Il depistaggio

Confondere le tracce in rete per salvare la privacy

Roma, 28 gennaio 2016 - Fabio Chiusi, Fellow Nexa Center su Internet e Società, Politecnico di Torino

Condivisione, profilazione, Big Data

- <u>Un trinomio solo apparentemente innocuo</u>
  - **Condividiamo tutto**
    - Non costa nulla (“tutto gratis”)
    - È sempre un bene! (“tutti connessi”)
    - Sinonimo di *esistere* (a livello individuale, sociale, professionale…)

- **Profilazione**
  - Meglio pubblicità personalizzata che generica
  - Facilità/comodità d'uso (es: cookie)
  - I dati sono *anonimizzati*!

- **Big Data**
  - Se i dati sono il petrolio della nostra era, imparare a trattarne quantità sempre più elevate in modo sofisticato significa imparare a ricavarne il massimo del profitto
    - Le cause sono sopravvalutate (bastano le correlazioni!)
  - *Era defining!* (e chi si oppone è un *luddista*)

L’apparenza inganna

- Le piattaforme di condivisione sono gratuite, funzionano e contribuiscono a definire identità e rapporti sociali

- I dati che condividiamo vengono usati a nostro vantaggio per offrirci pubblicità e servizi personalizzati ed efficienti

- Con i Big Data ci attendono miracoli!

- *Allora perché farsi troppe domande su come vengono usati davvero i dati che condividiamo?*

L'inganno

- <u>Risultato</u>:
  - Siamo sempre profilati in modo **opaco** (Chi tratta i nostri dati? Come? Secondo quali regole/norme? Bastano i TOS?)
  - e **sempre controllabili**: le infrastrutture del controllo privato sono spesso le stesse di cui si abbeverano i governi assetati di sorveglianza - dopo Snowden, sempre più *tutti*, democratici e non
  - e siamo comunque felici, **tanto è "gratis"** (no, il prezzo sono le nostre vite, i nostri dati personali - ma *la privacy è morta*, giusto?)

In concreto

- Nonostante Snowden, **14 paesi** hanno introdotto nuove leggi per la sorveglianza di massa in tutto il mondo (Freedom House)
- La censura aumenta per il **quinto anno consecutivo** (id.)
- Paesi democratici come Francia, USA e UK chiedono ***backdoor* alla crittografia** (come la Cina)
- Risposte **emergenziali** restrittive con il pretesto della "sicurezza nazionale" e della lotta al terrorismo (anche se non funzionano)
- E a buona parte dell'opinione pubblica **non interessa**
  - Anzi, la maggioranza degli americani secondo il Pew trova accettabile rinunciare alla propria privacy in cambio di benefici sul posto di lavoro o per i propri dati sanitari
  - In generale, la risposta al Datagate è stata inferiore alle aspettative

Che fare?

- Costituzionalizzare i diritti di base in Internet (Brasile, Italia)

- Chiedere reali riforme politiche (*get a warrant!*, controlli indipendenti, *accountability* delle istituzioni)

- Stabilire una valutazione di impatto di norme che influiscono sui diritti di base online, prima che siano discusse e approvate

- Cifrare tutto (senza *backdoor*)

