

# Stand up for your rights (through your ISP?)

Monica A. Senior  
Carlo Blengino

Nessun despota dell'antichità,  
nessun monarca assoluto dell'età  
moderna, pur circondato da mille  
spie, è mai riuscito ad avere sui  
suoi sudditi tutte quelle  
informazioni che il più democratico  
dei governi può attingere dall'uso  
dei cervelli elettronici”

# Di cosa parleremo?

- Delle richieste di accesso ai dati degli utenti da parte delle law enforcement ai grandi provider americani
- Di come i provider rispondono
- Dei problemi di diritto transnazionale
- Delle iniziative di contrasto a protezione degli utenti assunte dai provider stessi
- Del ruolo che i provider possono e potranno giocare nell'ecosistema della tutela dei nostri dati

TOP SECRET//SI//NOFORN

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

---

IN RE APPLICATION OF THE  
FEDERAL BUREAU OF INVESTIGATION  
FOR AN ORDER REQUIRING THE  
PRODUCTION OF TANGIBLE THINGS  
FROM VERIZON BUSINESS NETWORK SERVICES,  
INC. ON BEHALF OF MCI COMMUNICATION  
SERVICES, INC. D/B/A VERIZON  
BUSINESS SERVICES.

---

Docket Number: BR

13 - 8 0




<http://www.aclu.org/blog/national-security/nsa-surveillance-order-explained-aclu>

## Introducing the program

A slide briefing analysts at the National Security Agency about the program touts its effectiveness and features the logos of the companies involved.

The seal of Special Source Operations, the NSA term for alliances with trusted U.S. companies.

TOP SECRET//SI//ORCON//NOFORN



# PRISM/US-984XN Overview

OR

## *The SIGAD Used Most in NSA Reporting* Overview

April 2013

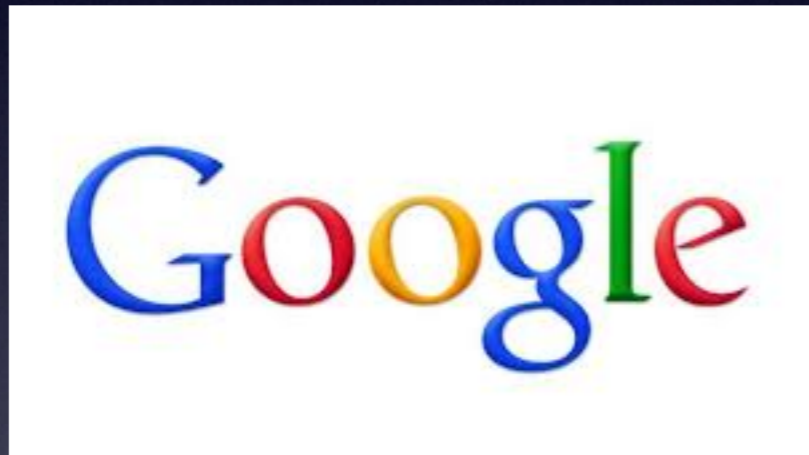
Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20360901

TOP SECRET//SI//ORCON//NOFORN

The program is called PRISM, after the prisms used to split light, which is used to carry information on fiber-optic cables.

This note indicates that the program is the number one source of raw intelligence used for NSA analytic reports.

# Trasparency reports



# Tipologia delle richieste di accesso ai dati

- **Non-content data**: includono nome utente, indirizzo, telefono, IP di registrazione dell'account, durata e tipi di servizi utilizzati, dati carta di credito, meta-dati di traffico telefonico
- **Content data**: includono file, e-mail, immagini, calendari

# Google

2012	Requests	Pertcentage info produced	Users/ account specified
Total	42.327	66%	68.249
Italy	1.687	34%	2.105



# Twitter

2° sem. 2012	Requests	Percentage info produced	Users/ account specified
Total	1.009	57%	1.433
Italy	< 10	0%	< 10

# Microsoft

2012	Requests	No data found	Non-content data	Content data	Rejected
Total	70.665	11.852 (16,8%)	56.388 (79,8%)	1.558 (2,2%)	866 (1,2%)
Italy	1.519	258 (17%)	1.261 (83%)	0	0

# Skype

2012	Requests	Accounts/ identifiers	Content data
Total	4.713	15.409	0
Italy	96	648	0

# Come acquisisco dati personali e contenuti in Italia?

- Per ottenere dati anagrafici degli utenti o meta-dati di connessione da un ISP occorre un ordine di esibizione emesso con decreto da un P.M.
- Per i dati di contenuto occorre un'ordinanza del G.I.P. solo se si tratta di intercettazioni (quindi in tempo reale) sia telefoniche che telematiche
- I dati di contenuto storici (ad es. testo di una e-mail), in genere, si ottengono con l'analisi forense che viene effettuata a seguito del sequestro del device

