C A N A D A

PROVINCE DE QUÉBEC
DISTRICT DE MONTRÉAL

DOSSIER R-3770-2011

RÉGIE DE L'ÉNERGIE

AUTORISATION D'INVESTISSEMENT
PROJET LECTURE À DISTANCE (LAD) – PHASE 1
D'HYDRO-QUÉBEC DISTRIBUTION

HYDRO-QUÉBEC
En sa qualité de Distributeur

Demanderesse

-et-

STRATÉGIES ÉNERGÉTIQUES (S.É.)

ASSOCIATION QUÉBÉCOISE DE LUTTE CONTRE LA POLLUTION ATMOSPHÉRIQUE (AQLPA)

Intervenantes

LA CAPACITÉ DE L'INFRASTRUCTURE PRÉVUE DE RÉPONDRE AUX PRÉOCCUPATIONS QUANT À LA PROTECTION DES DONNÉES PRIVÉES

RAPPORT AMENDÉ
JACQUES FONTAINE

Préparé pour:
Stratégies Énergétiques (S.É.)
Association québécoise de lutte contre la pollution atmosphérique (AQLPA)

Le 8 mars 2012

SOMMAIRE EXÉCUTIF

Il est souhaitable que la Régie de l'énergie et Hydro-Québec Distribution s'assurent que les avantages du présent Projet quant aux économies d'énergie et à la gestion de la consommation (avantages qui sont considérables) ne viennent se placer en opposition à des enjeux de confidentialité, qui nuiraient à l'acceptabilité et donc à la faisabilité de ce Projet.

RECOMMANDATION INITIALE NO. 3-2, CONFIRMÉE PAR LE PRÉSENT RAPPORT AMENDÉ :

Nous recommandons à la Régie de l'énergie de rendre son acceptation du présent Projet conditionnelle à un suivi, pour fins d'approbation par la Régie dans chaque cause tarifaire, de l'état annuel :

- des mesures mises en place par Hydro-Québec Distribution afin de protéger les données contre leur interception par des tiers et

- des mesures mises en place quant à la durée de conservation et quant aux échéances de destruction des données accumulées par Hydro-Québec Distribution sur ses clients.

TABLE DES MATIÈRES

PRÉSENTATION DU RAPPORT 1

1 - LA CAPACITÉ DE L'INFRASTRUCTURE PRÉVUE DE RÉPONDRE AUX PRÉOCCUPATIONS QUANT À LA PROTECTION DES DONNÉES PRIVÉES 3

1.1 LA PROTECTION CONTRE L'INTERCEPTION DES DONNÉES PRIVÉES 4

1.2 L'ENCADREMENT DE L'USAGE DES DONNÉES PRIVÉES PAR HYDRO-QUÉBEC DISTRIBUTION 7

2 - LES LACUNES DU RAPPORT D'ACCENTURE SUR L'ENJEU DE LA CONFIDENTIALITÉ 11

3 - CONCLUSION 22

PRÉSENTATION DU RAPPORT

Le soussigné avait reçu mandat initial, de la part de *Stratégies Énergétiques (S.É.)* et de l'*Association québécoise de lutte contre la pollution atmosphérique (AQLPA)*, de produire un rapport quant à la capacité de l'infrastructure prévue du projet *Lecture à distance (LAD)* d'Hydro-Québec Distribution (dossier R-3770-2011 de la Régie de l'énergie [1]) de répondre aux préoccupations quant à la protection des données privées. Ce rapport initial avait été remis à nos clientes et déposées par elles comme faisant partie de leur preuve devant la Régie de l'énergie, comme étant la section 2 de la pièce C-SÉ-AQLPA-0021, SÉ-AQLPA-3, Doc. 1.

Notre préoccupation centrale, dans ce rapport, consistait à inviter la Régie de l'énergie et Hydro-Québec Distribution à s'assurer que les avantages du présent Projet quant aux économies d'énergie et à la gestion de la consommation (avantages qui sont considérables) ne viennent se placer en opposition à des enjeux de confidentialité, qui nuiraient à l'acceptabilité et donc à la faisabilité de ce Projet.

Le présent rapport amendé remplace et complète ce rapport initial. Il est constitué de deux sections :

- En section 1, pour faciliter la référence, nous reproduisons l'intégralité de notre rapport initial (sur la question de la capacité de l'infrastructure prévue de répondre aux préoccupations quant à la protection des données privées), lequel constituait la section 2 de la pièce C-SÉ-AQLPA-0021, SÉ-AQLPA-3, Doc. 1.

- En section 2, nous déposons un rapport complémentaire, lequel vise principalement à appuyer davantage nos recommandations initiales, suite à des lacunes constatées sur le sujet dans la version publique du rapport de la firme *Accenture* déposé par Hydro-Québec Distribution auprès de la Régie de l'énergie en janvier 2012 (B-0088, HQD-1, Document 3.1).

[1] **HYDRO-QUÉBEC DISTRIBUTION**, Dossier R-3770-2011, Pièces B-0006 et B-0023, HQD-1, Document 1.