- **<u>Offuscare</u>**

L'offuscamento

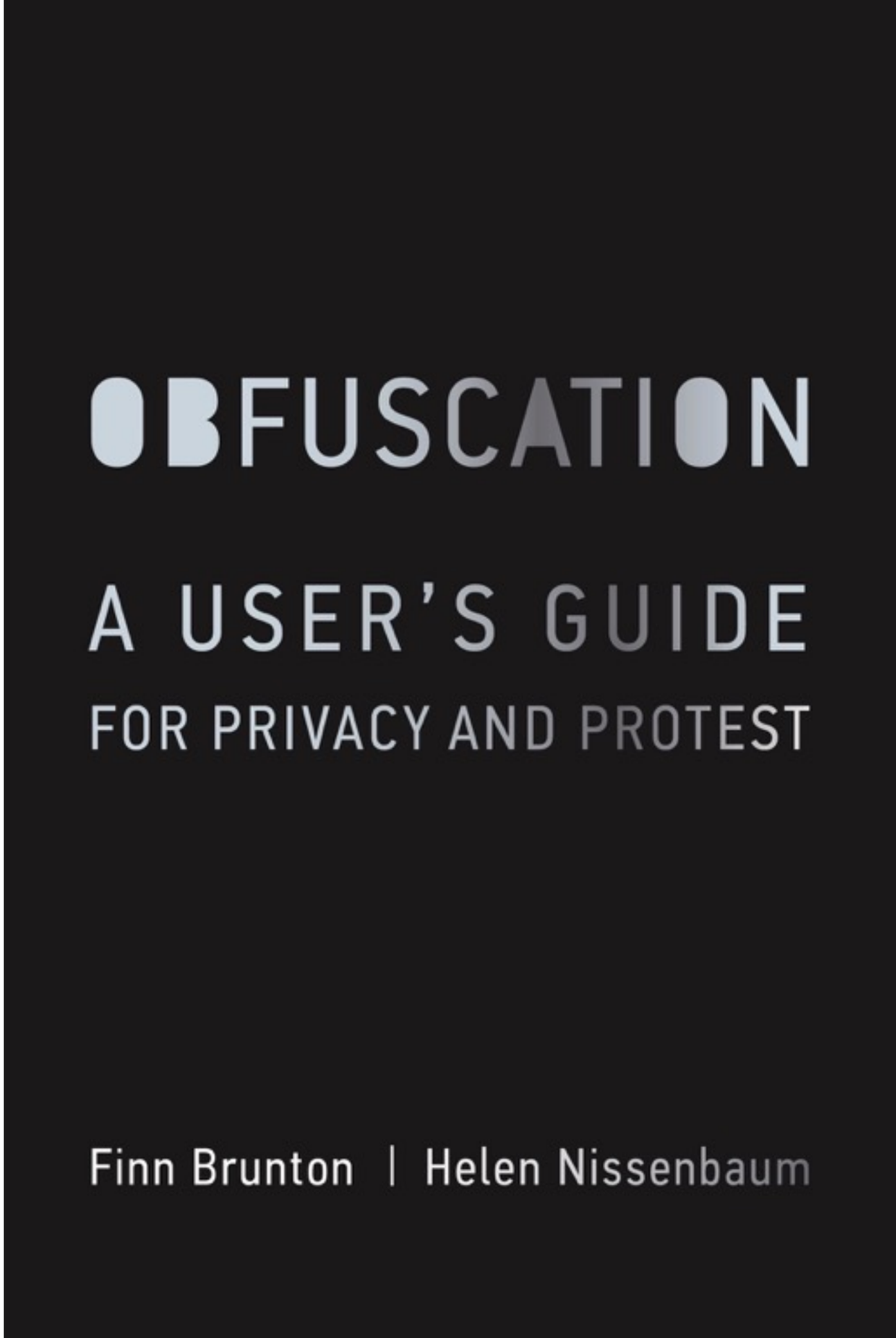
- Il trinomio condivisione-profilazione-Big Data regge **come pericolo** finché è <u>esatto, personale</u>, riguarda proprio ciascuno di noi

- Che accade quando invece confondiamo le nostre tracce, e il tracciamento finisce per riguardare una persona che in realtà **non esiste**?

Entra in gioco il depistaggio

"L'**offuscamento**, nella sua definizione più astratta, è la produzione di rumore modellato su segnali esistenti così da rendere la raccolta dei nostri dati **più ambigua, confusa, difficile da sfruttare e manipolare**, e da ultimo ridurne il valore"

- Finn Brunton e Helen Nissenbaum, 'Obfuscation. A User's Guide for Privacy and Protest'



Una rivoluzione DIY

- “Con questo libro vogliamo avviare una rivoluzione”, ma fatta delle cose quotidiane, di cui già disponiamo, e che possiamo già usare individualmente, ciascuno di noi, per proteggerci e dissentire. L’obiettivo è “mitigare e sconfiggere” la sorveglianza digitale

- L’offuscamento è diverso dall’approccio che mira alla sparizione o alla cancellazione: qui si tratta di aggiungere rumore plausibile ai segnali che emettiamo in rete, come fossimo in mezzo a “una folla in cui ci possiamo confondere e, anche se solo per poco, nascondere”

“Le armi dei deboli”

- “Una adeguata obfuscation può contribuire a proteggere la privacy e a **sconfiggere la raccolta, l’osservazione e l’analisi dei dati**”

- Come?

- Colmando l’asimmetria informativa tra noi che produciamo i dati e chi li raccoglie/analizza in circostanze che potremmo non comprendere, per scopi che non conosciamo, e con usi a noi ignoti (*ora nemmeno loro sanno!*)

- **Non serve a rimpiazzare soluzioni politiche, d’impresa o tecnologiche, non è soluzione per ogni problema** (“è una rivoluzione deliberatamente contenuta e distribuita”), ma “uno strumento che si inserisce in una rete più ampia di pratiche a tutela della privacy” - particolarmente utile per chi non può fare ricorso ad altre modalità di protezione più strutturate (per esempio, a causa della posizione di svantaggio in cui si trova rispetto al potere)

Come depistare il controllore

- Cliccare tutto (es: plugin AdNauseam - il singolo click pubblicitario vale al margine zero)

- Inondare Facebook di informazioni fasulle sulla propria vita e sui propri gusti

- Barare sulla propria localizzazione (es: CacheCloak - “oscuriamo la localizzazione dell’utente circondandola dei percorsi di altri utenti”)

- Far credere che chiunque accede al sito sia un whistleblower (WikiLeaks)

“In situazioni in cui non si può dire no, restano le opportunità per un coro di inutilissimi sì”

- Brunton e Nissenbaum