

# VĚDÍ O VÁS NAPROSTO VŠECHNO. CIA se zaměřuje na data z aplikací ve Vašem mobilu

- editor007 | 2. června 2024

**SVĚT: Díky nákupu těchto údajů od soukromých firem mohou agentury tvrdit, že toto špehování je „open source“, založené na „veřejně dostupných“ záznamech.**

Ředitelka Národního zpravodajství (DNI) Avril Hainesová, která dohlíží na 18 samostatných agentur tvořících širší „zpravodajskou komunitu“ - včetně CIA, FBI a NSA - zveřejnila „rámec politiky pro komerčně dostupné informace“. Nejenže jde o vůbec první veřejné potvrzení ze strany amerického vládního činitele, že špionážní subjekty na straně Států získávají rozsáhlé údaje o soukromých občanech od zprostředkovatelů třetích stran, ale přiznává, že tyto údaje jsou hluboce citlivé. Ačkoli údajně stanoví limity pro využívání těchto informací špióny, podrobnosti jsou vágní nebo neexistují.

„Komerčně dostupné informace“ (CAI) se týkají údajů shromážděných o jednotlivcích, obvykle prostřednictvím jejich chytrých telefonů a aplikací, které používají, a prodávaných třetími stranami. Prostřednictvím různých triků a bezohledného využívání mezer v právních předpisech získaly americké zpravodajské služby informace, které nejsou přístupné běžným občanům a k jejich získání by bylo obvykle třeba soudem schváleného povolení k prohlídce. Díky nákupu těchto údajů od soukromých zprostředkovatelů však mohou špionážní agentury stále tvrdit, že toto špehování je „open source“, založené na „veřejně dostupných“ záznamech.

Zvláště bohatým zdrojem CAI jsou údaje získané z digitální reklamy. Reklamní prostor v aplikacích a na webových stránkách se prodává na burzách s nabídkami v reálném čase (RTB) a jako bonus jsou často zahrnuty údaje o poloze a další údaje o uživateli, aby bylo zajištěno optimální cílení reklamy. Mnoho zprostředkovatelů dat se vydává za inzerenty, aby z nabídek „vyškrabali“ informace o uživateli a pak je prodali za účelem zisku. Hodnota těchto údajů a možnosti jejich zneužití jsou obrovské.

# Real-Time Bidding Process



Například dodavatel zpravodajských služeb kdysi využil údaje získané ze seznamovací aplikace Grindr ke sledování pohybu homosexuálních zaměstnanců americké vlády. Údaje RTB také využívaly skupiny bojující proti potratům ke sledování žen, které navštěvují kliniky plánovaného rodičovství v USA. Pozitivnější je, že data RTB pomohla vytvořit spis o spolupracovnících obchodníka s dětmi Jeffreyho Epsteina, který sledoval majitele chytrých telefonů, kteří navštívili jeho soukromý ostrov, na adresy v USA a dalších zemích.

## „Osobní atributy“

Jak uvádí Hainesův rámec, „komerční subjekty v současné době shromažďují a agregují bezprecedentní množství osobních údajů“ „z různých zdrojů“. Patří sem „mobilní telefony, automobily, domácí spotřebiče a další osobní zařízení“. Tyto informace jsou pak zpřístupňovány „různým odběratelům, včetně ziskových a neziskových subjektů, zahraničních protivníků a domácích i nadnárodních organizací“. Americká „zpravodajská komunita“, jak přiznává ředitel, běžně využívá možnosti „přístupu, shromažďování a zpracování“ těchto CAI.