1

LA CAPACITÉ DE L'INFRASTRUCTURE PRÉVUE DE RÉPONDRE AUX PRÉOCCUPATIONS QUANT À LA PROTECTION DES DONNÉES PRIVÉES

RAPPORT INITIAL
PAR
JACQUES FONTAINE
DÉPOSÉ LE 28 OCTOBRE 2011

La crainte que les technologies de mesurage avancées ne portent atteinte à la confidentialité des informations des clients constitue parfois un motif nuisant à l'acceptabilité sociale de ces technologies.

Les craintes sont habituellement de deux ordres :

- D'une part, l'on peut se préoccuper de la possibilité que des données privées soient interceptées par des tiers n'y ayant pas droit, dans le cours de leur transmission à distance.

- D'autre part, l'on peut se préoccuper que le distributeur d'électricité détienne une trop grande quantité de renseignements privés sur ses clients et qu'il puisse éventuellement en abuser ou les transmettre à des autorités ou des tiers.

Nous sommes généralement rassurés par les réponses d'Hydro-Québec Distribution au présent dossier, mais recommanderons néanmoins qu'une certaine vigilance et un suivi à ces égards fassent partie des conditions auxquelles une éventuelle autorisation du présent Projet serait assujettie.

1.1 LA PROTECTION CONTRE L'INTERCEPTION DES DONNÉES PRIVÉES

Le Distributeur nous informe que les données qui transiteront sur le réseau IMA seront protégées par l'utilisation du *«Black Cloud»*.

En réponse à notre demande d'engagement, HQD précise :

> *Le « Black Cloud » est une expression non consacrée qui illustre la difficulté de déterminer la provenance de l'information et d'identifier le client à partir d'informations qui pourraient être interceptées sur le réseau IMA :*
>
> *• Le réseau est dynamique; le chemin utilisé par un compteur pour acheminer son information vers les systèmes d'entreprise peut varier d'une fois à l'autre.*
>
> *• Les données qui transitent sur le réseau IMA sont chiffrées à l'aide de clefs personnalisées et d'un algorithme.*
>
> *• Les équipements (compteurs, routeurs ou collecteurs), qui agissent comme relais, ne détiennent aucune information sur l'origine topologique de l'information.*
>
> *• Il est impossible de retracer les compteurs à partir des informations qui transitent sur le réseau.* [2]

Nous sommes satisfaits de cette réponse du Distributeur mais, tel qu'exprimé dans nos recommandations plus loin, nous inviterons la Régie à requérir un suivi afin de s'assurer surveiller que les fonctionnalités tant actuelles que futures éventuelles (Profils de consommation, In-Home Display, Home Area Network, Gestion de la demande, Gestion des actifs, Autoproduction, etc.) demeureront à l'abri des interceptions.

[2] **HYDRO-QUÉBEC DISTRIBUTION**, Dossier R-3770-2011, Pièce B-0029, HQD-3, Document 2, partie de la réponse à l'engagement 3 envers SÉ-AQLPA-RNCREQ, page 8.

Pike Research, dans un rapport de la fin 2010, affirme en effet :

> *Security Will Become the Top Smart Grid Concern* [3]

Pike Research relate à ce sujet un récent bris de sécurité majeur (le ver informatique *Stuxnet*) survenu dans les *Smart Grid* des États-Unis :

> *Grid security has always been an industry concern, though usually one that lingers in the background. The infamous smart meter hacking demonstration at the 2009 Black Hat Conference may not have broken any new technical ground among metering vendors, but it did raise cyber security awareness within the smart grid community. However, once metering vendors demonstrated reasonable solutions, the sense of alarm quickly passed.*
>
> *If anyone in the smart grid community still has a sense of cyber security peace and serenity after the summer of 2010, they need to check their pulse. The Stuxnet worm, discovered in July 2010, awakened the industry to the tangible and very complex threats to the supervisory control and data acquisition (SCADA) systems that run today's "semi-smart" grid and are poised to take a central position in a fully integrated and interconnected "really smart" grid.*
>
> *Stuxnet is a relatively silent worm that specifically targets and embeds itself into SCADA systems, providing a potential means to wreak havoc. It blasted through many of the axioms that allowed utility managers to sleep at night:*
>
> - *"My SCADA system is safe because it is not connected to the Internet" – Stuxnet apparently entered via USB memory sticks, perhaps distributed at your favorite smart grid conference.*
>
> - *"I keep my SCADA Windows Machine updated with the latest security patches and antivirus protection" – Stuxnet exploited zero-day vulnerabilities in Microsoft Windows and avoided detection by the best protection software. Stuxnet existed for months (years?) before detection. Moreover, many SCADA controllers are not managed as part of the normal enterprise IT network and are NOT kept up to date with almost daily security patches.*

[3] **PIKE RESEARCH**, *Smart Grid: Ten Trends to Watch in 2011 and Beyond. Research report*, Boulder CO, Published 4Q 2010, http://www.pikeresearch.com/wordpress/wp-content/uploads/2010/10/SG10T-10-Pike-Research.pdf , section 2.1, page 2.

"At least the threats are limited to my Windows-based management consoles" – Stuxnet not only infected Windows machines, but also aimed to infect the SCADA Programmable Logic Controllers in the field.

The technical analysis on Stuxnet continues, and it appears to be a very sophisticated attack not aimed at the electrical infrastructure. But if nothing else, the threats security experts have been warning of for years have now moved from theory to reality. Since the industry is taking greater notice, especially regulators and government (including the U.S. Congress), utilities will need to determine what cyber security measures are required – even as standards and regulations are still evolving.

