MUNK SCHOOL OF GLOBAL AFFAIRS

UNIVERSITY OF TORONTO

TELECOM TRANSPARENCY PROJECT

cippic

« Aller Opaque? »

« Une analyse de la surutilisation des collecteurs de IIAM au Canada »

Sommaire exécutif | traduction

août 2016

Le rapport par Tamir Israel et Christopher Parsons

À propos du Telecom Transparency Project et de la Clinique d'intérêt public et de politique d'internet du Canada (CIPPIC)

Le **Telecom Transparency Project** étudie la façon dont les données de télécommunications sont surveillées, collectées et analysées aux fins commerciales, de sécurité publique, et services de renseignements. Le projet est associé au Citizen Lab, laboratoire interdisciplinaire basé à l'École Munk des Affaires internationales de l'Université de Toronto. Le Citizen Lab s'engage en recherche et développement de pointe, à l'intersection de l'information et des technologies de communication, des droits humains, et de la sécurité globale.

La Clinique d'intérêt public et de politique d'internet du Canada (CIPPIC) est une clinique juridique au Centre de recherche en droit, technologie et société à l'Université d'Ottawa. Son mandat principal est de protéger l'intérêt public dans les prise de décision se trouvant à l'intersection du droit et de la technologie. Elle fournit également de l'assistance juridique aux organisations et individus sous-représentés, pour des questions de droit et de technologie. CIPPIC possède aussi un mandat éducatif axé sur la formation juridique pratique, dans le cadre des lois et de la technologie.

Les auteurs

Ce rapport a été préparé et rédigé par Tamir Israel et Christopher Parsons.

Tamir Israel est un avocat à la Clinique d'intérêt public et de politique d'internet du Canada (CIPPIC) à la faculté de droit de l'Université d'Ottawa. Il dirige les programmes sur la vie privée, la neutralité du net, la surveillance électronique et la réglementation des télécommunications. Il mène aussi des recherches et des interventions juridiques sur une série d'autres sujets liés aux droits numériques. Il est également un chargé de cours sur la réglementation d'Internet à Faculté des études supérieures et postdoctorales de l'université d'Ottawa.

tisrael@cippic.ca
PGP: 0xF0F41649

Christopher Parsons possède un baccalauréat et une maîtrise de l'Université de Guelph, ainsi qu'un doctorat de l'Université de Victoria. Il est maintenant chercheur associé au Citizen Lab, à l'École Munk des Affaires internationales de l'Université de Toronto, ainsi que le directeur général du Telecom Transparency Project au Citizen Lab.

christopher@christopher-parsons.com
PGP: 0xDD8323FD

Sommaire exécutif

Ce rapport analytique, « Aller Opaque? Une analyse de la surutilisation des collecteurs de IIAM au Canada », examine une classe de systèmes de surveillance téléphonique appelés «cell site simulators» (simulateurs de sites cellulaire), aussi connus sous le nom «IMSI Catchers» (intercepteurs et/ou collecteurs de IIAM), «digital analyzers», «cell grabbers», ou «mobile device identifiers» en anglais, ou par des noms de marque tels que Stingray, DRTBOX et Hailstorm.

Les collecteurs de IIAM permettent aux organismes d'État d'intercepter les communications des appareils mobiles, et sont utilisés principalement pour identifier ou suivre des individus autrement anonymes, associés à un appareil mobile. Ces dispositifs de surveillance ne sont pas nouveaux: leur utilisation par les organismes d'État s'étend sur des décennies. Cependant, l'omniprésence de la communication mobile dans la vie moderne, ainsi que la réduction du coût de ces dispositifs, conduit à une augmentation considérable de la fréquence et la portée de leur utilisation. Comme ces appareils sont très intrusifs de par leur nature, l'usage clandestin et incontrôlé de ces systèmes constitue une menace insidieuse à la vie privée.

Plus généralement, le rapport examine les capacités de surveillance des collecteurs de IIAM, les efforts de l'Etat pour restreindre l'accès public aux informations concernant ces dispositifs (et les contre-efforts menés par la société civile), et le cadre juridique et politique qui régit l'utilisation des collecteurs de IIAM. Même si ce rapport se concentre principalement sur les organismes de l'État canadien, il contient des exemples comparatifs d'autres juridictions, notamment les États-Unis et l'Allemagne. Le rapport se termine par une série de recommandations pour la transparence et réformes juridiques visant à limiter l'utilisation de ces dispositifs et de réduire les aspects les plus intrusifs de ces technologies. Le rapport est divisé en quatre sections: les capacités techniques des collecteurs de IIAM, la transparence, les politiques de contrôle, et certaines recommandations de meilleures pratiques.

