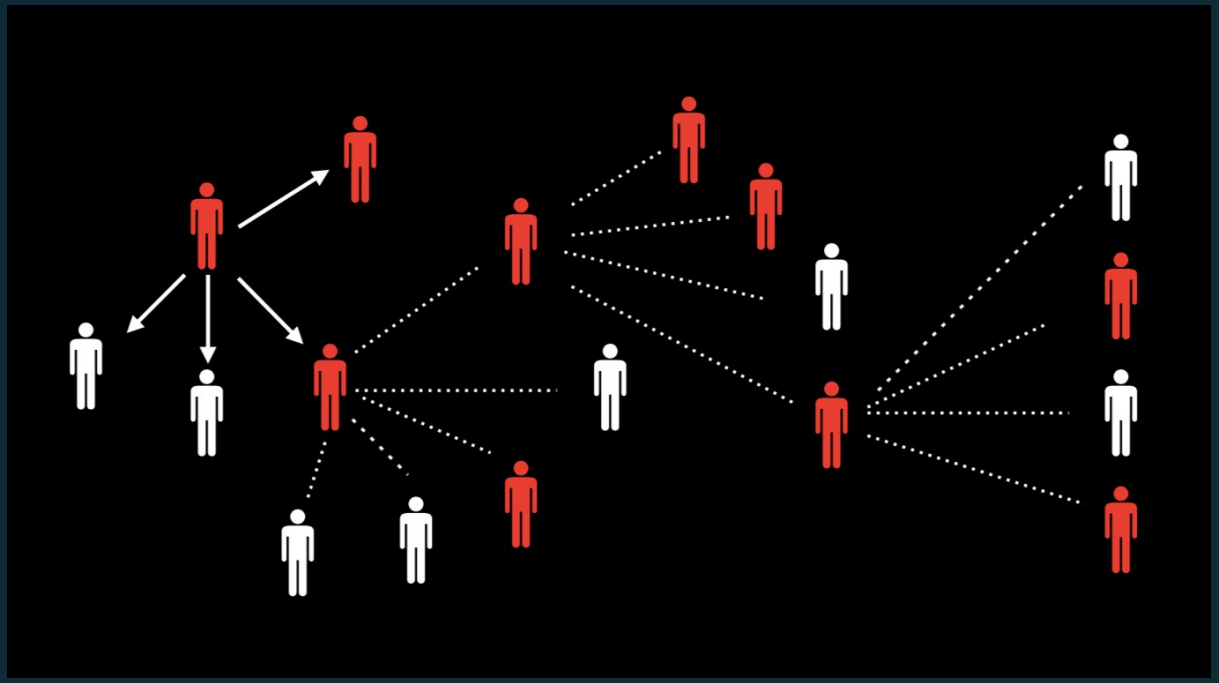
Privacidad: De las revelaciones de Snowden a la era COVID-19



Temes Avançats en Enginyeria de Dades – UPC – 2020-05-11

:~$ whoami

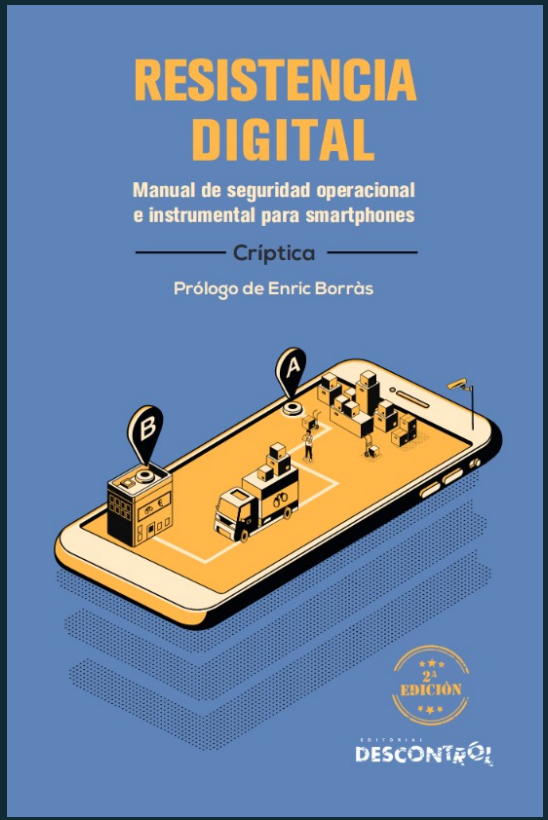
- **Carlos Fernández** (AKA Charlie)
- Cofundador y miembro de Críptica (@CripticaOrg)
- Coautor del libro “Resistencia Digital”, con Críptica
- Coordinador Técnico de *Security Assessment* en INCIDE
- Graduado en Ciencias y tecnologías de Telecomunicación en ETSETB, UPC
- Certificaciones de ciberseguridad: OSCP, CRTE
- Twitter: @cfsgranda

Qué es esta charla

- Una introducción a conceptos básicos de privacidad, vigilancia y sus implicaciones
- Hablaremos de:
  - Qué es Críptica y por qué la privacidad es importante
  - La información que compartimos en abierto
  - La información que compartimos con unos pocos
  - Por qué es importante que la privacidad se proteja por diseño
  - Privacidad en la era post-COVID-19