On the standards front, the recently released (September 2010) National Institute of Standards and Technology (NIST) "Guidelines for Smart Grid Cyber Security," at three volumes and 537 pages, is a testament to both the unprecedented industry efforts to establish clear smart grid security guidelines and the incredible complexity and difficulty in doing so. The document has already become a bit of a lightning rod for criticism, which is in itself a productive outcome.

The North American Electric Reliability Corporation (NERC) CIP (Critical Infrastructure Protection) specifications, which have thus far been the closest thing to a general security specification for utilities – much to the chagrin of serious security experts – are being extensively revised. More importantly, utilities that have treated these as a nuisance paperwork exercise – yielding such silliness as almost all assets being declared "non-critical" – will be increasingly pressured to use these imperfect tools to actually assess and correct their vulnerabilities, lest they risk a starring role in the cyber equivalent of the BP gulf oil spill. [4]

[4] **PIKE RESEARCH**, *Smart Grid: Ten Trends to Watch in 2011 and Beyond. Research report*, Boulder CO, Published 4Q 2010, http://www.pikeresearch.com/wordpress/wp-content/uploads/2010/10/SG10T-10-Pike-Research.pdf , section 2.1, pages 2-3.

1.2 L'ENCADREMENT DE L'USAGE DES DONNÉES PRIVÉES PAR HYDRO-QUÉBEC DISTRIBUTION

Sur le site Internet du Distributeur, la politique de protection des renseignements personnels est décrite comme suit :

> ***Protection des renseignements personnels***
>
> ***Confidentialité des renseignements personnels***
>
> *Tout renseignement personnel détenu par un organisme public au sujet d'une personne physique doit être protégé contre toute forme d'utilisation inappropriée.*
>
> *À cet effet, Hydro-Québec met tout en œuvre pour garantir à ses employés, clients et fournisseurs le respect de la confidentialité des renseignements personnels qui lui sont fournis en conformité avec la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*
>
> *Voici comment la Loi sur l'accès énonce les dispositions pour protéger les renseignements personnels de nature confidentielle dans les organismes publics :*
>
> ***Collecte** – Hydro-Québec ne doit recueillir sur ses employés ou ses clients que les renseignements personnels nécessaires à la pratique de sa gestion. Cette règle est impérative et l'entreprise ne peut y déroger.*
>
> ***Conservation** – Lorsqu'Hydro-Québec détient un renseignement personnel, elle doit le conserver de façon telle que sa confidentialité est assurée. Les seules personnes qui peuvent avoir accès à ces renseignements doivent être autorisées à les consulter et ne peuvent le faire que dans l'exercice de leurs fonctions.*
>
> ***Communication à des tiers** – Les renseignements personnels confidentiels ne peuvent être divulgués à un tiers sans le consentement de la personne qu'ils concernent. Ce consentement doit être libre, manifeste et éclairé. Il doit être donné à des fins spécifiques et pour une durée limitée.*

Non communication de liste d'adresses *– Hydro-Québec ne divulgue aucune liste d'adresses de clients. Une telle diffusion ne serait pas conforme à l'objet des dispositions sur la protection des renseignements personnels de la Loi sur l'accès.*

L'accès à votre dossier client

À titre de cliente ou de client d'Hydro-Québec, vous avez le droit de consulter votre dossier et de connaître les renseignements qu'Hydro-Québec détient à votre sujet.

En effet, si vous êtes le titulaire d'un compte ou le cotitulaire, le cas échéant, vous pouvez obtenir de l'information sur votre compte d'électricité en vous adressant par téléphone au numéro du Service à la clientèle qui apparaît sur votre facture d'Hydro-Québec pendant les heures ouvrables. Après avoir validé votre identité, un représentant d'Hydro-Québec pourra répondre à vos questions.

Vous pouvez également obtenir de l'information sur votre compte d'électricité par le biais de votre page personnelle.

La Commission d'accès à l'information reconnaît toutefois le caractère public de certains renseignements relatifs à l'abonnement résidentiel. En effet, les renseignements suivants, qui servent à évaluer la consommation d'électricité à une adresse de service donnée, sont accessibles à toute personne qui en fait la demande :

- *le type de compte et le tarif applicable ;*
- *la consommation d'électricité et le montant d'argent correspondant ;*
- *la fréquence de la relève des compteurs ;*
- *le numéro du compteur ;*
- *le type de facturation ;*
- *la date à laquelle l'abonnement entre en vigueur ;*
- *le mode de chauffage ;*
- *le multiplicateur utilisé.*

Par contre, tous les autres renseignements qui vous concernent sont strictement confidentiels et se trouvent protégés, notamment :

- *votre nom ;*
- *votre numéro de compte ;*
- *votre adresse de service et de facturation ;*

- *votre numéro de téléphone ;*
- *votre numéro d'assurance sociale (NAS) ;*
- *votre dossier de crédit (facture, frais d'administration, date du dernier paiement, etc.) ;*
- *votre adresse antérieure ;*
- *la puissance à laquelle vous souscrivez.*

Vos renseignements confidentiels ne peuvent être divulgués qu'à vous, à moins que vous ne consentiez à les rendre accessibles à un tiers ou lorsqu'une exception est prévue à la Loi sur l'accès. [5]

