Comunicaciones Seguras

Internet: Vigilancia masiva, privacidad y anonimato

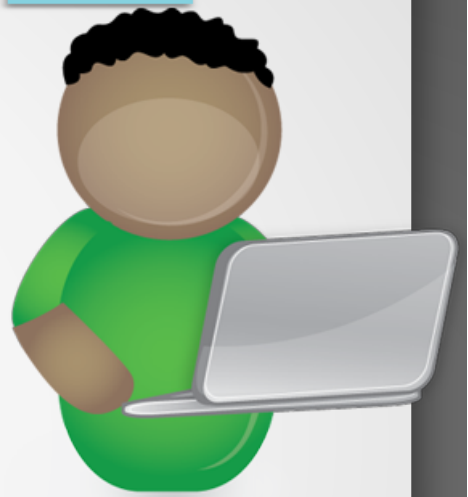
Rafael Bonifaz: rafael@bonifaz.ec

¿Si tu vecino te espía por la ventana?

- ¿Te molestarías?
- ¿Sentirías tu intimidad invadida?
- ¿Qué tanto puede saber de ti al mirar por la ventana?
- ¿Estarías de acuerdo en dejarte espiar por tu vecino por seguridad?
- ¿A ser grabado?

¿Si tu vecino espía tu computadora?

- ¿Qué tanto podría saber tu vecino al revisar tu computadora o celular?
- Correos, chats, redes sociales, contraseñas, cámara web, micrófono, historiales de búsqueda, fotos, videos, etc.
- ¿Quién sabe más el que espía por la ventana o el que espía por Internet?
- ¿Si las corporaciones o tu ISP te vigila?
- ¿Si tu gobierno te vigila?



¿Qué es la nube?

¿Dónde se guarda la información?