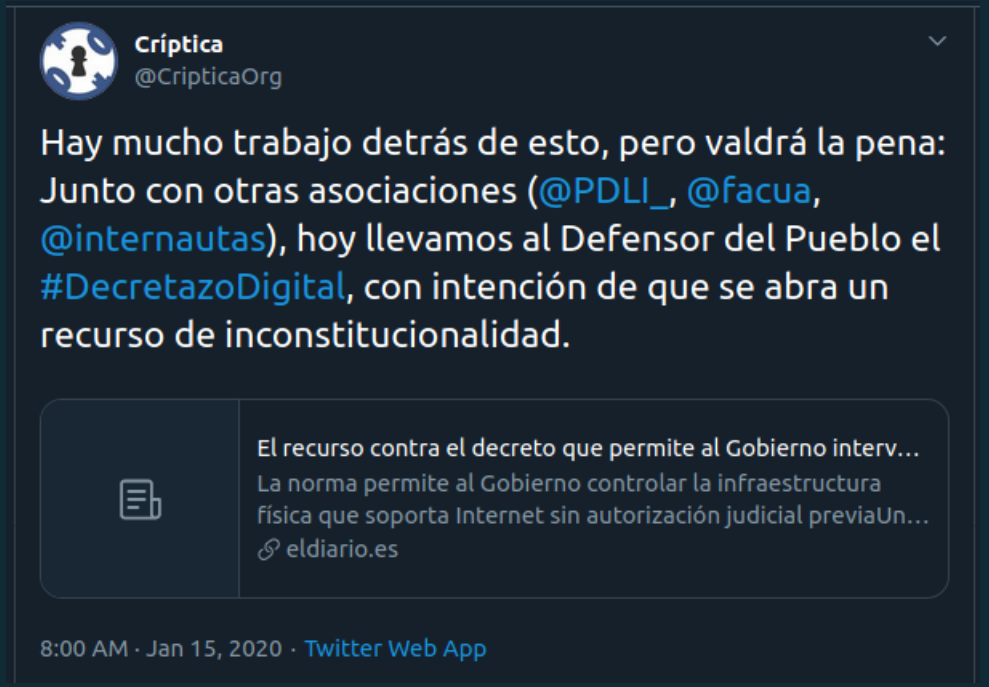
Acerca de Críptica

- Asociación cultural fundada en 2015
- Sin ánimo de lucro
- Eventos, materiales y formaciones de privacidad
- El año pasado publicamos el libro *Resistencia Digital: Manual de seguridad operacional e instrumental para smartphones*