Le Distributeur confirme que les consommations recueillies seront traitées confidentiellement :

Question 2.1.2 de la Régie : *Le cas échéant, veuillez préciser la politique du Distributeur sur la nature ou le type d'information sur la consommation des clients qui pourront être divulgués à l'extérieur de l'entreprise?*

Réponse d'Hydro-Québec Distribution : *Le Distributeur appliquera les mêmes pratiques et les mêmes restrictions d'accès aux informations détaillées qu'il détiendra sur la consommation que celles relatives à l'ensemble des renseignements personnels et confidentiels qu'il détient sur ses clients.* [6]

Malgré ces réponses rassurantes, il reste qu'un enjeu nouveau se posera : la durée de conservation de la somme considérable d'informations sur chaque client que le Distributeur acquerra dorénavant. D'un côté, il existera de multiples raisons de vouloir conserver des données de profils de consommation segmentées permettant de simuler de nombreuses hypothèses quant à la prévision de la demande et la construction de cas-types utiles au design des programmes d'efficacité énergétique et programmes commerciaux. D'un autre côté, cette conservation de données réduit la sphère de la vie privée et pourrait nuire à l'acceptabilité sociale du présent Projet. Le système permet d'établir et de conserver éternellement le profil de consommation de chaque client avec un degré de précision qui pourrait être considéré par ceux-ci comme une intrusion dans leur mode de vie. Les clients ne sont pas tous identiques et une connaissance précise et détaillée de leur consommation peut constituer une entrave à leur droits et privilège de confidentialité.

---

5 **HYDRO-QUÉBEC DISTRIBUTION**, *Site Internet,* http://www.hydroquebec.com/publications/fr/loi-acces/protection_renseignements.html, site consulté le 24 octobre 2011.

6 **HYDRO-QUÉBEC DISTRIBUTION**, Dossier R-3770-2011, Pièce B-0039, HQD-4, Document 1, Réponse 2.1.2 à la demande renseignements numéro 2 de la Régie, pages 4 et 5.

On peut aussi penser par exemple qu'en cas de plainte auprès du Distributeur ou auprès de la Régie, Hydro-Québec Distribution disposera d'une avalanche de données privées sur la consommation du client, dont elle pourra se servir pour répondre à sa plainte.

Il ne faudrait pas que les avantages du présent Projet quant aux économies d'énergie et à la gestion de la consommation (qui sont considérables puisqu'il permet la connaissance du profil de la consommation sur une base de quinze minutes) ne viennent se placer en opposition à des enjeux de confidentialité.

RECOMMANDATION INITIALE NO. 3-2 :

Nous recommandons à la Régie de l'énergie de rendre son acceptation du présent Projet conditionnelle à un suivi, pour fins d'approbation par la Régie dans chaque cause tarifaire, de l'état annuel :

- des mesures mises en place par Hydro-Québec Distribution afin de protéger les données contre leur interception par des tiers et

- des mesures mises en place quant à la durée de conservation et quant aux échéances de destruction des données accumulées par Hydro-Québec Distribution sur ses clients.

2

LES LACUNES DU RAPPORT D'ACCENTURE SUR L'ENJEU DE LA CONFIDENTIALITÉ

RAPPORT COMPLÉMENTAIRE
PAR
JACQUES FONTAINE
LE 8 MARS 2012

Le rapport *Accenture* du 18 janvier 2012 déposé par Hydro-Québec distribution traite notamment de la capacité de l'infrastructure prévue de répondre aux préoccupations quant à la protection des données privées. [7]

Dans notre rapport initial, reproduit en section 1 des présentes, nous formulions les craintes suivantes à l'effet que les technologies de mesurage avancées dans le projet LAD d'Hydro-Québec Distribution ne portent atteinte à la confidentialité des informations des clients :

- D'une part, l'on pouvait se préoccuper de la possibilité que des données privées soient interceptées par des tiers n'y ayant pas droit, dans le cours de leur transmission à distance.
- D'autre part, l'on pouvait se préoccuper que le distributeur d'électricité détienne une trop grande quantité de renseignements privés sur ses clients et qu'il puisse éventuellement en abuser ou les transmettre à des autorités ou des tiers. [8]

[7] **ACCENTURE**, *Rapport d'évaluation du projet de lecture à distance (LAD) d'Hydro-Québec Distribution*, 18 janvier 2012 (version expurgée des renseignements confidentiels), déposé sous : **HYDRO-QUÉBEC DISTRIBUTION**, Dossier R-3770-2011, Pièce B-0088, HQD-1, Document 3.1.

[8] **Brigitte BLAIS et Jacques FONTAINE pour Stratégies Énergétique (SÉ) et l'Association québécoise de lutte contre la pollution atmosphérique (AQLPA),** Dossier R-3770-2011, Pièce C-SÉ-AQLPA-0021, SÉ-AQLPA-3, document 1, section 2, page 17. Reproduit en section 1 des présentes.

