

Menyulit tidak bermakna peribadi: apa yang dikatakan metadata tentang anda

Kandungan yang disulitkan dan metadata yang kelihatan adalah dua perkara yang berbeza. Apabila perkhidmatan bercakap tentang "penyulitan end-to-end", ia hanya menceritakan separuh daripada ceritanya.

Mangga yang tidak melindungi segalanya

Sebahagian besar perkhidmatan pemesejan hari ini mengiklankan penyulitan end-to-end. Dan ia benar: kandungan mesej dihantar dalam keadaan disulitkan, supaya tiada sesiapa di tengah jalan – malah penyedia perkhidmatan sekalipun – dapat membaca teks tersebut semasa ia sedang dihantar. Sampai di sini, kenyataannya tepat.

Masalahnya ialah kandungan hanyalah sebahagian daripada cerita. Walaupun tiada siapa yang dapat membaca apa yang anda katakan, perkhidmatan tersebut mengetahui perkara lain dengan ketepatan yang sangat tinggi: dengan siapa anda bercakap, pada pukul berapa, seberapa kerap, dari lokasi mana kira-kira, pada peranti apa, berapa banyak mesej yang anda hantar dan berapa banyak yang anda terima, berapa banyak fail yang anda kongsi. Semua ini dipanggil metadata. Dan metadata, dalam banyak kes, mengatakan hampir sama banyak dengan mesej itu sendiri.

Apa yang didedahkan oleh metadata

Seseorang tidak perlu membaca mesej untuk mengetahui banyak perkara. Jika seseorang menelefon atau menulis mesej kepada pakar onkologi setiap pagi Selasa pada pukul sembilan selama enam bulan, tidak perlu mendengar perbualan tersebut untuk menduga apa yang sedang berlaku. Jika dua orang bertukar seratus mesej sehari dan tiba-tiba berhenti melakukannya, anda tidak perlu membaca satu pun untuk memahami apa yang telah berlaku. Jika seorang perunding cukai menerima dua puluh mesej berturut-turut daripada pelanggan yang sama pada malam sebelum penutupan suku tahunan, polanya bercakap sendiri.

Metadata mendedahkan pola tingkah laku: siapa yang berhubungan dengan siapa, apa jadual setiap orang, bila mereka bangun, bila mereka tidur, bila mereka mengembara, pelanggan mana yang paling aktif, hubungan profesional mana yang paling sengit. Pelayan yang mengumpul metadata dapat membina profil mendalam tentang kehidupan peribadi dan profesional mana-mana pengguna tanpa pernah membaca satu pun perkataan daripada apa yang dia tulis.

Ada contoh sejarah yang menggambarkan perkara ini dengan keras. Bekas pengarah NSA, Michael Hayden, merumuskannya secara terus terang pada tahun 2014: "*We kill people based on metadata*". Kenyataan tersebut merujuk kepada operasi ketenteraan AS terhadap sasaran yang dikenal pasti secara eksklusif berdasarkan pola komunikasi mereka. Tiada satu pun mesej yang dibaca. Hanya graf kenalan dan jadual waktu.

Bahawa suatu perkhidmatan mengumpul metadata tidak semestinya bermakna ia akan menggunakannya terhadap penggunanya. Ini bermakna ia mempunyai kapasiti untuk melakukannya, dan bahawa pihak ketiga

dengan akses kepada data tersebut – melalui perintah mahkamah, melalui pelanggaran keselamatan, atau melalui penjualan kepada pihak ketiga jika syarat perkhidmatan membenarkannya – juga mempunyainya.

Akses kepada buku kenalan

Satu lagi vektor yang hampir tidak disedari: senarai kenalan. Sebahagian besar perkhidmatan pemesejan meminta akses kepada buku kenalan telefon semasa mendaftar. Mereka memuat naik semua nombor ke pelayan mereka untuk menunjukkan siapa lagi yang menggunakan perkhidmatan tersebut. Sejak saat itu, syarikat mempunyai peta lengkap hubungan pengguna, walaupun dia belum pernah menulis satu mesej pun kepada sesiapa pun.

Bagi seorang profesional yang tertakluk kepada rahsia profesional – peguam, doktor, pakar psikologi, perunding – buku kenalan tersebut mengandungi pelanggan. Jika buku kenalan telah dimuat naik ke pelayan pihak ketiga, nama-nama pelanggan berada dalam infrastruktur yang bidang kuasa dan polisinya tidak dikawal oleh profesional tersebut. Rahsia profesional tidak pecah pada hari seseorang membocorkan perbualan: ia telah pecah jauh lebih awal, pada saat persetujuan pemuatan naik.