Compte tenu de la nature évolutive des questions abordées dans ce document, une série de récents développements ont été intégrés dans le rapport sous la forme de «boîtes mise à jour», avec l'intention de documenter ces développements et de les intégrer dans l'analyse contenue dans le rapport principal.

Section I du rapport donne un aperçu des capacités des collecteurs de IIAM. Comme ces appareils sont conçus pour simuler la fonctionnalité des tours cellulaires, nous pouvons en déduire beaucoup sur leurs capacités en regardant les protocoles et les spécifications régissant les communication cellulaires bien documentées. Le rapport se concentre principalement sur le fonctionnement de ces appareils en mode

«identification», où ces dispositifs interceptent les numéros numériques tels que les numéros IIAM (identité internationale de l'abonné mobile) et IIEM (identité internationale d'équipement mobile) qui identifient les appareils mobiles. Les collecteurs de IIAM trompent les appareils mobiles en leur faisant croire que le dispositif est une tour de cellule gérée par un fournisseur de service mobile légitime. Ensuite, ils induisent les appareils mobiles à transmettre leurs identificateurs numériques uniques, normalement exclusivement destinés aux fournisseur de services mobiles. cette section procède à explorer comment les collecteurs de IIAM peuvent être utilisés pour la surveillance, en particulier par les divers organismes d'État. Dans un contexte d'enquête, les collecteurs de IIAM sont principalement utilisés pour identifier ou localiser des individus, enfreignant le droit à l'anonymat et la protection de la vie privée. Les appareils mobiles dupés pour interagir avec un collecteur de IIAM sont retirés du réseau de communication mobile et, par conséquent, ne sont pas en mesure d'envoyer ni de recevoir appels, messages texte ou données. Ces dispositifs sont intrusifs par nature: ils sont conçus pour capturer les identifiants mobiles de tous téléphones à portée, ce qui mène à un impact collatéral sévère pour la vie privée: la surveillance d’une seule cible peut affecter des milliers d’individus.

Section II examine les efforts visant à identifier et comprendre la manière dont les gouvernements utilisent les collecteurs de IIAM dans plusieurs juridictions. Elle commence par analyser les activités se déroulant à l'extérieur du Canada, en décrivant les efforts de la société civile pour découvrir l'utilisation des collecteurs de IIAM face à l'obscurcissement du gouvernement. Après avoir souligné certains succès durement combattus aux États-Unis, nous examinons les efforts comparables pour découvrir comment les collecteurs de IIAM sont utilisés au Canada. Le rapport utilise un appel d'un refus d’une demande d'accès à l’information comme une étude de cas pour illustrer certains problèmes auxquels sont confrontés les canadiens qui cherchent à comprendre l’utilisation des collecteurs de IIAM. Le rapport critique plusieurs justifications fréquemment utilisées par les agences de l'Etat pour empêcher la publication d'informations relatives aux collecteurs de IIAM. L'étude conclut que fournir des détails sur l'utilisation des collecteurs de IIAM ne compromettrait pas leur utilité, et que la divulgation publique d’informations sur ces dispositifs est essentielle à l'intérêt public : la divulgation publique est importante afin que de s’assurer qu’aucune loi est violée. Ceci est particulièrement important car la possession et l'utilisation de ces dispositifs pourraient être incompatibles avec la *Loi sur la radiocommunication*, la *Loi sur la protection des renseignements personnels* et, dans certains cas, la *Charte canadienne des droits et libertés.* Le refus de fournir des informations concernant l'utilisation des collecteurs de IIAM reporte les débats publics importants concernant les paramètres appropriés de leur utilisation. De plus, ces dénis nuisent à la confiance, et nuisent à la

perception que ces dispositifs sont utilisés légalement, proportionnellement, et avec un impact minimal sur le public (non-ciblés).