CAI je běžně využívána „při plnění úkolů a tyto informace často poskytují kritickou zpravodajskou hodnotu“, tvrdí Haines. Přesto „tyto soubory dat mohou odhalit citlivé a intimní osobní údaje a činnosti“, připouští. Přiznané množství údajů, k nimž má CIA a spol. přístup o soukromých občanech prostřednictvím zprostředkovatelů třetích stran, není nic jiného než znepokojující. Např:

„Osobní atributy, stavy nebo identifikátory, které lze vysledovat u jedné nebo více konkrétních osob v USA, [včetně] rasy nebo etnického původu, politických názorů,

náboženského přesvědčení, sexuální orientace, pohlavní identity, lékařských nebo genetických informací, finančních údajů nebo jakýchkoli jiných údajů, jejichž zveřejnění by mělo podobný potenciál způsobit podstatnou újmu, rozpaky, nepříjemnosti nebo nespravedlnost osobě nebo osobám popsaným v těchto údajích.“



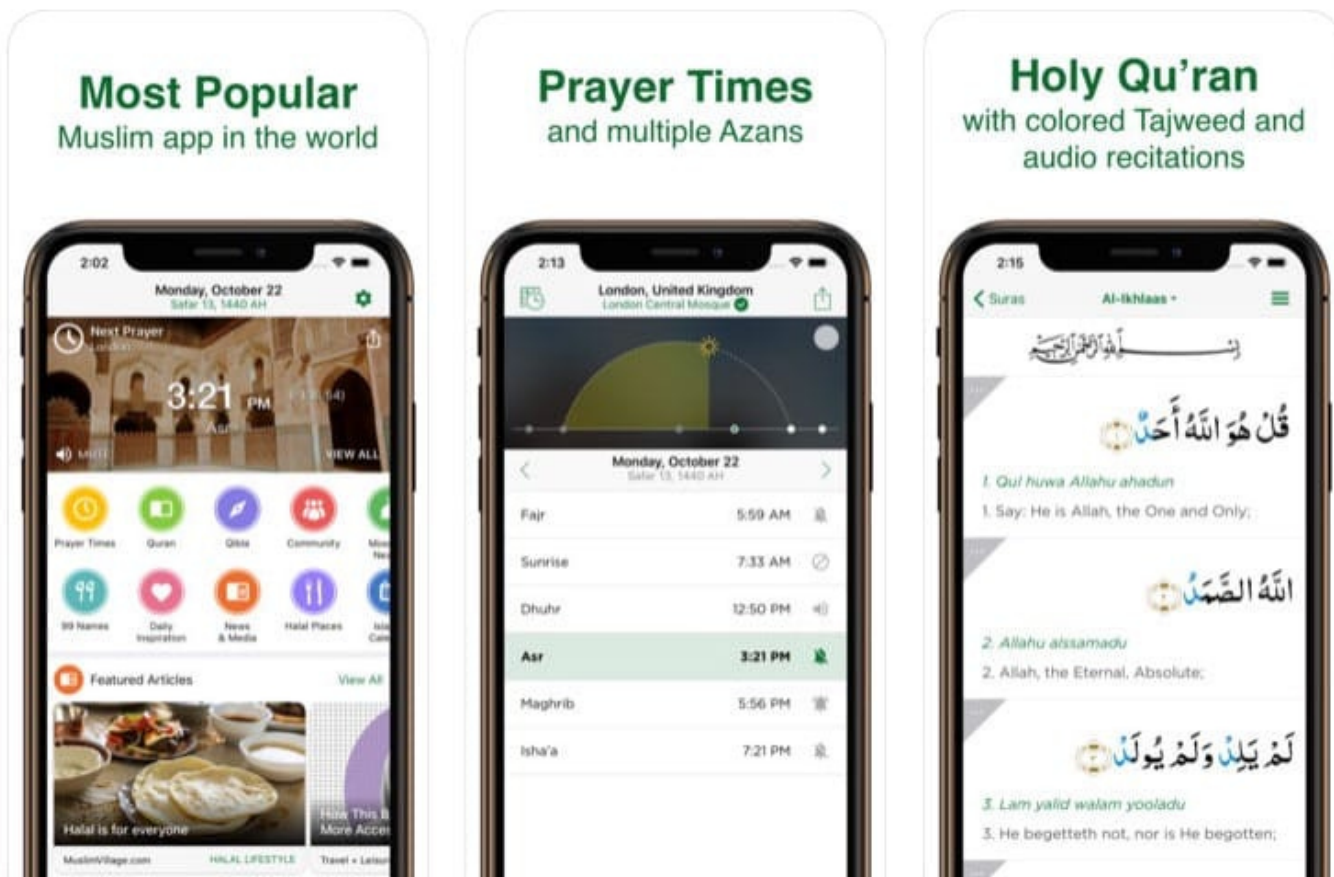
*Avril Haines*

Kromě toho mohou CAI zahrnovat „údaje, které zachycují citlivé činnosti“ cílových osob a skupin. „Citlivé činnosti“ jsou definovány jako jakékoli, „které po delší dobu vytvářejí vzorec života; odhalují osobní příslušnost, preference nebo identifikační znaky; usnadňují předvídání budoucích činů; umožňují cílenou činnost; odhalují výkon práv a svobod jednotlivce“. Děsivé věci – ale Hainesův rámec nenabízí téměř žádné jasné vodítka, jak bude nákup a používání CAI americkými zpravodajskými službami omezen.

### **„Geolokace osob“**

Dokument tvrdí, že „dodatečné vyjasnění“ bude chránit soukromí občanů, ačkoli v jeho obsahu žádné nenabízí. Znepokojivé je i to, že samotné špiónážní agentury mají za úkol formulovat „ochranná opatření přizpůsobená citlivosti“ CAI, které shromažďují, a vypracovávat výroční zprávy o využívání těchto údajů. Neexistuje žádný požadavek, aby zpravodajské služby za jakýchkoli okolností vymazaly všechny staré zakoupené údaje – a to ani v případě, že byly shromážděny omylem – a co je nejnepokojivější, neexistují žádná omezení týkající se toho, jaké informace mohou a nemohou být zakoupeny.