Perbezaan antara menyulit dan tidak mengumpul

Menyulit bermakna melindungi kandungan. Menjadi peribadi bermakna tidak mengumpul apa yang tidak diperlukan. Ini adalah perkara yang berbeza, dan perbezaannya sangat krusial secara operasi. Sebuah perkhidmatan boleh menyulitkan semua mesej dengan sempurna dan pada masa yang sama mengetahui hampir segala-galanya tentang penggunaannya melalui metadata. Kedua-duanya sangat serasi. Malah, ia adalah model perniagaan yang dominan dalam sektor ini.

Persoalan yang tepat untuk menilai privasi sebenar sesebuah perkhidmatan bukanlah "*adakah ia menyulitkan kandungan?*". Persoalan itu telah dijawab selama bertahun-tahun. Persoalan yang tepat adalah: "*metadata apakah yang dihasilkannya dan di mana ia disimpan?*". Dan yang paling penting: "*metadata apakah yang tidak perlu dihasilkannya?*".

Seni bina yang meminimumkan metadata melalui reka bentuk – bukan melalui janji, bukan melalui polisi dalaman – secara struktur lebih peribadi daripada seni bina yang mengumpul dan menyulitkannya. Kerana data yang tidak wujud tidak boleh dibocorkan, tidak boleh dijual, tidak boleh diserahkan kepada perintah mahkamah atau hilang dalam pelanggaran keselamatan.

Untuk pembaca profesional

Jika aktiviti profesional anda melibatkan rahsia, kerahasiaan, atau sekadar menghormati maklumat pihak ketiga, ada baiknya mengemukakan soalan dalam urutan ini:

1. Adakah aplikasi yang saya gunakan untuk berkomunikasi menyulitkan kandungan? (Mungkin ya.)
2. Adakah ia menyulitkan metadata? (Mungkin tidak.)
3. Adakah ia menghasilkan metadata yang ia *tidak perlukan* untuk beroperasi? (Hampir pasti ya.)
4. Di mana metadata itu disimpan dan di bawah bidang kuasa mana? (Kemungkinan besar di luar Kawasan Ekonomi Eropah.)
5. Adakah pelanggan atau pesakit saya tahu bahawa datanya ada di sana?

Soalan terakhir adalah yang tidak selesai. Kerana jawapan jujurnya dalam banyak kes adalah: tidak.

Artikel ini adalah yang pertama dalam siri tentang cara kerja sebenar alat komunikasi profesional. Edisi seterusnya akan membincangkan pematuhan GDPR dalam mesej dan konsep rahsia profesional dalam era digital.

Sumber dan bacaan lanjut

- Hayden, M. – Kenyataan di Universiti Johns Hopkins, 2014 ("We kill people based on metadata"). Transkrip awam tersedia.
- GDPR (Peraturan EU 2016/679), Pasal 4 dan 5 – definisi data peribadi dan prinsip-prinsip pemrosesan (metadata adalah data peribadi).
- EDPS dan EDPB – pendapat tentang pemrosesan data trafik dan metadata dalam komunikasi elektronik (arahan ePrivacy).

[← Sebelumnya](#)[Sejarah ringkas mohor lilin](#)[Seterusnya](#) → [Rahsia profesional dalam era digital](#)

Bacaan terkini

- [CUADERNOS LIST PREGUNTAS TITLE](#)
- [CUADERNOS LIST SELFHOST TITLE](#)
- [CUADERNOS LIST IDENTIDAD TITLE](#)

Bawa artikel ini bersama anda ke mana sahaja anda memerlukannya.

[↓ Markdown](#) [↓ Teks biasa](#) [↓ PDF](#)

Fail akan dimuat turun ke peranti anda. Dari sana anda boleh menyimpannya, mengimportnya ke Solo2, atau berkongsinya di mana sahaja anda mahu. Cuadernos tidak memutuskan destinasi untuk anda.

Mohor lilin · SHA-256 0b7d3a317073b28785af9960aedeef2f0b56ec67111ccfaa6984fbe11cd84195

Cuadernos Lacre · Penerbitan daripada [Menzuri Gestión S.L.](#) ·
ditulis oleh R.Eugenio · disunting oleh pasukan [Solo2](#).

Laman web ini tidak menggunakan kuki dan tidak memuatkan sumber daripada pihak ketiga. Ia menggunakan pembilang pelawat tanpa nama yang dihoskan sendiri (Umami, di pelayan Eropah kami) dan JavaScript minimum yang diperlukan untuk pilihan tema terang/gelap anda. Tiada penjejak, tiada pemprofilan, tiada perkongsian data. Jika anda ingin mengikuti kami: [RSS](#).