À la page 23 de son rapport, *Accenture* se contente de nous ramener aux normes qu'Hydro-Québec Distribution respecte :

> *Le respect de normes de sécurité de haut niveau, telles que NISTIR 7628 et NEMA SG-IMA 1-2009, était également exigé aux fournisseurs. D'ailleurs, le fournisseur retenu par Hydro-Québec rencontre de hauts niveaux de sécurité des données et du réseau. La solution IMA déployée dispose ainsi de mécanismes d'encryptage avancés : clés de chiffrement des données uniques et générées plusieurs fois à des points stratégiques sur le réseau IMA; paquets d'information scindés pour voyager sur le réseau IMA et reconstitués que lorsqu'ils atteignent le frontal d'acquisition.* [9]

Or ces normes ne portent que sur la première des deux préoccupations énoncées ci-haut (le risque d'interception par des tiers) et non la seconde (la politique de conservation des données par Hydro-Québec et d'accès à ces données).

Accenture ajoute très brièvement en pages 23 :

> *Le rapport entre le coût et la qualité du service proposé, ainsi que les aspects de sécurité des données qui transitent sur le réseau étaient également des points positifs de la solution de Rogers.* [10]

Puis, brièvement en 34-35, Accenture ajoute :

> *Au niveau de la sécurité du système, Hydro-Québec Distribution a entrepris de nombreux travaux permettant d'être conforme avec les normes et standards de l'entreprise, notamment à travers des simulations d'attaques qui ont confirmé la solidité de la solution.*
>
> *Par ailleurs, une analyse de sécurité, menée en septembre 2011 par la firme Lofty Perch, ne contient aucune préoccupation sur la qualité des mesures de*

9 **ACCENTURE**, *Rapport d'évaluation du projet de lecture à distance (LAD) d'Hydro-Québec Distribution*, 18 janvier 2012 (version expurgée des renseignements confidentiels), déposé sous : **HYDRO-QUÉBEC DISTRIBUTION**, Dossier R-3770-2011, Pièce B-0088, HQD-1, Document 3.1, page 23.

10 **ACCENTURE**, *Rapport d'évaluation du projet de lecture à distance (LAD) d'Hydro-Québec Distribution*, 18 janvier 2012 (version expurgée des renseignements confidentiels), déposé sous : **HYDRO-QUÉBEC DISTRIBUTION**, Dossier R-3770-2011, Pièce B-0088, HQD-1, Document 3.1, page 23.

> *sécurité du système IMA. Cette firme externe considère que les mesures mises en place par Hydro-Québec Distribution sont efficaces et robustes.* [11]

Le rapport d'Accenture omet toutefois totalement de traiter de l'enjeu nouveau que pose l'ampleur des données que le nouveau système permettra de colliger. Il s'agit pourtant d'un enjeu fondamental et omniprésent tant dans la littérature scientifique qu'auprès des autorités publiques :

- La fréquence de mesure de la consommation totale permettra de savoir à quel moment le client est présent et à quel moment il est absent de chez lui. L'on pourra en déduire approximativement le nombre d'occupants des lieux ainsi que diverses habitudes de consommation. Plus les données mesurées sont fréquentes (par exemple aux quelques minutes ou aux quelques secondes), plus il sera possible de reconnaître, dans la consommation totale, le profil de certains appareils particuliers (machine à laver la vaisselle, machine à laver le linge, sécheuse, ordinateur, télévision, etc.).

  Selon Quinn, dans un rapport mandaté par la *Colorado Public Utilities Commission* :

  > *High-resolution electricity usage profiles can expose individual behavior patterns through the identification of each specific appliance event within the household. Not just when a consumer is at home and when she is away, but further* ***when she cooks dinner, watches TV, takes a shower****.*
  >
  > *Access to electricity usage in real time adds a further privacy concern to the development of personal behavioral patterns.* ***Not only could models of consumer behavior be developed after examining electricity records, their behavior could be tracked in real time****.* [12]

---

11 **ACCENTURE**, *Rapport d'évaluation du projet de lecture à distance (LAD) d'Hydro-Québec Distribution*, 18 janvier 2012 (version expurgée des renseignements confidentiels), déposé sous : **HYDRO-QUÉBEC DISTRIBUTION**, Dossier R-3770-2011, Pièce B-0088, HQD-1, Document 3.1, pages 34-35.

12 **Elias Leake QUINN**, *Smart Metering & Privacy : Existing Law and Competing Policies. A Report for the Colorado Public Utilities Commission*, Spring 2009, http://www.dora.state.co.us/puc/docketsdecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-SmartGridPrivacy.pdf , page 11. Souligné en caractère gras par nous.

Selon Molina-Markham [13], dans son étude *Private Memoirs of a Smart Meter*, la connaissance de la consommation électrique totale d'un logis, à intervalles courts, permet aisément de répondre aux questions suivantes sur la vie privée de ses occupants :

Table 1. Private questions and answers that fine-grained power consumption data reveals.