# Come acquisisco i dati negli U.S.A.?

- subpoena
- court order
- search warrant
- NSLs (National Security Letters)

# subpoena (*duces tecum*)

È una citazione a giudizio, materialmente redatta da un avvocato (della Procura o della difesa), ma formalmente emessa dal tribunale

Può avere ad oggetto una testimonianza o l'esibizione di documenti (*duces tecum*), anche informatici

Può essere opposta con un'azione di annullamento ([motion to quash](#))



# court order

È un'ingiunzione emessa da un tribunale a fronte di "articulable facts showing that there are reasonable grounds to believe that ... information sought are relevant and material to an ongoing criminal investigation"

18 USC § 2703

APPLICATION AND EX PARTE ORDER TO DISCLOSE TELEPHONE OR INTERNET RECORDS		STATE OF CONNECTICUT SUPERIOR COURT		AGENCY NAME
JD-CR-142 Rev. 7-07		wwwjud.ctgov		New Canaan Police Department
C.G.S. § 54-47aa, P.A. 07-4 Sec. 98		See section 117 for Request to Delay Notification of Ex Parte Order.		AGENCY CASE NO. 11-717
NAME AND ADDRESS OF CORPORATION Business Insider, 119 Fifth Avenue, 7th Floor, New York, NY 10003				
1. APPLICATION FOR EX PARTE ORDER TO COMPEL DISCLOSURE OF TELEPHONE OR INTERNET RECORDS				
TO: A Judge of the Superior Court				
The undersigned hereby applies for an order compelling the above named corporation to disclose the below described telephone or internet records. The articulated reasonable suspicion that a crime has been or is being committed, or that exigent circumstances exist is indicated below:				
AGENCY	NAME OF AGENCY	TELEPHONE NO.	FAX NO.	
	New Canaan Police Department	203-594-3523	203-594-3551	
	ADDRESS OF AGENCY	174 South Avenue New Canaan, CT 06840		
DATE	SIGNED (Law enforcement officer)	TYPE/PRINT NAME OF LAW ENFORCEMENT OFFICER		
1/21/2011	<i>Sgt. Carol Ogrinc</i>	Sergeant Carol Ogrinc		
REASONABLE AND ARTICULABLE SUSPICION OR EXIGENT CIRCUMSTANCES				
The undersigned officer, being duly sworn, deposes and says:				
On 1/17/11 I received a call from _____ who stated the harassment has continued off and on regarding the complaint he and his daughter _____ made in June 2010.				
Mr. _____ stated there have been numerous negative postings on different websites about he and his family since Ms. Buhl was arrested on 10/27/10. Many of the postings were made in November and December and Mr. _____ believes Teri Buhl has been responsible for posting many of them using different user or screen names. Mr. _____ stated he has had to contact some of the sites to request they take certain postings off their site, which many of them did. Mr. _____ stated he noticed a posting on the website "businessinsider.com" dated _____ at _____ hours by _____ posted a comment mentioning _____ full name, his ex-wife's full name and that _____ is still posting photos of herself drinking in short skirts. The posting also mentions Mr. _____ brother having been in rehab. Mr. _____ stated few people were aware of Mr. _____ brother having been in rehab and Teri Buhl knew that information.				
I am requesting all Internet records including Internet Protocol Address (IP) as well as subscriber information for _____ who posted harassing comments on the Business Insider website on _____ (EST). The URL for the web page is;				
<input checked="" type="checkbox"/> continued on separate page.				
DATE AND SIGNATURE	DATE	SIGNED (Affiant) (To be signed and sworn to in the presence of a Superior Court Judge)		
	1/21/11	<i>Sgt. Carol Ogrinc</i>		

# search warrant

Equivale al nostro decreto di perquisizione

Consente alla polizia giudiziaria di cercare prove di un crimine o l'identità del presunto responsabile di un crimine su persone, locali e veicoli

Discende dal 4° Emendamento e riguarda luoghi fisici





# NSLs

- Sono semplici lettere firmate dal direttore dell'FBI o da un senior official con cui vengono chiesti agli ISP i dati dei loro utenti
- Il Patriot Act del 2001 ha esteso la loro applicazione a tutti i cittadini americani per indagini di terrorismo o antispionaggio
- Sono coperti da **gag order**, cioè un ordine di segretezza che vieta agli ISP, per ragioni di sicurezza nazionale, di rivelare a terzi la richiesta di accesso ai dati da parte del Bureau

