

V době umělé inteligence a rozpoznávání obličeje jsou osobní údaje viditelné na první pohled (video)

 necenzurovanapravda.cz/2024/10/v-dobe-umele-inteligence-a-rozpoznavani-obliceje-jsou-osobni-udaje-viditelne-na-prvni-pohled-video

11 října, 2024

Víte o tom, že dnes již existují natolik dokonalé šmírovací nástroje, že vás umí identifikovat i v davu na ulici? A to nemusíte být zrovna registrovaný kriminálník. Kdokoli tak může jen na základě skenu obličeje zjistit vaši identitu – a to včetně adresy a dalších údajů.

Přesně to dokázali dva studenti, kteří na zjištění identity náhodných kolemjdoucích potřebovali dnes dostupné prostředky. S takovou technikou nebude problém udržet obyvatelstvo v případě potřeby v 15minutových chytrých městech...

Dva studenti z Harvardské univerzity použili pár „chytrých brýlí“ meta a umělou inteligenci, aby ukázali, že ochrana našeho soukromí není zaručena ve věku digitální kontroly, kdy jsou technologie umělé inteligence a rozpoznávání obličeje na vzestupu.

AnhPhu Nguyen a Caine Ardayfio ve svém testu použili chytré brýle Ray-Ban Meta, kteře vyvinula společnost Marka Zuckerberga Meta a EssilorLuxottica.

Tyto brýle mají v rámu integrované dvě kamery, reproduktory, mikrofon a touchpad. Jedná se o nejnovější z řady chytrých brýlí, které uvedly na trh velké společnosti jako Google a Snap Inc. a jsou součástí plánů Facebooku na metaverse.

Výsledek byl šokující: Pomocí těchto brýlí a softwaru, který studenti vyvinuli, byli schopni použít stávající vyhledávače a technologii rozpoznávání obličejů k identifikaci lidí na ulici přímo na místě.

Jednoduše tím, že se díváte na lidi, zjistíte o nich vše. Data od nedobrovolně testovaných subjektů byla shromážděna během minuty v aplikaci, kterou vyvinuli.

Ardayfio vysvětluje, jak to funguje:

„Dostanete video z brýlí a my máme robota, který vezme tato video data a pokusí se v nich najít obličej. Když najde obličej, nahraje ho do nástroje zvaného ‚PimEyes‘, který v podstatě provádí zpětné vyhledávání obrázků, kdy pořídíte obrázek a najdete další podobné obrázky na internetu.

Jakmile budou mít adresy URL těchto dalších obrázků, použijeme AI ke zjištění jména osoby. Jakmile najdeme jméno, použijeme databáze, jako jsou databáze registrace voličů, abychom našli adresu, telefonní číslo nebo něco podobného.“

Studenti zaznamenali výsledky svého experimentu ve videu, které sdíleli na sociálních sítích. Když testovaným ukázali, jaké osobní informace o nich rychle zjistili, byli ohromeni a zděšeni.

„Byli jsme překvapeni, kolik dat lze nyní extrahovat. Většina lidí ani nevěděla, že tyto nástroje pro zjištění adresy osoby podle jména existují. Proto jsme se při zahájení vývoje rozhodli vytvořit také průvodce, který problém okamžitě vyřeší,“ říká Nguyen.

Studenti tedy sestavili seznam návodů, jak se odhlásit z vyhledávačů pro rozeznávání obličejů a jak se chránit před únikem dat.

Ve zprávě o testu Nguyena a Ardayfia Boston *Globe* poznámeneal, že federální zákon USA nezakazuje používání systémů rozpoznávání obličejů, i když se právní normy v jednotlivých státech liší.

Ohodnoťte tento příspěvek!

■ ■ ■ [Celkem: 11 Průměrně: 4.9]