Question	Pattern	Granularity
Were you home during your sick leave?	Yes: Power activities during the day No: Low power usage during the day	Hour/Minute
Did you get a good night's sleep?	Yes: No power events overnight for at least 6 hours No: Random power events overnight	Hour/Minute
Did you watch the game last night?	Yes: Appliance activity matching TV program No: No power event in accordance with game showtime	Minute/Second
Did you leave late for work?	Yes: Last power event time later than Google maps estimated travel time No: Last power event time leaves enough time for commute	Minute
Did you leave your child home alone?	Yes: Single person activity pattern No: Simultaneous power events in distinct areas of the house	Minute/Second
Do you eat hot or cold breakfast?	Hot: Burst of power events in the morning (microwave/coffee machine/toaster) Cold: No power event matching hot breakfast appliances	Second

Selon Molina-Markham :

> ***the widespread deployment of smart meters has serious privacy implications since they inadvertently leak detailed information about household activities***. *The information leaks directly correlate with the time granularity that a meter measures power consumption. Unlike traditional dumb meters that record aggregate monthly usage for a utility, today's smart meters allow an utility, or a malicious party, to glean detailed information about household activity in real-time from fine-grained usage measurements. Further, research on nonintrusive load monitoring (NILM) has shown that* ***it is possible to disambiguate individual appliance usage from an aggregate smart meter power trace by using prior knowledge of an appliance's power signature. Such techniques reduce or eliminate the need for outlet- or appliance-level meters, since they are able to extract detailed usage information for individual appliances from an aggregate household power trace***.
>
> *We show that* ***even without detailed knowledge of appliance signatures a priori or prior training, it is possible to extract***

[13] **Andres MOLINA-MARKHAM et als**, *Private Memoirs of a Smart Meter*, 2010, http://www.cs.umass.edu/~kevinfu/papers/molina-markham-buildsys10.pdf , section 1.

> ***complex usage patterns from smart meter data using off-the-shelf statistical methods. Our methods are able to label specific types of activity in the home over time based on a number of characteristics, including the level of power consumption, its intermittency, and its duration.*** *[…] with our limited data, we argue that* ***it is possible to infer detailed information about household activity—questions such as how many people are in a home at a given time and whether a resident went out for dinner on a particular evening, for example****. Entities that gather large amounts of data would potentially be able to* ***predict even more detailed facts, such as residents' genders and ages.***
>
> *Such information is a foundation for building powerful analytic tools for predicting behavior that could potentially be misused by companies or even criminals.* [14]

Selon Quinn, même des données de consommation totale obtenues aux 15 ou 30 minutes suffisent à identifier, avec un faible taux d'erreur, les équipements électriques effectivement utilisés dans un logis. [15]

Lam propose d'établir une banque de données des signatures électriques des différents appareils domestiques. [16]

- Si les données de consommation totale d'un logis sont mesurées à de très brefs intervalles, il est même possible d'en déduire quelle émission est regardée à la télévision. En effet, chaque programme de télévision possède sa signature propre, du fait que chaque image claire (lumineuse) nécessite plus d'électricité qu'une image foncée. Il est donc possible, à l'aide d'un logiciel qui neutraliserait les

---

14 **Andres MOLINA-MARKHAM et als**, *Private Memoirs of a Smart Meter*, 2010, http://www.cs.umass.edu/~kevinfu/papers/molina-markham-buildsys10.pdf , section 1. Souligné en caractère gras par nous.

15 **Elias Leake QUINN**, *Smart Metering & Privacy : Existing Law and Competing Policies. A Report for the Colorado Public Utilities Commission*, Spring 2009, http://www.dora.state.co.us/puc/docketsdecisions/DocketFilings/09I-593EG/09I-593EG_Spring2009Report-SmartGridPrivacy.pdf , pages 2-3.

16 **H.Y. LAM et als**, *A Novel Method to Construct Taxonomy of Electrical Appliances Based on Load Signatures*, Publié dans Transactions on Consumer Electronics, Vol. 53, no. 2, Mai 2007, pp. 653-660, Résumé publié à : http://ieeexplore.ieee.org/Xplore/login.jsp?reload=true&url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F30%2F4266888%2F04266955.pdf%3Farnumber%3D4266955&authDecision=-203 .

signatures plus constantes des autres sources de consommation électrique du logis, de déterminer la signature électrique du film ou du programme télévisuel regardé et de le comparer électroniquement à une banque des signatures des divers films ou programmes télé :

> *Our findings contribute to the overall debate of whether or not measurements of residential powerlines reveal significant information about the activities within a home. We find that* ***the power supplies of modern TVs produce discernible electromagnetic interference (EMI) signatures that are indicative of the video content being displayed****.* [17]
>
> *A new generation of smart meters generating high-resolution energy consumption data could henceforth cause new potentials concerns regarding consumers' privacy sphere. We have demonstrated that* ***particular information available on appliances in the household via its detailed power profile allow a fine-grained analysis of the appliance's behavior****. Taking measurements at an interval of two seconds is sufficient to* ***enable the identification of a television program or audiovisual content*** *if favorable conditions are in place (e.g., no major interference of other appliances for minutes long). Our research has shown that the electricity usage profile with a 0:5s^{-1} sample rate leads to an invasion into a person's private sphere regarding his TV watching habits.* ***Five minutes of consecutive playing of a movie is in many cases sufficient to identify the viewed content by analyzing the smart meter power consumption data****.* [18]

- À cela s'ajouteraient les renseignements personnels supplémentaires qui deviendraient disponibles en cas de déploiement de diverses fonctionnalités (*Home Area Network*, etc.).

---

17 **Miro ENEV et als.**, *Televisions, Video Privacy, and Powerline Electromagnetic Interference*, 2011, http://www.cs.washington.edu/homes/yoshi/papers/ccs2011-emi.pdf , sommaire. Souligné en caractère gras par nous.

18 **Ulrich GREVELER et als.**, *Multimedia Content Identification Through Smart Meter Power Usage Profiles*, 2012, http://www.its.fh-muenster.de/greveler/pubs/preprint_online.pdf , conclusion. Souligné en caractère gras par nous.