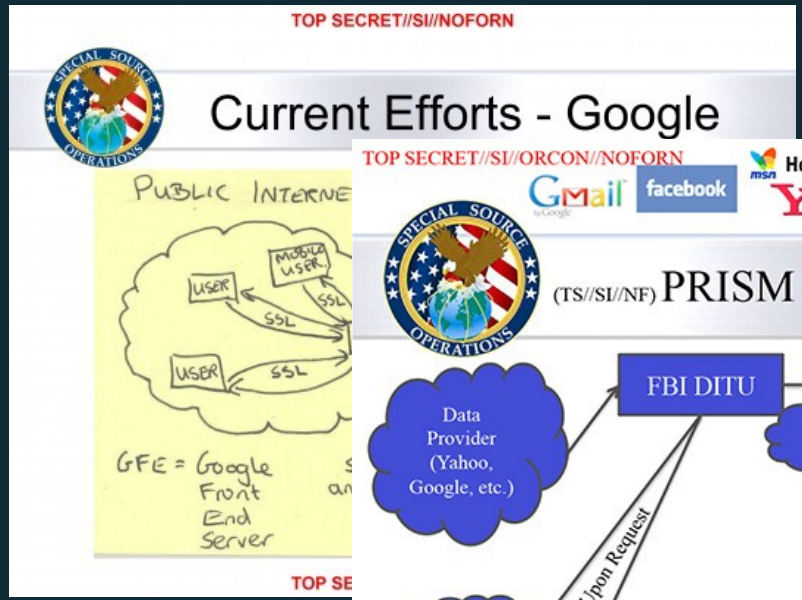
Actividad

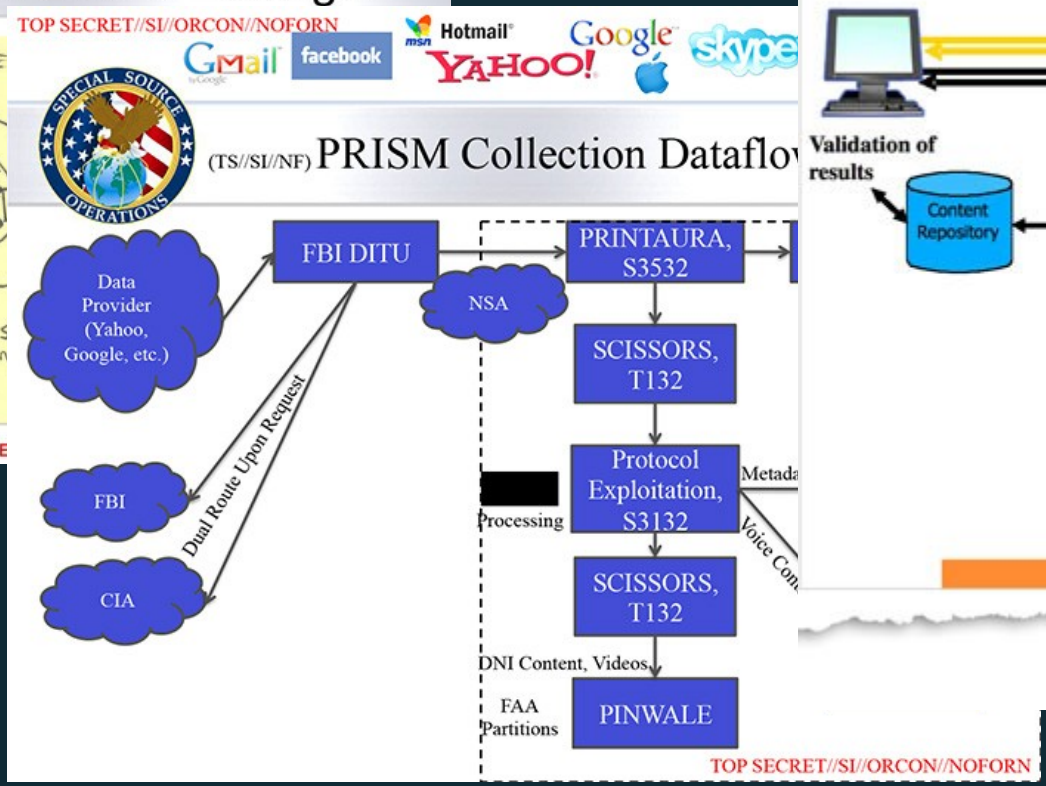

Resistències digitals 2
TROBADES TECNOPOLÍTIQUES OBERTES PER DEBATRE LA NOSTRA RELACIÓ AMB LA TECNOLOGIA
IPHONE I ANDROID: HI HA ALTERNATIVES?
16/01
18.30h
Lleialtat Santsenca
(c/Olzinelles 31, Barcelona)
Críptica
CripticaOrg
criptica.org

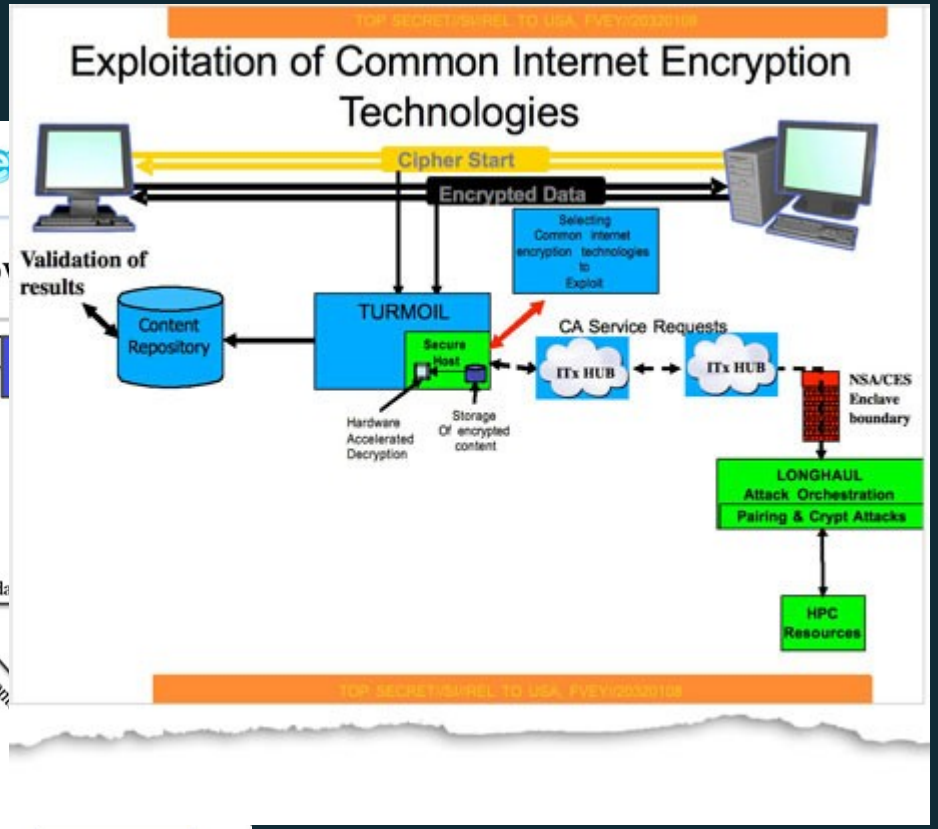

Críptica
@CripticaOrg
Hay mucho trabajo detrás de esto, pero valdrá la pena: Junto con otras asociaciones (@PDLI_, @facua, @internautas), hoy llevamos al Defensor del Pueblo el #DecretazoDigital, con intención de que se abra un recurso de inconstitucionalidad.
El recurso contra el decreto que permite al Gobierno interv…
La norma permite al Gobierno controlar la infraestructura física que soporta Internet sin autorización judicial previaUn…
eldiario.es
8:00 AM · Jan 15, 2020 · Twitter Web App

¿Por qué?

2013-2015: Revelaciones de Edward Snowden







Yo no soy nadie. No tengo nada que esconder.

Tras la frase...