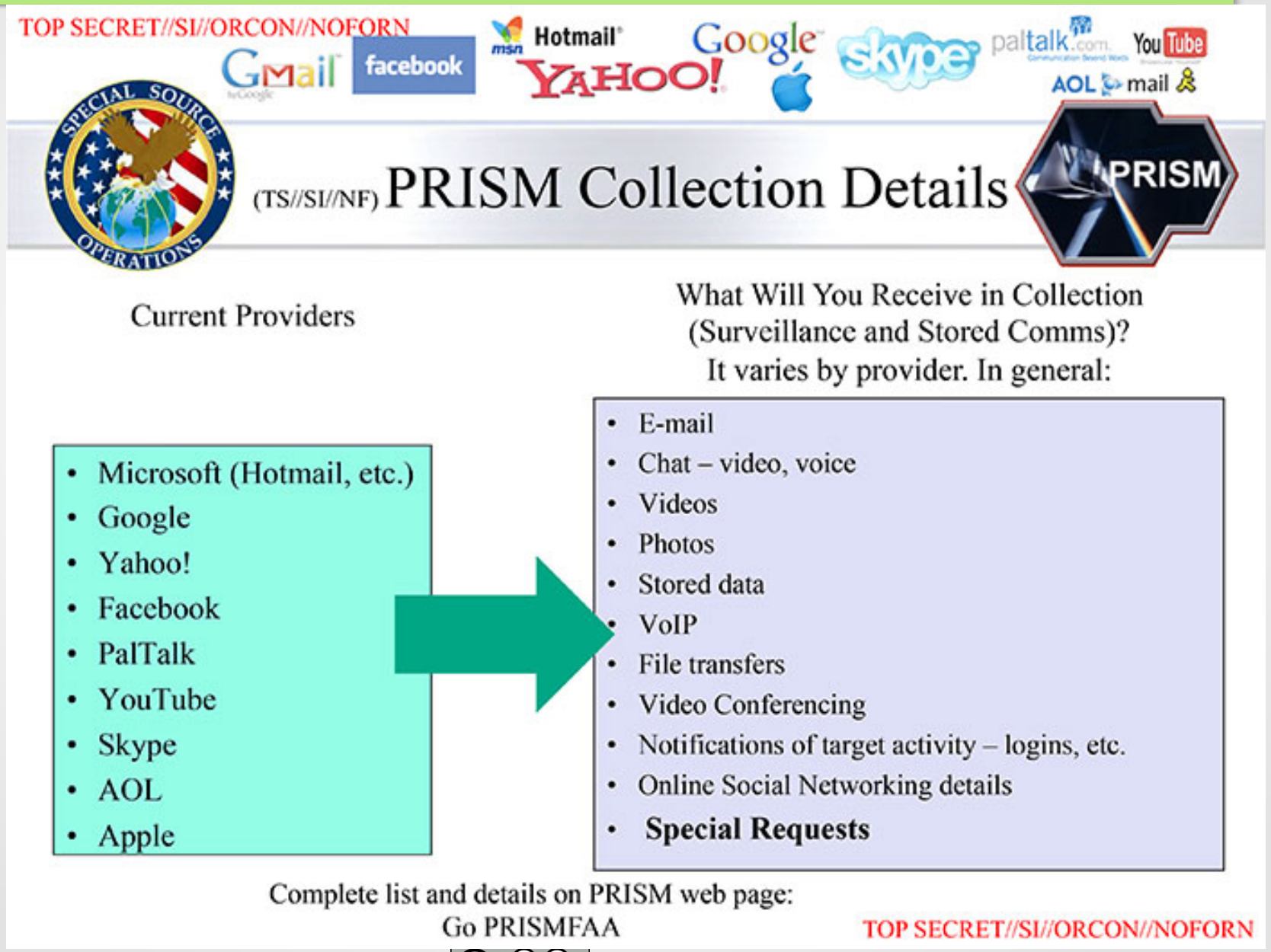
Existe la computadora de otra persona

Imagen tomada de revista Wire online:
http://www.wired.com/politics/security/news/2007/10/domestic_taps

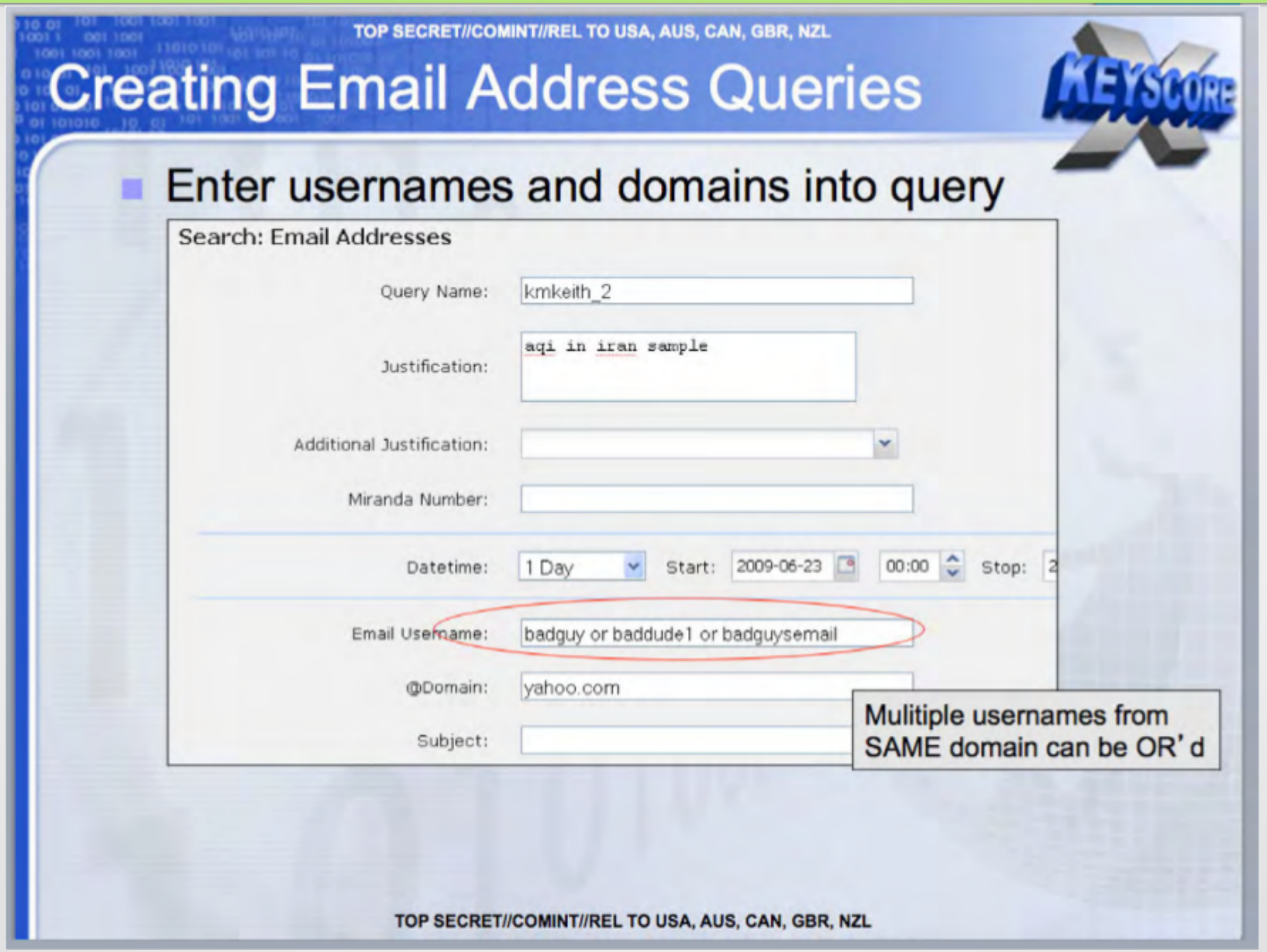
Snowden, Wikileaks y la Vigilancia Masiva