Section III examine la réglementation des collecteurs de IIAM et les diverses avenues vers l'autorisation légale de leur utilisation. Nous analysons les modèles réglementaires en Allemagne et aux États-Unis afin de mieux comprendre les lacunes potentielles dans le contexte canadien. Ensuite, le rapport explore le cadre législatif de la surveillance électronique, ambigu au Canada, afin de mieux comprendre les moyens juridiques disponibles aux organismes d'État pour l'autorisation de l'utilisation d'un collecteur de IIAM. Le rapport montre comment une combinaison de pouvoirs peut justifier l'autorisation de ces dispositifs, et comment cette ambiguïté pourrait permettre aux organismes d'État à déployer des collecteurs de IIAM de façon à mettre en péril la vie privée des citoyens. Cela pourrait permettre l'utilisation des collecteurs de IIAM de manière disproportionnée et même inconstitutionnelle. La section se termine par l'analyse des implications de l'utilisation des collecteurs de IIAM du point de vue de la *Charte canadienne des droits et libertes*. Même si certaines agences de l'Etat peuvent croire qu'il est possible d'utiliser ces appareils sans autorisation judiciaire préalable, leur raisonnement est quasi-certainement incompatible avec la Charte. Le rapport examine les justifications possibles pour le déploiement d'un collecteur de IIAM en l'absence d'autorisation judiciaire préalable, et rejette chacune de ces justifications. Les collecteurs de IIAM fonctionnent comme des outils d'identification et de géolocalisation, et les tribunaux ont jugé que la surveillance électronique d'identifiants numériques et géolocalisation nécessitent une autorisation judiciaire préalable. L'article 8 de la Charte devrait donc obliger les agences gouvernementales à obtenir une autorisation judiciaire avant d'utiliser un collecteur de IIAM. Cette section se conclut en énumérant les garanties et les conditions nécessaires pour s'assurer que l'utilisation des collecteurs de IIAM ne constitue pas une fouille inconstitutionnelle.

Section IV présente plusieurs meilleures pratiques pour réglementer l'utilisation des collecteurs de IIAM. Ces meilleures pratiques sont distillées à partir de diverses limites imposées à l'utilisation des collecteurs de IIAM dans d'autres juridictions, des mécanismes imposés sur les systèmes de surveillance électronique comparables au Canada, ainsi que des meilleures pratiques pour la surveillance électronique en général. La section recommande que l'utilisation des collecteurs de IIAM par les organismes publics devraient être soumis à des mécanismes de transparence complets, y compris (1) un rapport statistique annuel sur leur utilisation, (2) une obligation d'aviser les personnes dont leurs renseignements personnels ont été recueillis, et (3) le respect des obligations généralement appliquées aux appareils de radio appartenant aux organismes d'État. Il fait ensuite valoir que l'utilisation non autorisée d'un collecteur de IIAM doit être criminalisée. Afin d'assurer que l'utilisation de ces dispositifs est

uniquement autorisée de façon proportionnée, le rapport suggère que leur utilisation devrait être soumise à un régime d'autorisation strict ainsi qu'un critère de « nécessité d'enquête », et un disposition qui réserve leur utilisation à l'enquête de crimes particulièrement graves, énumérés de façon exhaustive dans la loi. En plus desmesures de proportionnalité, il est nécessaire de cibler et de réduire au maximum l'utilisation des collecteurs de IIAM afin d'atténuer leur impacts collatéraux sur les tiers innocents. Cela comprend (1) une interdiction, dans la mesure du possible, de l'utilisation de ces appareils dans les zones ou durant les périodes où de nombreuses personnes non ciblées seront soumises à cet outil de surveillance intrusive, (2) l'obligation de supprimer rapidement les données des personnes non ciblées et (3) des limites strictes sur l'utilisation de telles informations.

En conclusion, le rapport souligne quelques-uns des résultats les plus essentiels, et souligne également l'importance de la vie privée dans toute société démocratique. Le défaut de rendre les technologies de surveillance transparentes ou de réglementer leur utilisation soulève des questions essentielles aux libertés individuelles et droits fondamentaux. Ceci est particulièrement vrai étant donnée la nature subreptice des outils de surveillance électronique. Le gouvernement du Canada ainsi que ses homologues provinciaux devraient suivre l'exemple d'autres juridictions, en fournissant des informations au public sur la manière dont les collecteurs de IIAM peuvent être utilisées par les agences de l'Etat. Ils devraient également se tourner vers les expériences d'autres pays pour, à l'avenir, strictement réglementer toute utilisation de ces dispositifs intrusifs. L'utilisation de ces appareils menace de placer les citoyens sous un régime de surveillance dangereux et peut avoir des effets négatifs sur les libertés fondamentales des Canadiens.