- Idea errónea: Sólo los “malos” tienen cosas a esconder y yo no soy malo.
- ¿Malo para quién? Para quien ostenta poder, cualquier persona que le desafía gana la etiqueta de “malo”: Activista, disidente político, periodista de investigación…
- No sabes cómo te afectará mañana la información que generas hoy
- Derecho a la intimidad

Intimidad

- Tenemos derecho a una vida privada
- ¿Por qué cierras el pestillo del baño?
- ¿Vivirías en una casa de cristal?
- ¿Me dejarías conocer todos tus problemas personales, familiares o amorosos?
- ¿Por qué no me dejas leer tus mensajes, analizarlos y compartirlos con quien yo quiera?
- ¿Puedo acceder a tu historial de navegación y publicar lo que quiera?
- ¿Puedo seguirte por la calle todo el día?
- **¿Acaso tienes algo que esconder?**

Privacidad como garante de otros derechos

- La vigilancia condiciona nuestras libertades:
  - Comportamiento
  - Reunión
  - Asociación
  - Expresión
  - Pensamiento
- En definitiva: La privacidad es fundamental para una sociedad democrática

¿Está todo perdido?

Hay esperanza

Open Source Privacy Tools NSA Can't Crack: OTR, PGP, RedPhone, Tor And Tails

By Lucian Armasu December 30, 2014

US & WORLD

New documents reveal which encryption tools the NSA couldn't crack

By Russell Brandom | Dec 28, 2014, 6:23pm EST

Source Chaos Computer Club Conference 2014 and Der Spiegel

Defensa: Manos a la obra

Filosofía

- Modelado adversarial
- Seguridad operacional
- Privacidad por diseño
- Código abierto
- Descentralización
- Usabilidad

Tu información al alcance de todos: Datos en abierto

OSINT

- Conjunto de técnicas y herramientas para recopilar información pública, correlacionar los datos y procesarlos
- Puede ser usada por cualquiera con el tiempo, conocimiento y motivación necesarios.
- Ejemplo 1: Descubrir empleados, servidores, dominios, correos, contraseñas filtradas, servicios utilizados de una organización a la que se quiere atacar.
- Ejemplo 2: Descubrir los integrantes, patrones, relaciones, localización y perfilado de los integrantes de una organización o movimiento.

Ejemplo: Análisis de Twitter

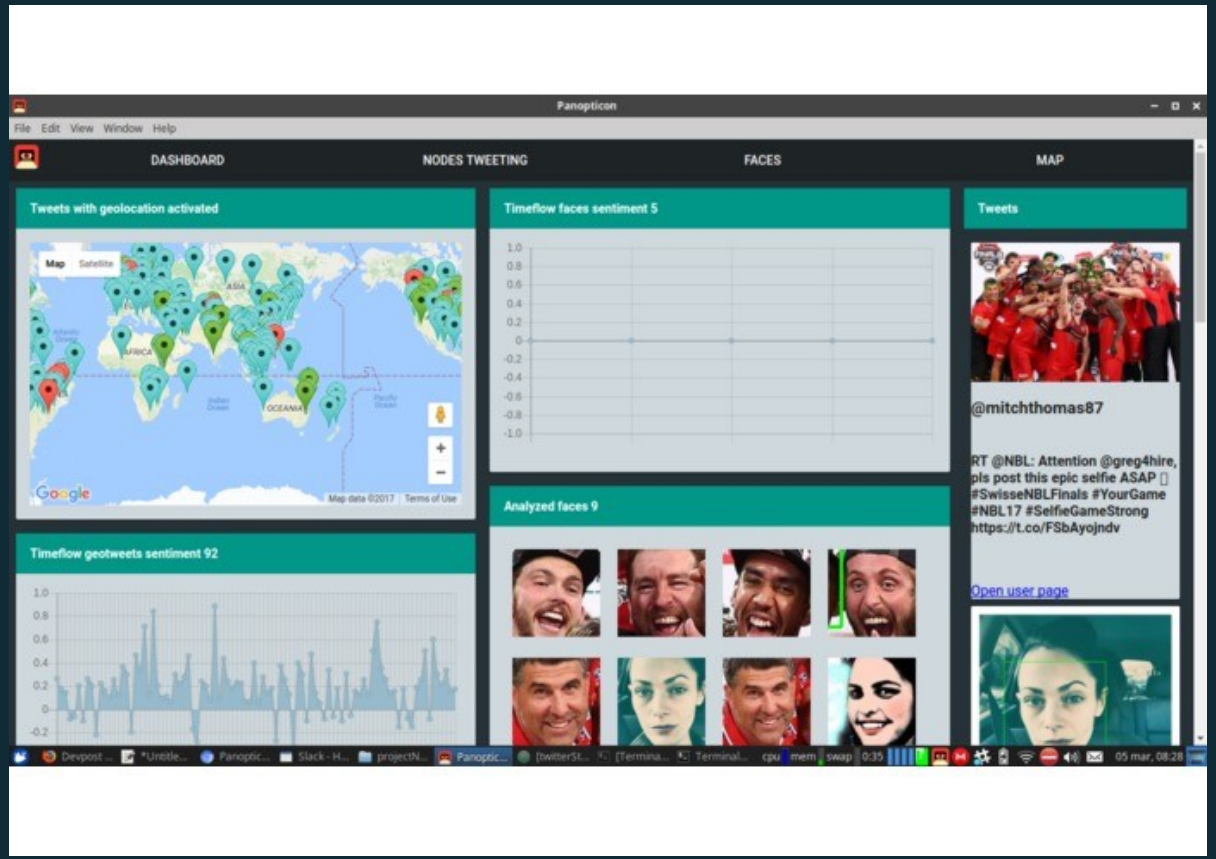
Datos accesibles, almacenables y analizables por cualquiera:

- Contenido de los tuits
- Contenido de la bio
- Fecha y hora de publicación de los tuits
- Hashtags en los que participas
- Multimedia que publicas: ¿Salen caras? ¿Tienen etiquetas?
- A quién sigues y quién te sigue
- Nivel de interacción con otras cuentas: RT, likes, replies
- Geolocalización (si está activada)

Ejemplo: Análisis de Twitter

Ejemplo: Análisis de Twitter

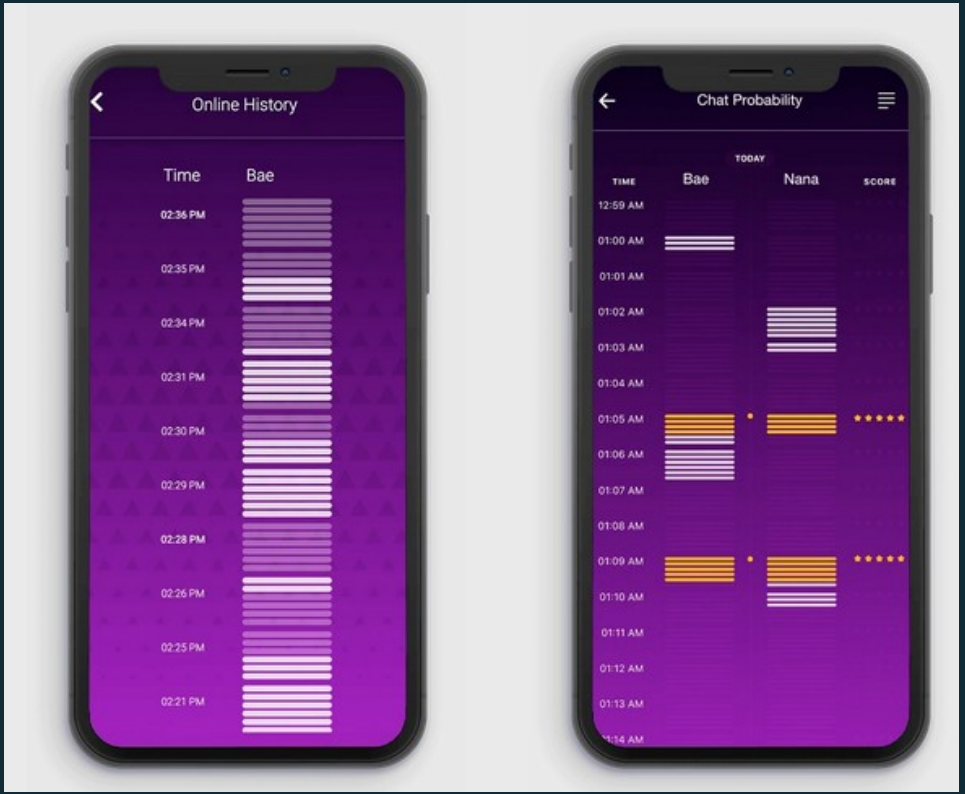
Ejemplo: Análisis de Twitter



Ejemplo: Chat Watch

“Who where you chatting with at 3am?!”