- A finales de 2011 Wikileaks publica los Spyfiles
  - Empresas que venden a gobiernos software de espionaje masivo
  - Más publicaciones en 2013 y 2014
- Revelaciones de Snowden
  - Internet máquina de vigilancia masiva
  - Alianza de los 5 ojos: EEUU, Reino Unido, Canadá, Australia y Nueva Zelanda
  - Grandes empresas de Internet espían a sus usuarios
- ¿América Latina?
  - Gamma Group
  - Hackingteam

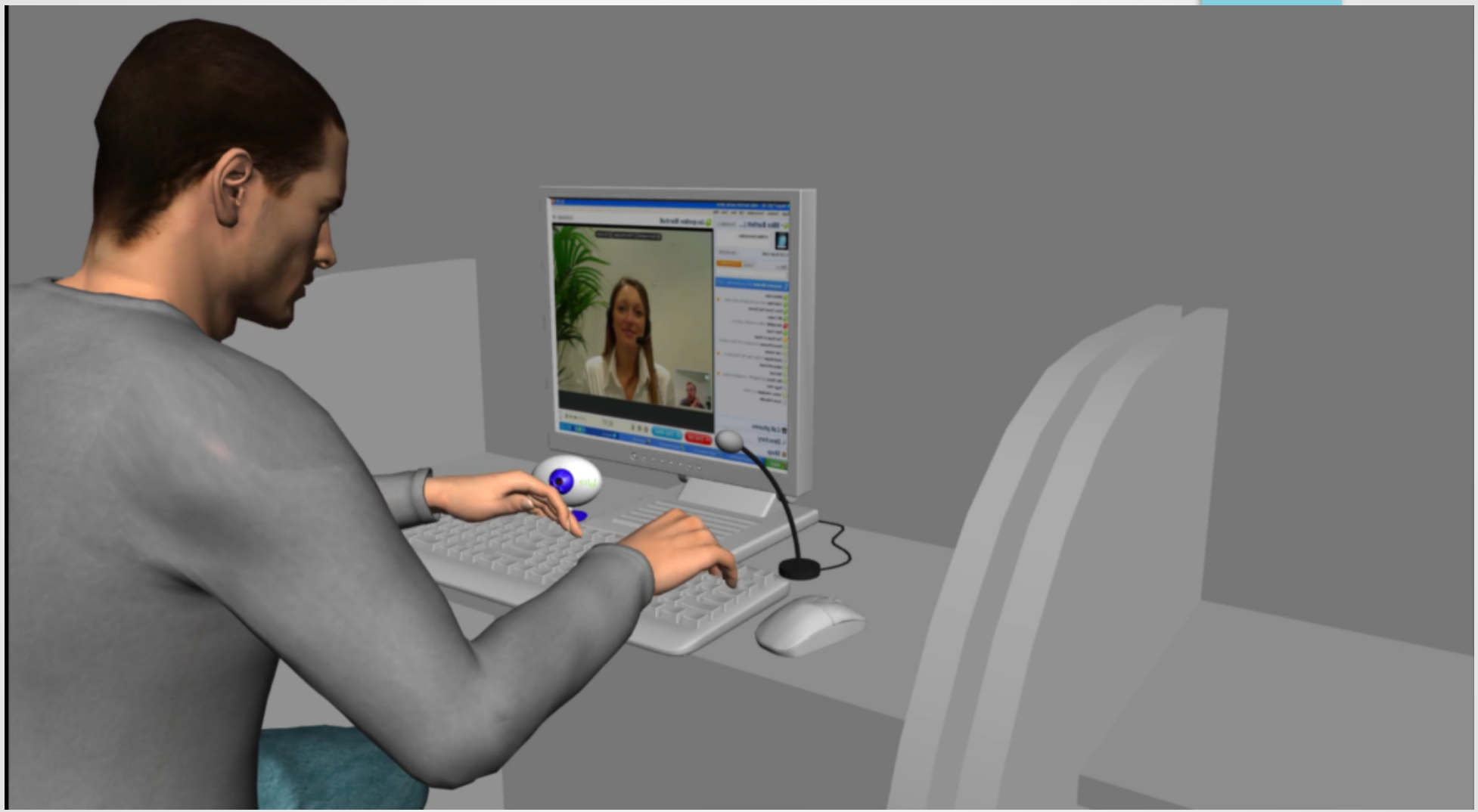
Programa PRISM



Programa X-KEYSCORE



Los EEUU no son los únicos que espían

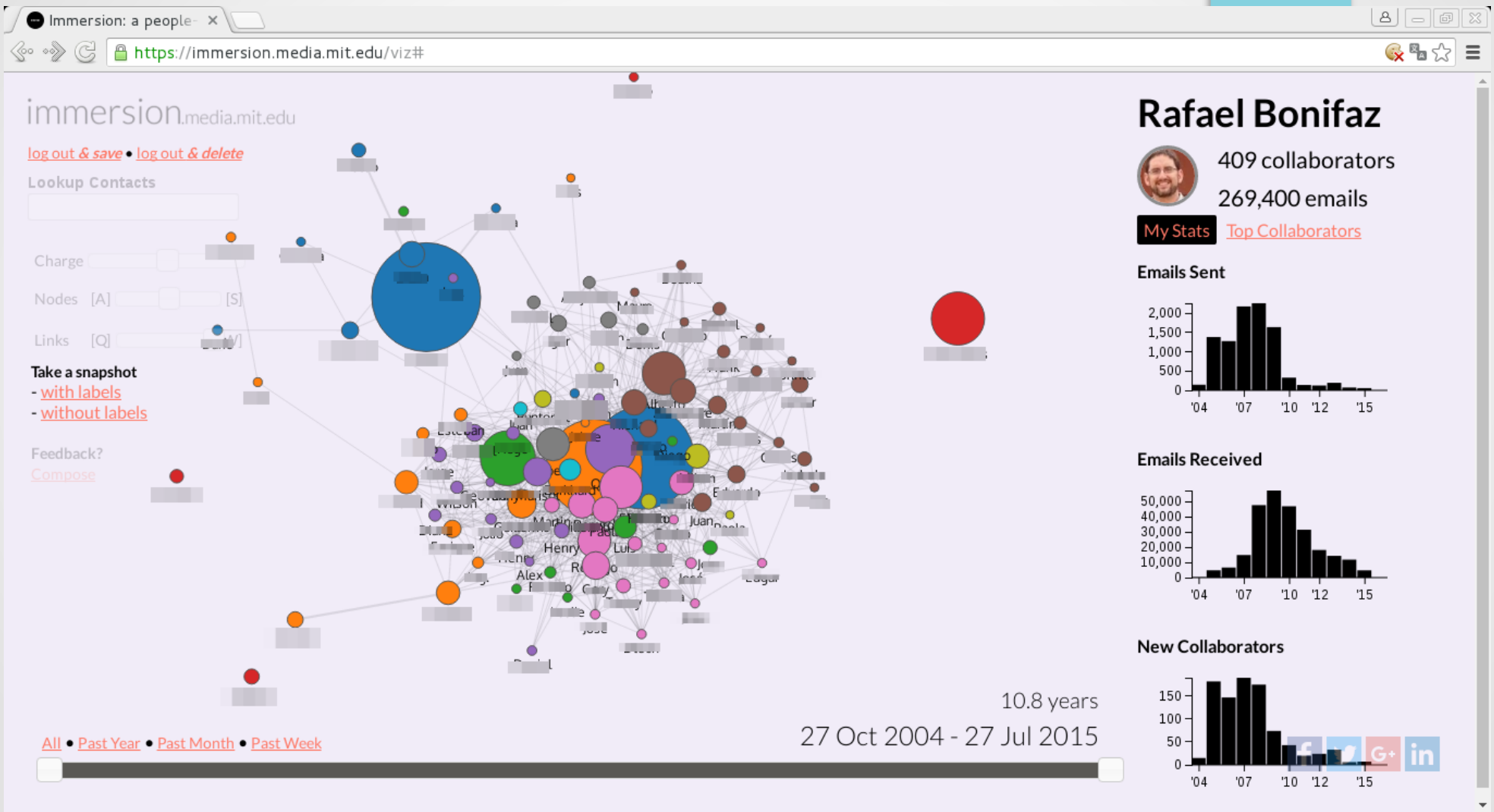


https://wikileaks.org/spyfiles/docs/gamma/301_remote-monitoring-and-infection-solutions-finspy.html

