

Soukromí jako asána: nauč se ho držet (a malý návod k tomu)

„Nemám co skrývat...“

„Stejně o mně ví všechno...“

„Slušný člověk se nemusí bát...“

„Nedělám nic zakázaného...“

„To kdyby měli monitorovat každého...“

„O to se nikdo nezajímá...“

Internet je tak trochu jiný vesmír. Neplatí zde pravidla, na která jsme po generace zvyklí. Některá jsou úplně otočená. V první řadě se zde nezapomíná, prakticky nikdy. Kopírování je levnější než mazání. A poslední paradox, narozdíl od analýzy hromady papírových šanonů, čím více dat je, tím lépe se s nimi pracuje.

Zdánlivě nevinná zpráva, jako poblahopřání babičce k narozeninám nebo domlouvání se s kámošem na kafe, jsou pak puzzlíkem skládačky, který tvoří tvůj virtuální profil mnohem věrohodnější, přesnější. Vypovídající jsou obsahy i četnosti zpráv, provázanost uživatelů, vyhledávání nebo geografická poloha (která nejde snadno vypnout, protože se bere i z internetového připojení - operátor mobilní sítě zná vaši polohu neustále s přesností desítek metrů). V praxi taková data mají cenu tisíce korun za uživatele, ročně¹. Což vysvětluje, proč zejména **reklamní společnosti**^{2 3} (Facebook ~ Meta nebo Google, který čte všechny emaily⁴) jsou nejen největší firmy světa, ale mohou si dovolit poskytovat služby „zdarma“.

Pokud neplatím za produkt, nejspíš jsem sám produktem.

Jenže zde to nekončí. Tato data se dle podmínek (která odsouhlasujeme, pokud chceme používat takové služby) dále obchodují, legálně. Například PayPal (platební brána) poskytuje vaše osobní údaje (včetně možných podrobností o nákupu samotném) více než 600 (!) třetích stran⁵.

¹ <https://security.it.utah.edu/data-privacy-week/price-personal-data.php>

² <https://www.financestrategists.com/wealth-management/stocks/alphabet-stock/>

³ <https://blog.valuesense.io/how-meta-meta-platforms-makes-money-in-2025/>

⁴ <https://policies.google.com/terms>

Jak to, že tato data mají takovou hodnotu?

Lidstvo totiž vynalezlo úžasný nástroj, říká se mu strojové algoritmy nebo umělá inteligence - AI. Je založen na poměrně jednoduchém principu, a proto umožňuje počítat s obrovským množstvím dat. AI sice není inteligentní, ale dokáže zpracovávat enormní množství dat. Pokud jich má dostatek, dokáže hledat propojení, která ani člověk není schopen zachytit. Čím více jich má, tím lépe, „inteligentněji“ a přesněji pracuje.

Jeden příklad, lékaři chtěli AI naučit z rentgenových snímků rozeznávat nemocné pacienty. AI se to skutečně naučilo. Umělo rozeznávat druhy jednotlivých onemocnění, podobně jako zkušený lékař. Jenže se přišlo i na to, že AI dokázalo propojit mnohem více souvislostí, než jakýkoliv člověk. S velmi vysokou přesností (přes 90%) umí ze snímku pouze samotných plic rozeznat rasu pacienta.⁶

AI je tedy výborný nástroj k práci s ohromnými, nudnými a zdánlivě nesouvisejícími daty.

Může fungovat jako takový filtr na eshopu. Po zadání parametrů dokáže najít osoby, které vyhovují zadaným kritériím. Dokonce umí předvídat, jak lidi z různých kategorií oslovit. Co jim říct, pokud chceš jako politik jejich hlas.

Přijde ti to přehnané? Odhalil se třeba případ ovlivňování 87 milionů uživatelů Facebooku v roce 2014 právě kvůli volbám (ano, strojové učení je zde déle než nám známé AI jako ChatGPT)⁷.

Zpět k nevinným datům. V některých zemích jako Čína, se AI nástroje již používají k hledání nevyhovujících menšin v populaci a jejich genocidě⁸. Čína mimochodem plně kontroluje a monitoruje u nich nejpoužívanější aplikaci WeChat, která umožňuje nejen psaní zpráv ale i platby⁹, což je v podstatě většina tvého soukromí (proč jsou informace o platbách podobně zásadní píšou níže). Je to téměř úplný popis tvé interakce se světem.

⁵ <https://www.paypal.com/ie/legalhub/paypal/third-parties-list>

⁶ [https://www.thelancet.com/journals/landig/article/PIIS2589-7500\(22\)00063-2/fulltext](https://www.thelancet.com/journals/landig/article/PIIS2589-7500(22)00063-2/fulltext)

⁷ https://en.wikipedia.org/wiki/Cambridge_Analytica

⁸ <https://giswatch.org/node/6165>

⁹ <https://worldpopulationreview.com/country-rankings/wechat-users-by-country>

Pokud se tato data centralizují (sbírají jedním subjektem), může je využít i šikovný zločinec. Nebo dokonce kdokoliv, kdo se (třeba i nechtěně) dostane do vedení naší společnosti.