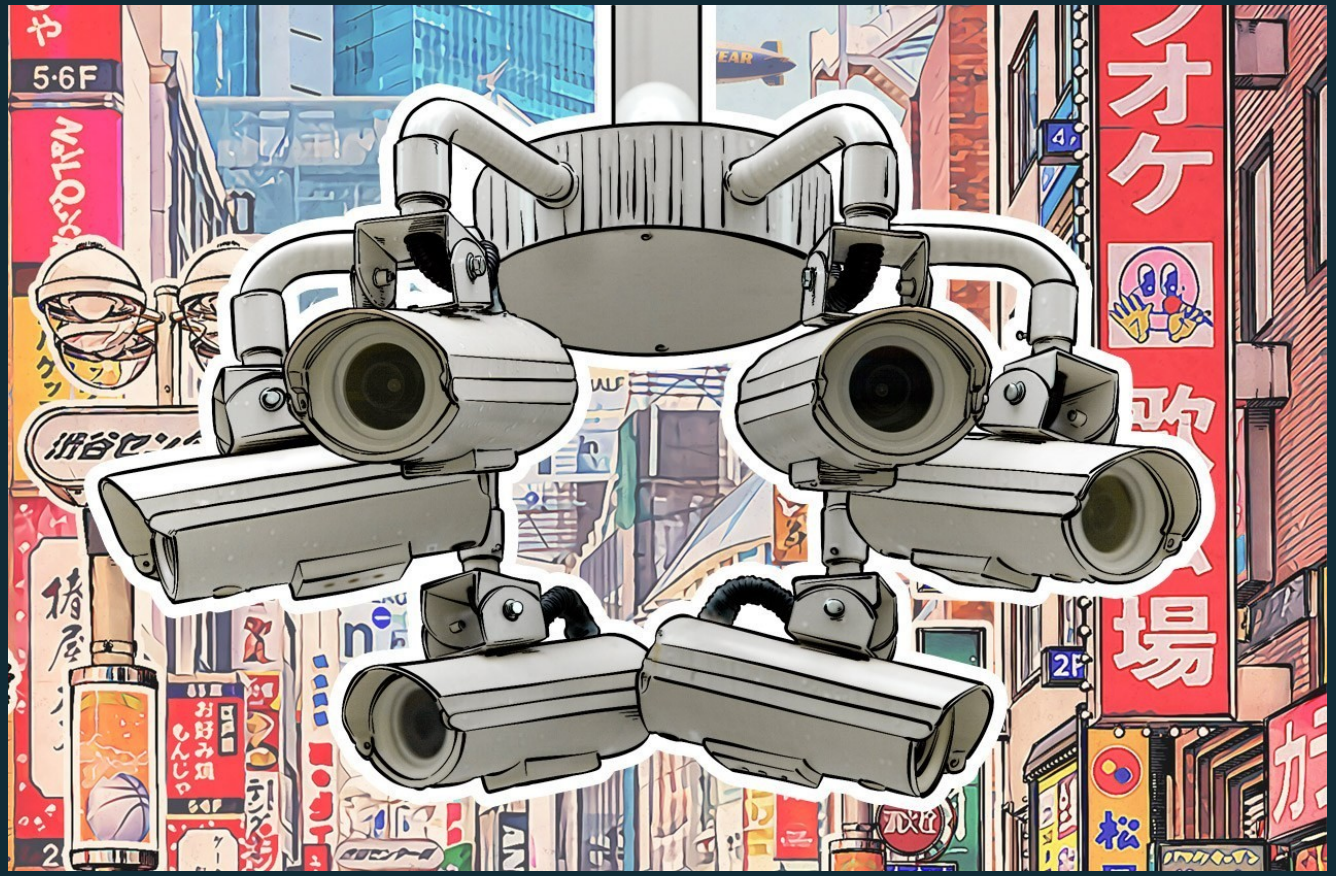
Chatwatch is here to answer that age old question.



Brechas de seguridad

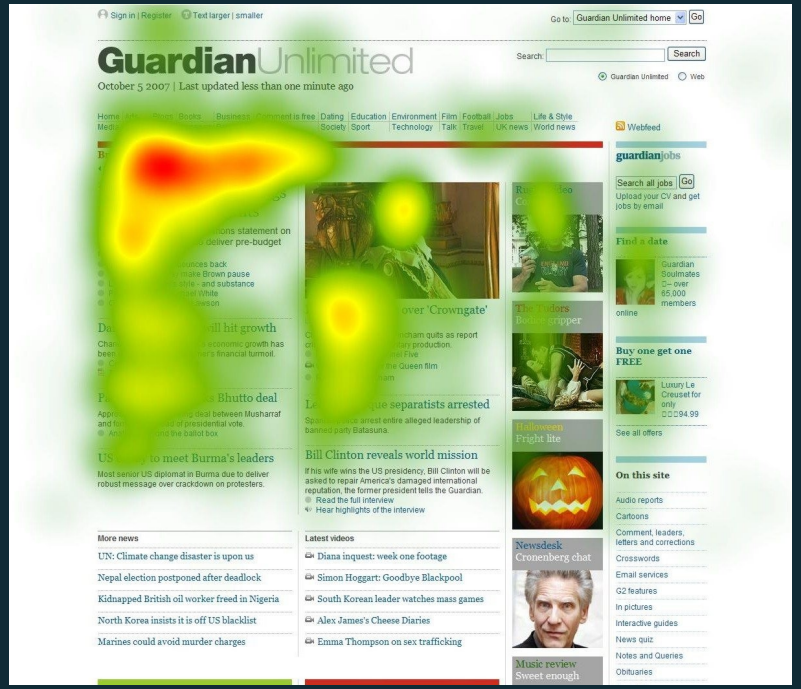
Hay información que proporcionamos a servicios y que no esperamos que sea pública, pero a veces esta información se filtra por culpa de una brecha de seguridad.

Tu información al alcance de unos pocos: Datos que cedemos a servicios



Web tracking

- Dirección IP
- Navegador
- Sistema operativo
- Idioma del navegador
- Cookies: Correlación con actividad previa o futura
- Monitorización de la actividad en el sitio web
- Información que hayamos introducido explícitamente
- Google Analytics, Facebook, Twitter, plataformas de publicidad



Redes sociales

Lo mismo que el web tracking añadiendo:

- Grafos sociales (A quién conoces y quién te conoce)
- Interacciones sociales (Con quién te llevas y con quién no)
- Intereses políticos, artísticos, personales, sociales…
- Eventos y lugares a los que asistes
- Correlación de estos datos con muchos otros:
  - Análisis biométrico de las imágenes
  - Datos obtenidos de tu smartphone: Contactos, red wifi, localización...