To je obzvláště znepokojivé, protože je zřejmé, že některé aplikace pro chytré telefony jsou ochotny přijímat pokyny od soukromých zpravodajských firem a zprostředkovatelů údajů o tom, jaké informace mají o svých uživatelích shromažďovat, které jsou pak prostřednictvím třetích stran předávány americkým špiónážním subjektům. Bylo potvrzeno, že aplikace MuslimPro, která nabízí denní modlitební kalendář a kompas směřující k Mekce, začala tajně sledovat polohu uživatelů na přímou žádost zprostředkovatele, který následně tyto informace prodal vládním klientům.



Jiní zprostředkovatelé slouží převážně nebo výhradně státním organizacím. Patří mezi ně Babel Street – „společnost, která se zabývá přeměnou dat na znalosti s využitím umělé inteligence“ -, která poskytuje údaje o poloze americkým agenturám včetně DEA, ICE, IRS, Secret Service a ministerstva financí, a firma Barbaricum, která se zabývá „integrovanou komunikací“. Smlouva v hodnotě 5,5 milionu dolarů, kterou společnost získala od ICE v roce 2020, odkazuje na její schopnost „geolokace osob nad rámec standardního geotagování“, „monitorování a analýzy všech aktivit na sociálních sítích“ na všech platformách, včetně „zahraničních/temných/hlubokých webových sociálních sítí v REÁLNĚM ČASE [důraz v originále]“, a zároveň vytváření „psychologických profilů“ cílů.

Na jiném místě smlouva uvádí, jak může společnost Barbaricum vytvářet „psychologické profily“ cílů a „zjišťovat, zda uživatel smazal zprávy, a poskytovat obsah ze smazaných účtů a/nebo smazaných zpráv“. Před zveřejněním „politického rámce“ ředitele Národního zpravodajství nebyl rozsah špiónážních aktivit CAI prováděných americkými špióny znám. Bylo nutné, aby nezávislí výzkumníci a skupiny pro kampaně dali dohromady hrubý nástin z omezených veřejně dostupných záznamů.

Nyní je stejným agenturám, které po léta zcela beztrestně používaly a zneužívaly soukromé údaje uživatelů, svěřena odpovědnost za vytváření vlastních interních zásad pro to, co je a co není přípustné zachycovat, analyzovat, využívat a konat. Hlídní kurníků liškami ještě nikdy nedopadlo dobře.

Zpracoval: Cecília Jílková/Reportéři on-line!

AUTOR: Kit Klarenberg

[ZDROJ](#)