McGill Law Journal — Revue de droit de McGill

LAW ENFORCEMENT ACCESS TO ENCRYPTED DATA: LEGISLATIVE RESPONSES AND THE *CHARTER*

*Steven Penney and Dylan Gibbs**

In our digital age, encryption represents both a tremendous social benefit and a significant threat to public safety. While it provides the confidence and trust essential for digital communications and transactions, wrongdoers can also use it to shield incriminating evidence from law enforcement, potentially in perpetuity. There are two main legal reforms that have been proposed to address this conundrum: requiring encryption providers to give police "exceptional access" to decrypted data, and empowering police to compel individuals decrypt their own data.

This article evaluates each of these alternatives in the context of policy and constitutional law. We conclude that exceptional access, though very likely constitutional, creates too great a risk of data insecurity to justify its benefits to law enforcement and public safety. Compelled decryption, in contrast, would provide at least a partial solution without unduly compromising data security. And while it would inevitably attract constitutional scrutiny, it could be readily designed to comply with the *Charter*. By requiring warrants to compel users to decrypt and giving evidentiary immunity to the act of decryption, our proposal would prevent inquisitorial fishing expeditions yet allow the decrypted information itself to be used for investigative and prosecutorial purposes.

À l'ère du numérique, la cryptographie représente à la fois un avantage social considérable et une menace importante à la sécurité publique. Bien que cet outil assure la confiance essentielle à l'intégrité des communications et transactions numériques, des malfaiteurs peuvent également s'en servir pour dissimuler des preuves incriminantes des forces de l'ordre. Deux réformes juridiques ont été principalement proposées pour remédier à cette problématique: obliger les fournisseurs de systèmes cryptographiques à offrir à la police un « accès exceptionnel » aux données décryptées et à leur donner le pouvoir d'obliger les particuliers à décrypter leurs propres données.

Cet article évalue ces deux options dans le contexte de politiques publiques et du droit constitutionnel. Nous concluons que l'option de l'accès exceptionnel, bien que très probablement constitutionnelle, génère un risque d'insécurité trop important pour en justifier les avantages qu'il peut offrir aux forces de l'ordre et à la sécurité publique. Le déchiffrement forcé, en revanche, proposerait au moins une solution partielle à la problématique, sans compromettre indûment la sécurité des données visées. Et bien que cela attirerait inévitablement un examen constitutionnel, cela pourrait être facilement conçu pour se conformer à la *Charte*. En exigeant des mandats pour obliger les utilisateurs à décrypter leurs données et en donnant l'immunité en matière de preuve à l'acte de décryptage, notre proposition empêcherait les *expéditions de pêche inquisitoriales* tout en permettant l'utilisation des informations déchiffrées à des fins d'enquête et de poursuite.

* Steven Penney, Professor, Faculty of Law, University of Alberta. Dylan Gibbs, JD, University of Alberta, 2018; BSc (Computing Science), University of Alberta, 2013. Thanks to the three anonymous reviewers for their helpful comments.

Citation: (2017) 63:2 McGill LJ 201 — Référence : (2017) 63:2 RD McGill 201