Correo electrónico

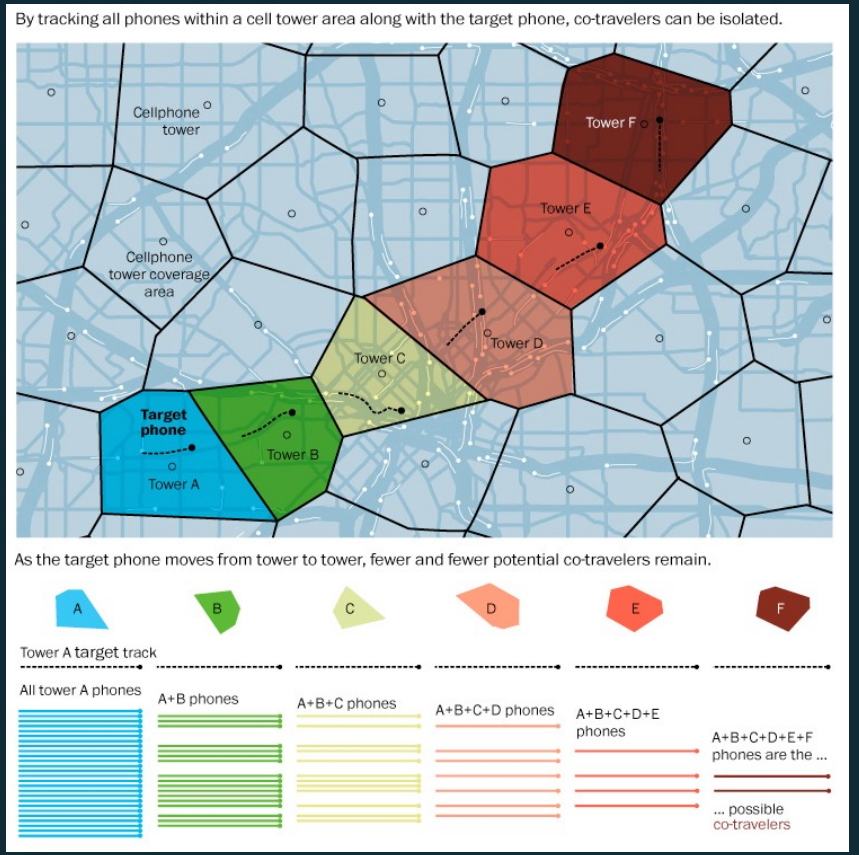
¿Por qué nos parece inconcebible que alguien abra y analice nuestro correo postal pero nos parece normal en el caso del correo electrónico?

Telefonía móvil

Un operador puede acceder a:

- Localización aproximada (antena de telefonía)
- SMS enviados y recibidos: metadatos y contenido
- Llamadas enviadas y recibidas: metadatos y su contenido
- Direcciones IP visitadas y con qué protocolo
- Contenido de los paquetes, si no van cifrados
- Dominios resueltos vía DNS

Ejemplo de visualización de estos datos: https://www.zeit.de/datenschutz/malte-spitz-data-retention



Cuestiones

- ¿Estos datos podrían ser usados contra las personas que los generan?
- ¿Por que permitimos que se nos perfile y monitorice de esta forma como sociedad?
- ¿Y como individuos?

Por qué la privacidad debe protegerse por diseño

Function Creep

- “Desviación de uso” o “Desvirtuación de funciones”
- *La ampliación gradual del uso de una tecnología o sistema más allá del propósito para el que fue originalmente diseñado, especialmente cuando esto conduce a una posible invasión de la privacidad*
- Ejemplos:
  - Servicios de correo, videollamadas y redes sociales convertidos en aparatos de vigilancia masiva por parte de la NSA.
  - Datos de telefonía movil usados para controlar los movimientos de la ciudadanía.

Privacidad por diseño: Qué es

1) *Proactive not Reactive; Preventative not Remedial*
2) *Privacy as the Default Setting*
3) *Privacy Embedded into Design*
4) *Full Functionality — Positive-Sum, not Zero-Sum*
5) *End-to-End Security — Full Lifecycle Protection*
6) *Visibility and Transparency — Keep it Open*
7) *Respect for User Privacy — Keep it User-Centric*

https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

Conceptos interesantes

- Minimización de datos: Usar el mínimo de información de usuario para ofrecer la funcionalidad deseada.
- Cifrado extremo a extremo: El contenido de los mensajes sólo es accesible por los interlocutores, no por el proveedor
- Descentralización / P2P: No existe un único proveedor con todos los datos o puedes ser tu proveedor.
- Código abierto: Transparencia de qué hace y qué no hace una aplicación o programa

Una nota sobre Biometría

- A la hora de identificarte se pueden usar tres factores:
  - Algo que sabes (Contraseña)
  - Algo que tienes (tarjeta de crédito, token, smartphone)
  - Algo que eres (biometría)
- El uso de biometría tiene un alto impacto sobre la privacidad ya que:
  - Puede ser usado para identificarte en contra de tu voluntad. Esto no sucede con la contraseña, por ejemplo.
  - Es irrevocable. Puedes cambiar fácilmente de contraseña o de tarjeta, pero no de cara, iris o huella dactilar.

Privacidad en la era post-COVID-19

Vigilancia y COVID-19

El 'terrorífico' perro-robot que utiliza Singapur para mantener la distancia social

El país asiático usa a Spot, un perro-robot que pasea por el parque Bishan-Ang Mo Kio y le recuerda a la gente que debe mantenerse separada por su propia seguridad

El perro que ayuda a mantener la distancia social en Singapur. EFE

China

China is using practically every surveillance system in its toolbox: Authorities are tapping publicly located cameras to run facial recognition searches, citizens are being location-tracked through their phones, and drones are being put to use in order to give directions from the government, according to CNBC.

https://www.elconfidencial.com/mundo/2020-05-09/peculiar-manera-distancia-social-singapur-perro_2587440/
https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9

Vigilancia y COVID-19

Israel

The Israeli government is using data from telecom providers to track the locations of millions of citizens in an attempt to find people diagnosed with the coronavirus and alert those with whom the infected person might have interacted. Those breaking quarantine are threatened with up to six months of imprisonment.