Nechci, aby mne kdokoliv znal lépe, než já sama, přesně z důvodů popsaných výše. Toto nebezpečí nelze potlačit žádným slibem, podpisem či zákonem. Pouze tím, že tyto informace v první řadě neodevzdám. Protože jak jsem psala na začátku, princip internetu je nezapomínat.

Digitální svět je zkrátka příliš nový na to, abychom si hned uvědomili všechny jeho rozdíly a dopady. Ve fyzickém světě existuje zase spousta jiných nástrah, na které jsme vymysleli účinné metody. Třeba eliminovali nemoci z špinavých rukou. Přitom nejsme vystrašení z bacilů, prostě si je umyjeme :)

Pokud existují nástroje na internetu, které vrací soukromí do tvých rukou, nedává mi smysl riskovat cokoli z toho. Jednoduše změním ikonku zelenou (WhatsApp) na modrou (Signal).

Internetové soukromí ctím. Je to základní forma hygieny v digitálním světě.

Signal, o co tedy jde?

Je to soukromá alternativa WhatsAppu, plně šifrovaná a téměř naprosto shodná na používání (jen s více vychytávkami a není propojena s Facebookem). Začít používat Signal znamená jen ho stáhnout, vyplnit telefon a psát si s přáteli. Po importování kontaktů možná budeš překvapen, kolik lidí ho má ve tvém okolí. Nastává otázka, nic za něj neplatím, nejsem tedy také produktem? Signal je narozdíl od WhatsAppu zdarma díky dobrovolným příspěvkům, které financují jeho běh a vývojáře (příspěvek můžeš poslat kdykoliv i ty), nebo díky programátorům, kteří ve volném čase přispívají do plně zveřejného kódu. Protože je celá aplikace „odhalená“, neexistují zde „zadní vrátka“ a každý s náležitými znalostmi je schopný celou aplikaci a protokol kontrolovat a auditovat¹⁰.

Tento přístup otevřeného či veřejného kódu se nazývá „open-source“. Doporučuji u služeb, které používáte, hledat alternativy právě open-source. Pozor, není to vždy zárukou soukromí, ale téměř jistou podmínkou.

¹⁰ <https://bluegoatcyber.com/blog/signal-app-review-security-and-privacy-evaluated/>

Aplikace je navržena tak, že servery Signalu (prostě místo na internetu, které přeposílá zprávy mezi účastníky) nemají z principu možnost vidět nejen obsahy zpráv (díky šifrování), ale dokonce ani metadata (jako třeba kdo tuto zprávu odesílá, pouze ji doručí) nebo členy skupin.

Hovory jsou šifrované (i skupinové), stejně tak videohovory nebo v případě aplikace na počítači sdílení obrazovky. Plně soukromě.

Veškeré zprávy, fotografie či videa jsou zašifrovány a uloženy pouze v zařízeních, mezi kterými probíhá komunikace a nad daty se neprovádí žádná dodatečná analýza. Data neleží nikde mimo. To vše víme, protože je transparentní.

Ještě k WhatsAppu, Messengeru nebo třeba Telegramu. Tyto aplikace nenabízí tento otevřený, „veřejný“ kód. Tedy nikdo do nich ani trochu nevidí. Motivaci k tomu mohou mít různou, pro nás uživatele to znamená, že bez ohledu na to, co deklarují, NELZE garantovat žádné soukromí (pokud ano, „A můžeme ho vidět?“ :)). WhatsApp i ostatní aplikace společnosti Meta navíc v podmínkách i přiznávají, že data využívají pro personalizování reklam a sdílením s třetími stranami.

Změň svůj digitální život. K lepšímu.

Stojí jen maličké a jednorázové úsilí. Signal není jediná aplikace (a upřímně, existují co se hlediska soukromí a anonymity týče i lepší, třeba SimpleX nebo Element), ale nenašla jsem lepší soukromý komunikátor, tak jednoduchý na používání jako aktuální „mainstream“ (dokonce shodný). Signal už teď aktivně používají desítky milionů lidí po celém světě a má stovky milionů stažení.

Nakonec pro tebe mám jednoduchý návod, jak si (nejen!) mé členství můžeš zakoupit co nejsoukromněji.

1. Pokud to není potřeba (komunikace s úřadem), používej co nejběžnější pseudonym (více na stránce <https://peter.horvath.digital/>¹¹), třeba Jan Novák.
2. Používej e-mail, který neobsahuje tvé jméno a ideálně umožňuje masky – jednorázové adresy pro každý nákup. Emaily respektující soukromí jsou třeba proton.me nebo tuta.mail (pravý opak Gmailu). Pozor, z principu fungování je e-mail nejméně soukromá komunikace VŮBEC, tak ho používej jen když musíš.