# Come ottiene l'Italia i dati dagli ISP americani?

- Se si tratta di dati non di contenuto viene trasmesso (in genere via posta elettronica dalla P.G.) al provider il decreto del P.M. ed il provider risponde direttamente alla stessa P.G. richiedente
- Se si tratta di dati di contenuto, si seguono le procedure di mutua assistenza giudiziaria che comportano l'intervento del DOJ americano il quale, attraverso il procuratore competente (in genere della California), applica il diritto U.S.A. idoneo al caso di specie (subpoena, order o warrant) per ottenere i dati dal provider



Il caso Twitter/Occupy Wall Street

- Il 26 gennaio 2012 il NY County District Attorney invia a Twitter un subpoena chiedendo i dati dell'account @destructuremal (Malcolm Harris) ed i suoi tweet (già cancellati) per provare che aveva partecipato alla marcia sul ponte di Brooklyn
- Il 30 gennaio Twitter informa Harris del subpoena
- Il 16 marzo Harris propone una motion to quash avverso il subpoena
- Il 20 aprile la Criminal Court di NY respinge il ricorso
- Il 7 maggio Twitter impugna il subpoena confermato dalla Corte
- Il 30 giugno la Criminal Court rigetta il ricorso di Twitter
- Il 27 agosto Twitter appella l'ordine alla Corte Suprema di New York
- Il 14 settembre Twitter è costretta a consegnare comunque i dati
- Il 12 dicembre Harris viene condannato per "disorderly conduct" sulla base di due tweet: "We took the bridge", "they tried to stop us"

La Criminal Court di New York ha rigettato la richiesta di annullamento del subpoena sostenendo che:

1. I tweet sono pubblici
2. Anche se la Corte Suprema ha riconosciuto in passato una "reasonable expectation of privacy" sui dati memorizzati dagli ISP (United States v. Warshak), la decisione riguardava e-mail inviate a determinati soggetti non tweet che si rivolgono ad un numero indeterminato di persone
3. I tweet non sono coperti dal 4° Emendamento che garantisce protezione solo ai luoghi fisici ed Internet non è un luogo fisico ("that "home is a block of ones and zeros stored somewhere on someone's computer")

Nel suo appello Twitter ha sostenuto che:

1. I tweet sono coperti dal 1° Emendamento che protegge la libertà di espressione
2. I tweet sono coperti anche dal 4° Emendamento perché il Governo stesso ha ammesso, col subpoena, che non erano pubblicamente accessibili (erano stati cancellati) e dunque l'utente, che stando ai termini del servizio ne è proprietario, ha una ragionevole aspettativa di privacy su di essi



# Il caso Google/NSLs

- Google, seguita a ruota da Microsoft, quest'anno nel suo Transparency Report ha per la prima volta pubblicato (sebbene in forma aggregata) il numero delle NSLs ricevute
- Il 29 marzo 2013 Google ha sollevato una questione di incostituzionalità delle sezioni 2709 e 3511 del Titolo 18 dello USC che disciplina l'obbligo di segretezza delle lettere
- La causa è stata assegnata al giudice Susan Ilston che sempre lo scorso marzo aveva dichiarato incostituzionali gli stessi articoli per violazione del 1° Emendamento in un'azione promossa dalla EFF, un'associazione per i diritti civili (decisione peraltro appellata dal Governo americano)
- A fine maggio il ricorso di Google è stato respinto, ma il giudice si è riservato su 2 delle 19 lettere impugnate





Il digital due process

- È una campagna promossa da associazioni, avvocati, accademici, studenti, start-ups e major ICT tesa all'aggiornamento dell'ECPA (Electronic Communications Privacy Act)
- L'ECPA, che disciplina le modalità di accesso delle law enforcement ai dati elettronici, è infatti considerato obsoleto
- L'ECPA viene definito un "patchwork of confusing standards" che i tribunali interpretano in modo incoerente, generando incertezza sia nei provider che nelle forze dell'ordine

Le modifiche richieste riguardano:




- **Comunicazioni e documenti elettronici**: si chiede che il Governo si munisca di un search warrant per ottenere da un ISP il contenuto di e-mail, instant messages, file, foto, Internet search queries e chat sui social network di un utente, archiviati online (in quanto protetti dal 4° Emendamento esattamente come le telefonate e tutto ciò che è conservato nelle private dimore). Google applica già questa procedura sulla base della sentenza (unica) del 2010 del Sesto Circuito, *United States v. Warshak*
- **Mobile location**: si chiede parimenti un search warrant per la richiesta agli ISP di dati di localizzazione (cellulare, GPS e WiFi) sia in tempo reale che archiviati

## Introducing the program

A slide briefing analysts at the National Security Agency about the program touts its effectiveness and features the logos of the companies involved.

The seal of Special Source Operations, the NSA term for alliances with trusted U.S. companies.

