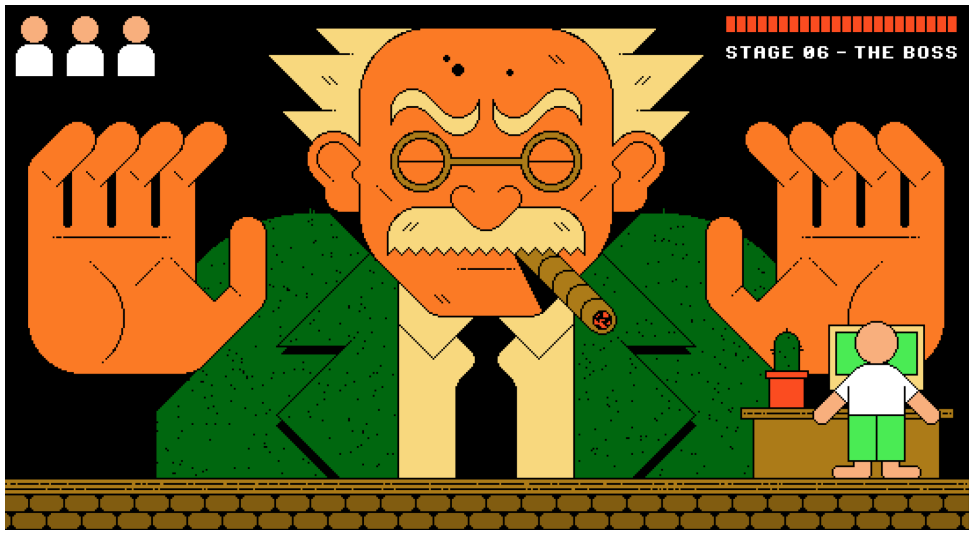
Exemple de nouvelle problématique : collecte des données de santé

- La pandémie a amené à la collecte de données de santé afin de pouvoir évaluer le niveau de risque d'un employé.
- Risques spécifiques :
  - Partage direct d'informations avec les employeurs (par exemple sur le résultat de tests de santé) sans forcément respecter le consentement de l'utilisateur.
  - Les données collectées sont considérées par les compagnies comme n'étant pas des données de santé ce qui diminuent les attentes en termes de vie privée et sécurité.
  - Exemple : la législation HIPAA (*Health Insurance Portability and Accountability Act*) aux USA demandent des contraintes beaucoup plus fortes sur la sécurité et la vie privée des données collectées pour les données personnelles "standards".

Traçage et surveillance dans le cadre du télétravail (partie 3)

Patrongiciels (1/2)

- Patrongiciel (*bossware* en anglais) : logiciel résident sur l'ordinateur portable ou le téléphone intelligent et ayant les privilèges pour collecter beaucoup d'informations sur ce qui se passe sur l'appareil.



- Finalité première : suivre à distance les activités et la productivité d'un employé.

Patrongiciels (2/2)

- Existait avant la pandémie mais a connu un gain important de popularité avec le confinement et la généralisation du télétravail.

Bosses Panic-Buy Spy Software to Keep Tabs on Remote Workers

Phones are ringing off the hook at companies providing a bit of Big Brother.

By **Polly Mosendz** and **Anders Melin**
27 mars 2020 07:00 HAE

The email came from the boss.

We're watching you, it told Axos Financial Inc. employees working from home. We're capturing your keystrokes. We're logging the websites you visit. Every 10 minutes or so, we're taking a screen shot.

- Au delà des enjeux de vie privée et de sécurité semble éthiquement injustifiable si cela est installé sans le consentement de l'employé.
- Finalité secondaire : accumuler des preuves pouvant servir à justifier un licenciement.

Surveillance d'activités

- Type le plus commun de patrongiciel.
- Données collectées :
  - Garde un enregistrement de toutes les applications utilisées par un travailleur ainsi que de son comportement de navigation.
  - Peut aussi inclure les destinataires des courriels ou des messages, ainsi que les méta-données associées comme le titre du courriel, ou encore les posts faits sur un média social.
  - Potentiellement enregistre aussi la vitesse de frappe ou encore le nombre de clicks comme indicateurs de "productivité".
- Objectif : fourni cette information de manière agrégée et visuelle à l'employeur pour avoir une vue haut niveau de ce que fait l'employé.

Logiciel de surveillance d'activités Interguard (1/3)

Employee Monitoring Software

InterGuard's employee monitoring software lets you track all employees activity from any endpoint - even when they **work from home**. Monitoring employee computer activity helps you proactively identify which employees are being productive and how much time is spent idle or on non-work related tasks. Set up "suspicious behavior alerts" and get a remote view of the employee's desktop.

