

Reconnaissance faciale, une menace pour la vie privée ? | Le Net Expert Informatique



Reconnaissance faciale, une menace pour la vie privée ?

Pour le «Washington Post», les nombreuses applications capables de reconnaître les visages créent des bases de données biométriques dangereuses pour la «confidentialité numérique». «L’anonymat en public pourrait être une chose du passé.» Dans le Washington Post du 11 juin, Ben Sobel, chercheur au Centre sur la vie privée et la technologie de l’école de droit de Georgetown, consacre un article au risque qui pèse sur notre «confidentialité biométrique». Selon lui, les technologies de reconnaissance faciale se développent à la vitesse grand V sous l’impulsion du marketing individualisé. Et pas toujours de manière très légale. Aux Etats-Unis, Facebook fait l’objet d’un nouveau procès en action collective, concernant la violation du droit à la protection des données personnelles de ses utilisateurs. En cause, le réseau social serait en train de créer «la plus grande base de données biométriques privées au monde» sans demander assez explicitement le consentement de ses utilisateurs comme l’explique le site Sophos. Le gouvernement américain et le département du Commerce auraient déjà invité des associations de défense de la vie privée ainsi que des représentants des grandes entreprises de ce secteur comme Google et Facebook pour essayer de réglementer l’usage de ces technologies. Mais pour le moment, seul l’Illinois (2008) et le Texas (dès 2001) ont des lois interdisant l’utilisation de cet outil sans le «consentement éclairé» des utilisateurs, explique Ben Sobel. Selon lui, l’issue de ce procès, qui devra déterminer si Facebook a enfreint la «Biometric Information Privacy Act» (BIPA) de l’Illinois, déterminera l’avenir des applications de reconnaissance faciale sur le marché. Il encourage ainsi les Etats-Unis à adopter une loi fédérale pour garantir la «confidentialité biométrique» des Américains. LE BOOM DES APPLICATIONS DE RECONNAISSANCE FACIALE FaceNet (Google), Name Tag (FacialNetwork) ou encore Moments (Facebook). Toutes ces applications utilisent des algorithmes de reconnaissance faciale. Et pour les imposer sur le marché, les entreprises sont prêtes à tout pour mettre leur adversaire échec et mat. FaceNet, la technologie développée par le géant Google, possède une précision de 99,63 % selon Ben Sobel. Elle est actuellement utilisée par Google Photos dans ses versions non européennes. Dans la même lignée, Name Tag, développé par FacialNetwork, ambitionne de fonctionner sur les Google Glass. Cette application permettrait de rassembler tous les profils sur les réseaux sociaux disponibles sur Internet (Twitter, Instagram, Google+ et sites de rencontres américains) selon un article du Huffington Post. Une application qui pourrait permettre d’avoir le profil social de quelqu’un en temps réel. Parmi les fonctionnalités envisagées, il y aurait par exemple celle de révéler la présence de quelqu’un dans les bases de données criminelles. Pour le moment, Google a refusé que NameTag soit disponible sur ses Google Glass, pour des questions de problèmes de respect de la vie privée... Mais il n’est pas le seul à s’engouffrer dans ce marché. Depuis 2011, Facebook utilise un système de suggestion de tags (identifications) sur les photos. Bien qu’interdit en Europe, Deepface, l’algorithme expérimental du réseau social, serait capable de reconnaître les gens à leur posture corporelle. De fait, son algorithme utilise ce que l’on appelle des «poselets». Inventés par Lubomir Bourdev, ancien chercheur de Berkeley œuvrant désormais chez Facebook IA Research. Ceux-ci repèrent les caractéristiques de nos visages et trouvent ce qui nous distingue de quelqu’un d’autre dans une pose similaire, explique un article de Numérama (http://www.numerama.com/magazine/33826-meme-de-dos-facebook-sait-vous-reconnaître-sur-les-photos.html). Mais Facebook ne s’arrête pas là. En juin, le réseau social a présenté Moments, une application permettant de partager de manière privée des photos avec des amis utilisant elle aussi une technologie de reconnaissance faciale. D’ores et déjà disponible gratuitement aux Etats-Unis, elle permet à un utilisateur d’échanger avec ses amis des photos où ils figurent de manière synchronisée. Une vidéo en explique les rouages : Moments ne devrait pas s’exporter en Europe de sitôt, puisque l’UE exige la mise en place d’un mécanisme d’autorisation préalable qui n’est pas présent sur la version américaine. Et ce, bien que les utilisateurs puissent désactiver les suggestions d’identification sur les photos, via les paramètres de leur compte. L’INQUIÉTUDE AUTOUR DU SUCCÈS DE CES TECHNOLOGIES En 2012, une recommandation formulée par le G29, qui réunit les commissions vie privée de 29 pays européens, mettait déjà en garde contre les dangers de la reconnaissance des visages sur les médias sociaux. Notamment concernant les garanties de protection des données personnelles, tout particulièrement les données biométriques. Pour le moment relativement bien protégés par la législation européenne, nous ne sommes pas pour autant épargnés par ces outils. Tous les jours, 350 millions de photos sont téléchargées sur Facebook, selon Ben Sodel. Or, le public semble majoritairement insouciant face à la diffusion de son identité (nom, image...), souligne InternetActu. A l’exemple de l’application How Old mise en ligne fin avril, qui se targue de deviner votre âge grâce à une photo. Corom Thompson et Santosh Balasubramanian, les ingénieurs de Microsoft à l’origine du projet, ont été surpris de constater que «plus de la moitié des photos analysées» par leur application n’étaient pas des clichés prétextes mais de vraies photos, rapporte le Monde. Mais le succès (bien qu’éphémère) de cette application démontre bien que le public n’est pas vigilant face à la généralisation de la reconnaissance faciale. Un peu comme avec la diffusion des données personnelles au début de Facebook. Il ne s’agit pas tant du problème de stocker des photos d’individus que de mémoriser l’empreinte de leur visage. Entre de mauvaises mains, ces bases de données pourraient mettre à mal notre «confidentialité biométrique».
Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l’hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d’informations complémentaires ? Contactez-nous Denis JACOPINI Tel : 06 19 71 79 12 formateur n°93 84 03041 84
Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en cybercriminalité et en déclarations à la CNIL, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu’intervenant de confiance, la sensibilisation ou la formation de vos salariés afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d’entreprise. Contactez-nous
Cet article vous plait ? Partagez ! Un avis ? Laissez-nous un commentaire ! Source : http://ecrans.liberation.fr/ecrans/2015/06/26/reconnaissance-faciale-une-menace-pour-la-vie-privee_1337015 Par Camille PETTINEO