Voir aussi : **Dario CARLUCCIO et als.**, *Smart Hacking for Privacy*, 28th Annual Chaos Communication Congress, Janvier 2012, http://www.cs.washington.edu/homes/yoshi/papers/ccs2011-emi.pdf (quant à la partie qui traite des signatures de programmes).

L'accroissement du volume et de la précision des données collectées accroît donc nettement les conséquences d'un bris de confidentialité (par interception par un tiers ou au niveau de la politique de conservation et d'accès aux données chez HQD).

L'absence de réflexion d'*Accenture* sur ce sujet est grave, compte tenu de l'importance de l'enjeu de la confidentialité dans le débat public et dans le débat au sein de l'industrie relatifs aux compteurs avancés, tel qu'amplement illustré dans notre rapport initial auquel nous référons le lecteur (reproduit en section 1 des présentes).

Les renseignements personnels sur les clients détenus par les utilités publiques, dont les règles de conservation et d'accès font actuellement l'objet de nombreuses études et débats, sont généralement connus sous l'acronyme *CEUD (consumer-specific energy-usage data)*. [19]

Selon la *National Association of Regulatory Commissioners (NARUC)* :

> *While the deployment of smart grid technologies may empower the consumer and provide more options, **it also poses significant privacy issues that need to be considered and resolved by regulators*** [20]

Selon l'*Office of the National Coordinator for Smart Grid Interoperability* du *National Institute of Standards and Technology (NIST)* du *Département du Commerce* des États-Unis :

> ***The privacy implications of frequent meter readings being fed into the Smart Grid networks could provide a detailed time line of activities***

---

19 **U.S. DEPARTMENT OF ENERGY**, *Data Access and Privacy Issues Related to Smart Grid Technologies*, October 5, 2010, http://energy.gov/sites/prod/files/gcprod/documents/Broadband_Report_Data_Privacy_10_5.pdf , Page 9.

20 **U.S. NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS (NARUC)**, *Resolution on Smart Grid*, Adopted by the NARUC Board of Directors July 21, 2010, http://www.naruc.org/Resolutions/Resolution%20on%20Smart%20Grid1.pdf .La NARUC avait déjà reconnu le caractère de la protection des données personnelles obtenues par les entreprises d'utilité publique : **U.S. NATIONAL ASSOCIATION OF REGULATORY UTILITY COMMISSIONERS (NARUC)**, *Resolution Urging the Adoption of General Privacy Principles For State Commission Use in Considering the Privacy implications of the Use of Utility Customer Information*, Adopted by the NARUC Board of Directors, July 26, 2000, http://www.naruc.org/Resolutions/privacy_principles.pdf . Souligné en caractère gras par nous.

> ***occurring inside the home**. This data may point to a specific individual or give away privacy sensitive data.*
>
> ***The constant collection and use of smart meter data has also raised potential surveillance possibilities posing physical, financial, and reputational risks that must be addressed**.* [21]

Selon le *Commissaire à l'information et à la protection de la vie privée* de l'Ontario :

> *Privacy concerns arise when there is a possibility of **discovering personal information such as the personal habits, behaviours and lifestyles of individuals inside dwellings**, and to use this information for secondary purposes, other than for the provision of electricity. Electric utilities and other providers may have access to information about what customers are using, when they are using it, and what devices are involved. **An electricity usage profile could become a source of behavioural information on a granular level**.* [22]
>
> ***Capturing the flow of electricity into one's home, and the manner in which it is used over a period of time, may be revealing and highly intrusive**. The overarching privacy concerns associated with Smart Grid technology are its ability to greatly increase the amount of information that is currently available relating to the activities of individuals within their homes.* [23]
>
> ***We must take great care not to sacrifice consumer privacy amidst an atmosphere of unbridled enthusiasm for electricity reform. Information***

---

21 **U.S. DEPARTMENT OF COMMERCE, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST), OFFICE OF THE NATIONAL COORDINATOR FOR SMART GRID INTEROPËRABILITY**, NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0, NIST Special Publication 1108, January 2010, http://www.nist.gov/public_affairs/releases/upload/smartgrid_interoperability_final.pdf , Section 7.3.3, page 119. Souligné en caractère gras par nous.

22 **ONTARIO INFORMATION AND PRIVACY COMMISSIONER**, *Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf , page 10. Souligné en caractère gras par nous.

23 **ONTARIO INFORMATION AND PRIVACY COMMISSIONER**, *Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf , page 18. Souligné en caractère gras par nous.

> ***proliferation, lax controls and insufficient oversight of this information could lead to unprecedented invasions of consumer privacy***. [24]

L'*Association canadienne de l'électricité* cite ces propos du *Commissaire à l'information et à la protection de la vie privée* de l'Ontario, avec approbation. [25]

Pour toutes ces raisons, il est donc très surprenant qu'*Accenture* ait omis de traiter de ces préoccupations dans son rapport.