Coronavirus (covid-19) & Remote Employee Monitoring

Even before the outbreak of Coronavirus (covid-19) made working-from-home the new normal for the global workforce, many business were already shifting to a "flexible workplace" by allowing teleworking, remote work and work-from-home arrangements. While allowing remote employees to work from home has many benefits, teleworking does come with a new set of challenges that did not exist when employees worked exclusively from the office. To overcome these challenges, businesses have chosen InterGuard as the best employee monitoring software for monitoring remote workers. InterGuard Employee Monitoring includes:

- ✓ **Remote Employee Time Tracking**: Track when work-from-home employees start and end their days. Monitor remote employee work hours and make sure they are working their full shift.
- ✓ **Remote Employee Productivity Tracking**: When remote workers know they are being monitored with an employee monitoring software, they are less likely to give in to distractions or make excuses for missed deadlines and sloppy work.
- ✓ **Data Theft & Fraud Detection**: If remote employee need to access sensitive data from outside the perimeters of your secure network, use InterGuard employee monitoring software to set up alerts to warn you if sensitive data is being sent by email, uploaded to cloud storage or copied to an external USB storage.

Logiciel de surveillance d'activités Interguard (2/3)

Employee Monitoring Software: Recorded Activity Types

You don't have to be an IT pro to set up and start monitoring employee activity with InterGuard's employee monitoring software. Just install the software on the PC or Mac desktop or laptop that you want to monitor and InterGuard starts track exactly what your employees are doing on their computers. You can easily search data to view logs and desktop screenshots of employee activity, including the following recorded data types:

- Email/Webmail
- Social Media
- File Tracking
- Instant Messages
- Website Searches
- Website History
- Screenshots
- Program Use
- Idle & Active Time
- Productivity
- Geolocation
- Print Tracking

Logiciel de surveillance d'activités Interguard (3/3)

TRACK AND IMPROVE EMPLOYEE PRODUCTIVITY

Employee monitoring software with productivity and time tracking features will quickly identify your team's superstars, time-thieving slackers and in-betweeners. You'll have more time plan business growth by automating the time-consuming job of manual employee productivity tracking. InterGuard gives you quantifiable metrics on time spent on websites and apps that you consider productive or non-productive. Take it a step further by blocking websites or apps that are against employee web usage policy.

PREVENT EMPLOYEE DATA THEFT & SECURITY LEAKS

31% take of outgoing employees ADMIT to taking client lists with them to competitors. Make sure your employees aren't abusing your trust with employee monitoring software. Employees who know their computers are being monitored are far less likely to attempt to email, print, upload or share your company secrets with others. Get notified if an employee is sending or sharing your sensitive information by outlook, webmail, USB or cloud-hosting file sharing sites and stop data ex-filtration before it happens.

CONDUCT EMPLOYEE INVESTIGATIONS

InterGuard employee monitoring software can be silently and remotely installed, so you can conduct covert investigations and bullet-proof evidence gathering without alarming the suspected wrongdoer. Every HR investigation is unique, and InterGuard is the easiest way to get full visibility into any use case. Fight potential financial fraud, employee misconduct, and wrongful termination suits.

SATISFY THE AUDITOR WITH ACTIVITY LOGGING

Regulatory bodies around the world require companies and organizations to comply with certain regulations for data security and privacy. Make sure employees are adhering to these guidelines with InterGuard's employee monitoring software. InterGuard lets you quickly produce detailed audit logs to satisfy auditors from CIPA, PCI, HIPAA, FINRA, FERPA and more.

Accès à la webcam

- Certains patrongiciels ont un accès continu ou ponctuel à la webcam de l'ordinateur.
- Pour certains, l'enregistrement se fait en continu pendant toute la journée avec l'option pour l'employeur de visionner n'importe quel moment de travail de la journée plus tard.
- Exemple : CleverControl demande l'accès de la webcam d'un employé à son insu, en prenant des photos à intervalles réguliers.
- Risques pour la privée : capture d'informations personnelles telles que les habitudes de vie aux domiciles mais aussi possiblement d'autres informations pouvant conduire à des problèmes de sécurité (numéro de carte bancaire, modèle d'alarme, ...).

Tableau comparatif des patrongiciels

Table: Common surveillance features of bossware products

	Activity monitoring (apps, websites)	Screenshots or screen recordings	Keylogging	Webcam/ microphone activation	Can be made "invisible"
ActivTrak	confirmed	confirmed			confirmed
CleverControl	confirmed	confirmed	confirmed	confirmed	confirmed
DeskTime	confirmed	confirmed			confirmed
Hubstaff	confirmed	confirmed			
Interguard	confirmed	confirmed	confirmed		confirmed
StaffCop	confirmed	confirmed	confirmed	confirmed	confirmed
Teramind	confirmed	confirmed	confirmed		confirmed
TimeDoctor	confirmed	confirmed			confirmed
Work Examiner	confirmed	confirmed	confirmed		confirmed
WorkPuls	confirmed	confirmed			confirmed

Features of several worker-monitoring products, based on the companies' marketing material. 9 of the 10 companies we looked at offered "silent" or "invisible" monitoring software, which can collect data without worker knowledge.