Palestinians checking the status of their permits to stay in Israel must now download an app that tracks their location, since the offices typically visited for this kind of paperwork is closed.

Hong Kong

Those quarantined in Hong Kong must wear electronic wristbands that track their locations. Wristbands are handed out at the airport and must be paired with the individual's smartphone.

https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9

Vigilancia y COVID-19

South Korea

Confirmed cases of the coronavirus are being tracked in South Korea by a fusion of credit card purchases, smartphone location tracking, and CCTV footage, presumably analyzed by facial recognition algorithms, according to Reuters.

This allows the Korean government to reconstruct the past actions of those diagnosed with the virus with incredible granularity, like using the person's location data to check nearby CCTV footage and see if they were wearing a mask, Reuters reports.

India is forcing people to use its covid app, unlike any other democracy

Millions of Indians have no choice but to download the country's tracking technology if they want to keep their jobs or avoid reprisals.

https://onezero.medium.com/the-pandemic-is-a-trojan-horse-for-surveillance-programs-around-the-world-887fa6f12ec9
https://www.technologyreview.com/2020/05/07/1001360/india-aarogya-setu-covid-app-mandatory/

Privacidad en la era post-COVID19

- Solución tecnológica a problemas de la pandemia: Aplicaciones de *contact tracing*
- *Efectividad:*
  - *¿Qué pasa con la gente que no tiene smartphone*?
  - ¿Qué pasa si no se la descarga suficiente gente?
  - ¿Existen alternativas igual o más eficientes?
- Impacto:
  - ¿Cómo afectará la normalización de la vigilancia gubernamental de los contactos del día a día a la sociedad del mañana?

Aplicaciones de *contact tracing:* Propuestas

- Sistemas centralizados usando GPS (con o sin bluetooth, con o sin datos personales):
  - Las apps envían la geolocalización a un servidor central en todo momento
  - El estado sabe dónde, cuándo y con quién ha estado cada persona.
  - Si alguien da positivo, se identifica con quién ha estado en contacto.
  - Corea del Sur, Singapur

Aplicaciones de *contact tracing:* Propuestas

- Sistemas “anónimos” usando bluetooth + gestión **centralizada** *(ROBERT)*:
  - No usan datos personales
  - Las apps anuncian pseudónimos aleatorios vía bluetooth. Los pseudónimos cambian cada pocos minutos
  - La app guarda una lista de pseudónimos anunciados y otra de los escuchados. Los pseudónimos escuchados se suben al servidor central
  - Cuando alguien da positivo en COVID-19, sube la lista de pseudónimos anunciados. El servidor cruza los datos y alerta a los usuarios que han escuchado esos pseudónimos.
  - Sistema pseudónimo, el servidor sabe que IDs han estado cerca de otros y cuando. Podrían cruzarse estos datos con otros para desanonimizar a personas

Aplicaciones de *contact tracing:* Propuestas

- Sistemas “anónimos” usando bluetooth + gestión **descentralizada** (DP3T):
  - No usan datos personales
  - Las apps anuncian pseudónimos aleatorios vía bluetooth. Los pseudónimos cambian cada pocos minutos
  - La app guarda una lista de pseudónimos anunciados y otra de los escuchados. **No se envían datos al servidor central por defecto**
  - Cuando alguien da positivo en COVID-19, sube la lista de pseudónimos anunciados. Las apps descargan esta lista y alertan a su usuario si ha entrado en contacto con alguno.
  - El servidor no tiene información de los contactos pero la lista de pseudónimos que se suben al servidor es pública
  - Vulnerable a ataques de usuarios / entidades malintencionadas: Si se registra la hora y lugar de los pseudónimos que se van escuchando se puede cruzar esta información con la lista del servidor.

Aplicaciones de *contact tracing:* Preguntas

- ¿Preferimos un sistema centralizado que revela grafos sociales que se pueden cruzar para desanonimizar a personas o grupos?
- ¿Preferimos un sistema descentralizado que permite a usuarios malintencionados obtener información de dónde y cuándo han estado algunas personas con COVID-19?
- ¿Merece la pena el impacto si el sistema no funciona?¿Y si funciona?
- Disclaimer: Este fin de semana se ha publicado DESIRE, otro protocolo de contact tracing que asegura resolver estos problemas.

Conclusiones y preguntas

- Con la crisis del COVID-19 somos conscientes de los riesgos de salud que hemos asumido al ignorar las señales de alarma anteriores.
- ¿Somos conscientes de los riesgos que implican los sistemas invasivos con la privacidad que usamos hoy en día?
- ¿Qué podemos hacer como ingenieros e ingenieras?

¡Gracias por vuestra atención!

Contacta con Críptica

- Web: https://criptica.org
- Twitter: @CripticaOrg
- Canal de Telegram : t.me/cripticaorg
- Matrix: #criptica:matrix.org
- Mail: info [at] criptica.org