¹¹ V češtině: <https://poboril.notion.site/Jsem-Jan-Nov-k-a2dbf3737399a84c0b9ba474ff971d78cc>

3. Napiš mi zde na Signal (záložka kontakt) a vyřeš se mnou platbu pomocí kryptoměn a nebo na lekci hotově. V Herohero pak nemusíš zadávat už žádné další osobní údaje.

That's it :) Jako komunita máme skupinu taky právě na Signalu, kdyby ses chtěl(a) připojit. Pokud některý z bodů nemůžeš splnit (třeba ten 3), i každý jeden se počítá.

Cože, platit hotově? Nebo kRyPtoMěňOu??

Už rozumíme hodnotě všech (nejen) textových dat co necháváme na internetu a jejich použití. To však stále není naše celá komunikace s okolním světem. Velice zásadní je komunikace jazykem peněz. Peníze jsou totiž univerzálním jazykem celého světa. Ukazují vzácnost. Vyjadřují subjektivní hodnotu čehokoliv, co nás napadne. Sdělujeme jimi také své skutečné preference.

Pokud v zelenině necháme 20 Kč za jablko, tak tím říkáme, že pro nás má momentálně vyšší hodnotu, než těch 20 Kč. Říkáme to bez ohledu na status, který pak na Twitteru napíšeme o tom, jak jsou jablka strašně drahá. Jinak bychom si to jablko v první řadě vůbec nekoupili.

Podobně, bez ohledu na naše zprávy kamarádům o škodlivosti cigaret, platba za krabičku vypovídá o našich skutečných preferencích. Pokud někdo nebo něco dokáže monitorovat naše „finanční konverzace“, hodnota takových dat je minimálně podobná těm textovým. Takové firmy (teď tě možná nepřekvapím) existují, třeba Google Pay, Visa, MasterCard nebo zmiňovaný PayPal...

Řešení je používat hotovost s téměř absolutním soukromím a anonymitou. Podporujete zároveň i soukromí protistrany, obchodníka. Navíc jsou odolné vůči cenzuře - platba je také komunikace a elektronické platby a zůstatky se mohou zmrazovat.

Hotovost však nejde použít vždy a navíc digitální platby mají některé své výhody (jsou třeba pohodlnější). Cena za toto pohodlí při používání ale může být neúměrně vysoká.

Pokud by však existoval bankovní účet, který umí dělat transakce soukromě a třeba ani jeho zůstatek není vázaný na tvoje jméno, navíc nejde efektivně nijak cenzurovat, může se úroveň soukromí rovnat hotovosti.

A to je jeden z důvodů, proč vůbec kryptoměny vznikly.

Založit si „účet“, přesněji peněženku, znamená jen vytvořit náhodný klíč a ten nezapomenout. To vytváření je rychlá matematická operace podobná házení kostkou. Trvá to asi sekundu a nepotřebuješ na to kromě aplikace peněženky vůbec nic. Pak nastává otázka, jak získat nějakou tu kryptoměnu na takto vytvořený prázdný účet, ale to už je mimo rozsah tohoto dokumentu.

Důvodů proč používat kryptoměny je ještě více, ale jak jsem psala, je to nad rámec tohoto dokumentu (a na tvoje dlouhé samostudium :)).

Nakonec zmíním, že drtivá většina kryptoměn mohou být podvod, a proto se minimálně ze začátku zaměř pouze na Bitcoin (později možná Monero nebo Zcash). Nepísané pravidlo, nerozumíš-li opravdu Bitcoinu, nezajímej se o jiné.

Nehledej zde zbohatnutí, hledej alternativu. Věnuj čas vzdělání, ne nakupování. A pokud se budeš zabývat tématem více do hloubky, doporučuji se také zaměřit na pochopení slovního spojení KYC (a co je aplikace Vexl).

„Postupem času bude stále náročnější se k těmto nástrojům dostat (viz chat-control¹², ověřování věku (podrývající anonymitu) a podobné regulace). Nezapomeňte ale, že nástroje pro soukromí vznikly, jsou tu a efektivně už zakázat nejdou.“

Kdykoliv ve svém životě narazíš na potřebu podobných nástrojů, neboj se věnovat čas průzkumu a nebo kontaktovat známé, kteří by o tomto tématu mohli vědět trochu více. Třeba přes platformu Signal.

Lokah Samastah Sukhino Bhavantu (लोकाः समस्ताः सुखिनो भवन्तु)

"May all beings in the entire world be happy and free"

¹² Krátké video vysvětlující Chat control (v moment dopsání textu bohužel již schváleného radou Evropské Unie, i když trochu „volnější“ varianty než původně navrhované):
<https://www.youtube.com/watch?v=nsbgkQcvR6I> (zapněte si české titulky)