Metadatos

- Son datos de los datos
- Dicen mucho de una persona
- Ubicación desde donde se realiza la comunicación
- Con quién se comunica
  - Con qué frecuencias
  - Con quién cifra y con quién
  - Red de contactos

Metadatos



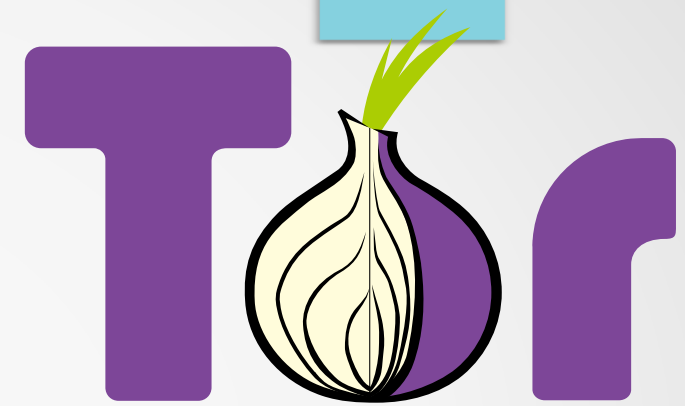
https://immersion.media.mit.edu/

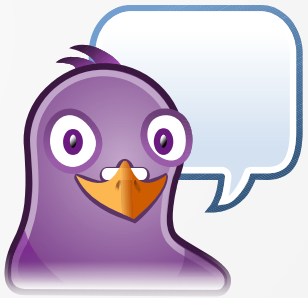
¿Qué hacer?

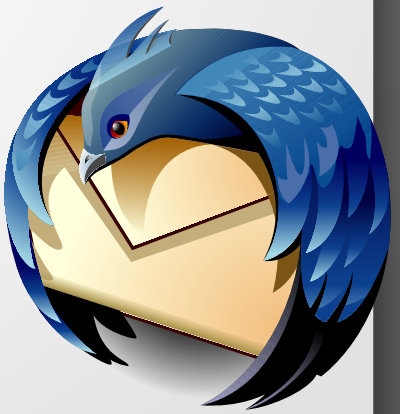
- **Usar software libre:**
  - El software libre permite auditar su funcionamiento
  - Es accesible para todos ya que no pone barreras artificiales
- **Cifrar las comunicaciones fin a fin:**
  - Permite que solo las partes interesadas puedan leer las comunicaciones
  - El software para cifrar debe ser libre para ser confiable
- **Internet descentralizado:**
  - Evitar usar servicios hipercentralizados
  - En lo posible usar infraestructura propia
  - Si es posible redes p2p

¿Qué vamos a aprender?

- Navegar Internet de forma anónima
- Gestionar contraseñas seguras
- Chat cifrado
- Llamada y video llamada cifrada
- Correo electrónico cifrado
- Tails, el sistema operativo pensado en privacidad y anonimato







Algunas reflexiones

- No existe una sola solución
- Nada es 100% seguro
- Hay que tener visión crítica de la tecnología. ¿Por qué usamos lo que usamos?
- Estar abiertos al cambio
- Cuestionarnos todo
- El Internet debe servir para liberar no para controlar
- ¡Sumar a más gente! La criptografía vale cuando todos la usamos

Un pensamiento

"*Si quieres construir un barco, no empieces por buscar madera, cortar tablas o distribuir el trabajo, sino que primero has de evocar en los hombres el anhelo de mar libre y ancho.*"

Antoine de Saint-Exupéry

Referencias

- “Sin un Lugar Donde Esconderse” de Glen Greenwald (2014)
  - http://glenngreenwald.net/#BookDocuments
- “Cryptopunks”, Julian Assange, Jacob Appelbaum, Jérémie Zimmerman y Andy Muller-Maguhn (2012)
  - http://assange.rt.com/es/episodio-8--assange-y-los-criptopunks/
  - http://assange.rt.com/es/episodio-9--assange-y-los-criptopunks/
- Documental “Citizenfour” de Laura Poitras (2014)
- Filtraciones de Snowden:
  - https://search.edwardsnowden.com/
- “1984” de George Orwell (1949)
- Los Spyfiles de Wikileaks
  - https://wikileaks.org/spyfiles
- “Cuando Google Conoció Wikileaks”, Julian Assange 2014
- Libros de Cory Doctorow (Marcus Yallow)
  - Pequeño Hermano, Homeland