Source : Electronic Frontier Foundation.

Frontière floue entre patrongiciel et espiongiciel

- Certains patrongiciels vont jusqu'à enregistrer tout que l'utilisateur frappe au clavier ou encore permet de prendre le contrôle de l'ordinateur de l'employé.
- Même comportement que certains espiongiciels (*spyware* en anglais) tels que les enregistreurs de frappe (*keylogger* en anglais).

- Risques pour la privée : le logiciel ne fait pas de différence entre les données liées au travail et celles qui sont personnelles (numéros de carte de crédit, courriels personnels, ...).

Surveillance visible

- Le patrongiciel peut soit être clairement *visible* de l'employé (et éventuellement contrôlable) ou *invisible* pour lui en fonctionnant caché en tâche de fond.
- L'employé peut avoir la possibilité d'activer ou d'éteindre le logiciel de traçage (forme de pointage horaire, surtout si le temps de travail compté est celui où le logiciel est allumé).
- Possibilité ou non de voir complètement ou partiellement les données collectées et le profil généré.
- Souvent un avantage mis en avant pour l'employé est qu'il va pouvoir lui aussi s'améliorer grâce à l'information qui est fournie.
- Impact sur le comportement : l'employé adapte (possiblement inconsciemment) son comportement afin d'optimiser les métriques de productivité (ex : bouger la souris ou taper au clavier pour sembler être actif)

Surveillance invisible

- Tout comme un espiongiciel, l'employé n'est pas au courant qu'il est tracé car le patrongiciel est invisible.
- L'installation peut possiblement être faite à distance si l'employeur a les droits administrateurs sur la machine (ce qui est commun s'il s'agit d'un ordinateur fourni par l'employeur).
- Parfois l'employeur va demander à ce que le logiciel antivirus soit configuré de manière à ne pas bloquer et détecter l'espiongiciel.

Nécessité d'un cadre légal sur l'utilisation des patrongiciels

- Pour se protéger au niveau individuel : Autant que possible, essayer de séparer les usages personnels et professionnels.
- Exemple : création de deux comptes distincts sur son ordinateur ou sur une application de communication.
- Quelques pistes de réflexion au niveau collectif :
  - Si nécessaire la surveillance des employés devrait être proportionné par rapport à la finalité.
  - Des outils devraient être mis en place pour minimiser l'information collectée et éviter de collecter des données personnelles comme les mots de passe ou messages personnels.
  - Les employés devraient avoir le droit de connaître l'information collectée par leurs employeurs.
  - Les employés devraient avoir le droit de poursuivre leur employeur s'il viole leurs droits fondamentaux en matière de vie privée.

Application de traçage de contact

- Traçage de contact : méthode visant à retracer les personnes ayant étant en contact (à risque) avec une personne testée positive pour leur demander d'aller se faire tester et/ou se mettre en confinement.
- Classiquement se faire de manière "manuelle" par des humains qui appellent la personne infectée pour retracer son itinéraire.
- Objectif principal de l'application : automatiser la détection et notification des contacts si jamais l'utilisateur est testé positif,
- Avantage principal : pouvoir pallier à certaines limites de l'approche manuelle comme l'impossibilité de pouvoir se souvenir de toutes les personnes avec qui on a été en contact dans les deux dernières semaines.
- Enjeu dans le contexte du retour au travail : une organisation pourrait conditionner le retour au travail à l'installation de l'application et demander accès au score de risque.

Situation au Québec

- Une consultation publique à eut lieu en juillet suivi d'auditions d'experts devant une commission de l'assemblée nationale du Québec en août.
- Résumé des observations de la commission après consultation :

OBSERVATIONS

Au terme de ce mandat, les membres de la Commission des institutions observent que :

1. La confiance des citoyens et des citoyennes demeure la pierre angulaire du succès de toute démarche;
2. La quasi-totalité des experts rencontrés en commission ont émis des réserves importantes sur l'efficacité et la fiabilité de ces technologies et sont d'avis que la technologie Bluetooth souffre de vulnérabilités qui représentent des risques réels d'attaques informatiques;
3. Il n'existe pas d'opinion majoritaire d'experts sur l'utilité des applications de notification de contacts dans le contexte de la lutte contre la COVID-19, que ce soit lors de nos consultations ou sur le plan international;
4. Il n'existe pas d'opinion majoritaire d'experts sur l'efficacité des applications de notification de contacts dans un contexte de pandémie ni d'études publiées à ce sujet;
5. Il existe une opinion majoritaire d'experts selon laquelle les populations les plus vulnérables à la COVID-19 sont celles qui auraient le moins accès aux applications de notifications de contacts;
6. Le cadre juridique du Québec est inadéquat quant à la protection des données et des renseignements personnels et l'accès à l'information, le consentement éclairé et la lutte contre la discrimination.