Le rapport 2010 du *Smart Grid Interoperability Panel* souligne que quatre (4) dimensions de la vie privée doivent être prises en compte dans l'implantation de la nouvelle infrastructure, à savoir la sécurité personnelle, la privité de la personne, la privité de ses choix de vie et de comportements, et la privité de ses échanges avec autrui. [26]

L'accroissement des conséquences d'un bris de confidentialité quant à tous ces aspects de la vie privée confirme l'importance du suivi que nous avons recommandé, dans notre recommandation initiale 3-2 reproduite plus haut :

- En ce qui concerne le risque d'interception des données par des tiers, un suivi permanent reste toujours nécessaire afin de s'assurer que le fournisseur du service maintienne toujours à la fine pointe sa technologie de protection contre les interceptions, afin de parer à la sophistication de plus en plus grande des intercepteurs potentiels. [27] L'on garde à l'esprit que chaque compteur est déjà conçu pour recevoir et ré-émettre les données de consommation de tous ses voisins.

---

24 **ONTARIO INFORMATION AND PRIVACY COMMISSIONER**, *Smart Privacy for the Smart Grid: Embedding Privacy into the Design of Electricity Conservation*, http://www.ipc.on.ca/images/resources/pbd-smartpriv-smartgrid.pdf , page 3. Souligné en caractère gras par nous.

25 **ASSOCIATION CANADIENNE DE L'ÉLECTRICITÉ, L'ÉLECTRICITÉ**, *Le réseau intelligent. Une démarche pragmatique*, 2010, http://www.electricity.ca/media/SmartGrid/SmartGridpaperFR.pdf , page 23.

26 **THE SMART GRID INTEROPERABILITY PANEL, CYBER SECURITY WORKING GROUP**, *Introduction to NISTIR 7628-Guidelines for Smart Grid Cyber Security*, September 2010, pages 18 et 19, http://csrc.nist.gov/publications/nistir/ir7628/introduction-to-nistir-7628.pdf .

27 Voir notamment : **Dario CARLUCCIO et als.**, *Smart Hacking for Privacy*, 28th Annual Chaos Communication Congress, Janvier 2012, http://www.cs.washington.edu/homes/yoshi/papers/ccs2011-emi.pdf .

- En ce qui concerne, la politique de conservation et accès aux données chez HQD, il y a lieu de s'interroger sur la fréquence des données dont le Distributeur a réellement besoin. HQD a-t-elle besoin de posséder les données de consommation de tous ses clients aux 15 minutes? Plus fréquemment ? Moins fréquemment ? Pour quel usage ? Une fois les données obtenues, serait-il opportun que seule une partie des données reste conservée d'une manière qui permette l'identification du client et que le reste des données, plus précises, deviennent amalgamées à des fins de statistiques ou de profils moyens seulement ? Dans tous les cas, quelle devrait être la durée de conservation par HQD des données fines personnalisées (aux 15 minutes par exemple) : un mois ? six mois ? un an ? dix ans ? éternellement ?

  Si des données fines personnalisées existent sur un client au sein de HQD, il est théoriquement possible à des tiers de les obtenir par voie judiciaire. *Le procureur de nos clientes nous informe en effet que : i) Dans un procès criminel, les données pourraient être obtenues d'un poursuivant si un mandat est émis à cette fin par le Tribunal de juridiction criminelle (qui ne l'émet que lorsque certains critères sont respectés). Toutefois, il se pourrait que certaines informations sur la consommation du client soient obtenables par le poursuivant auprès de l'utilité publique même sans mandat.* [28] *ii) En outre, dans un procès civil, toute partie pourrait théoriquement requérir par sub poena les données possédées par HQD afin de les opposer à sa partie adverse pour faire ressortir la vérité (telle que la présence ou l'absence d'une personne à une certaine date ou des renseignements plus pointus pouvant être déduits des relevés de consommation). iii) De surcroît, les données déposées lors d'un procès criminel ou civil deviendraient alors accessibles à tous, sauf si le Tribunal en ordonne la confidentialité.*

  Dans notre rapport initial, nous avions aussi souligné qu'en cas de plainte auprès du Distributeur ou auprès de la Régie, Hydro-Québec Distribution disposera d'une avalanche de données privées sur la consommation du client, dont elle pourra se servir pour répondre à sa plainte.

[28] Références à des jugements de la *Cour suprême du Canada* fournies par le procureur de nos clientes : *R.* c. *Gomboc*, [2010] 3 R.C.S. 211, *R.* c. *Plant*, [1993] 3 R.C.S. 281, *R.* c. *Tessling*, [2004] 3 R.C.S. 432.

Nous réitérons donc notre souhait que la Régie de l'énergie et le Distributeur s'assurent que les avantages du présent Projet quant aux économies d'énergie et à la gestion de la consommation (qui sont considérables) ne viennent se placer en opposition à des enjeux de confidentialité, lesquels nuiraient à l'acceptabilité (et donc à la faisabilité) du Projet.

Nous continuons de recommander à la Régie de l'énergie de rendre son acceptation du présent Projet conditionnelle à un suivi, pour fins d'approbation par la Régie dans chaque cause tarifaire, de **l'état annuel** :

- ❑ des mesures mises en place par Hydro-Québec Distribution afin de protéger les données contre leur interception par des tiers et

- ❑ des mesures mises en place quant à la durée de conservation et quant aux échéances de destruction des données accumulées par Hydro-Québec Distribution sur ses clients.

3

CONCLUSION

Nous invitons donc la Régie de l'énergie à accueillir les recommandations qui sont exprimées au présent rapport, que l'on trouve également reproduites en son sommaire exécutif.