TOP SECRET//SI//ORCON//NOFORN



# PRISM/US-984XN Overview

OR

## *The SIGAD Used Most in NSA Reporting* Overview

April 2013

Derived From: NSA/CSSM 1-52  
Dated: 20070108  
Declassify On: 20360901

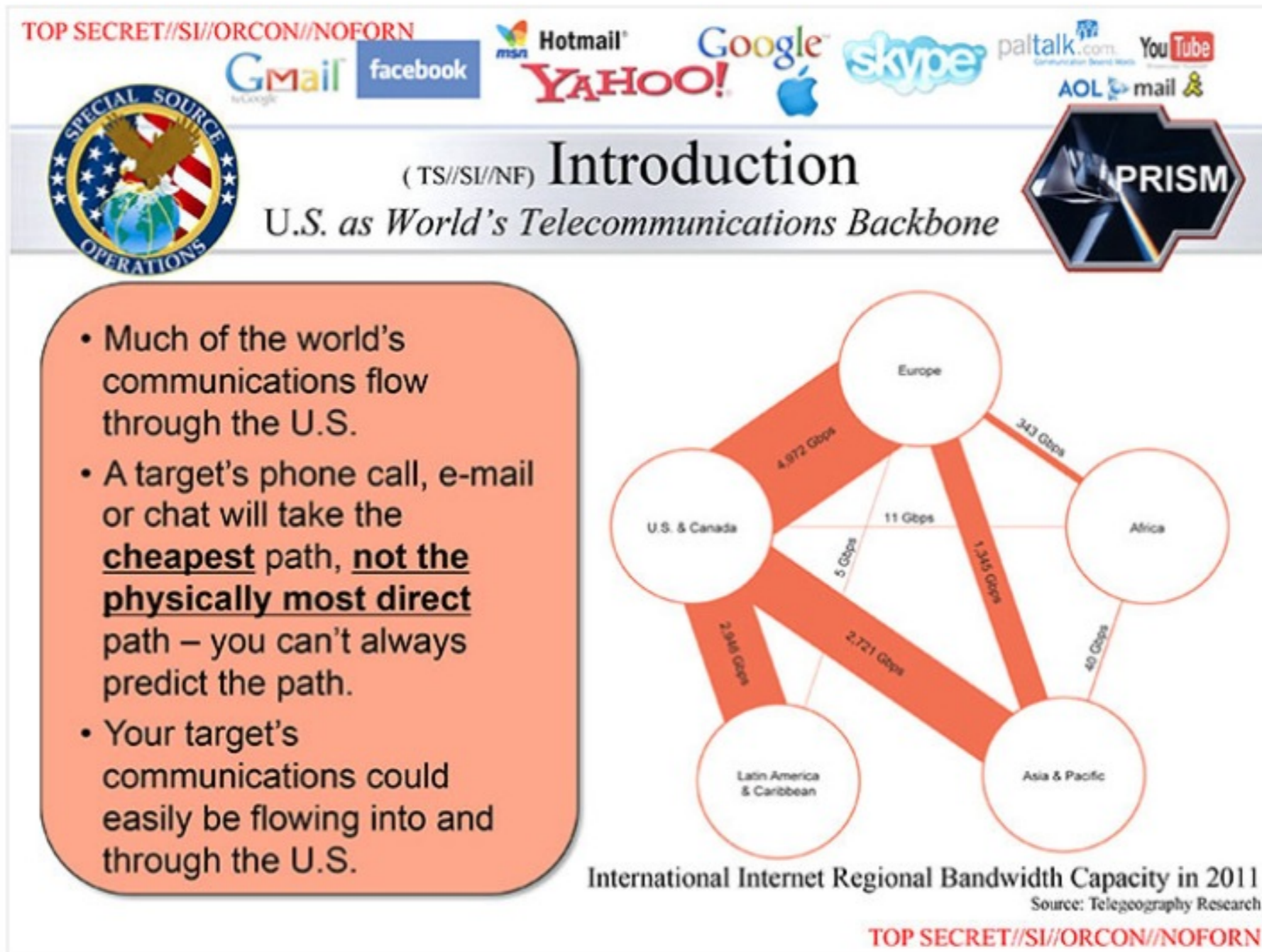
TOP SECRET//SI//ORCON//NOFORN

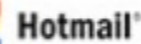
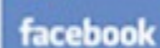
The program is called PRISM, after the prisms used to split light, which is used to carry information on fiber-optic cables.

This note indicates that the program is the number one source of raw intelligence used for NSA analytic reports.

## Monitoring a target's communication

This diagram shows how the bulk of the world's electronic communications move through companies based in the United States.





# (TS//SI//NF) PRISM Collection Details



## Current Providers

- Microsoft (Hotmail, etc.)
- Google
- Yahoo!
- Facebook
- PalTalk
- YouTube
- Skype
- AOL
- Apple

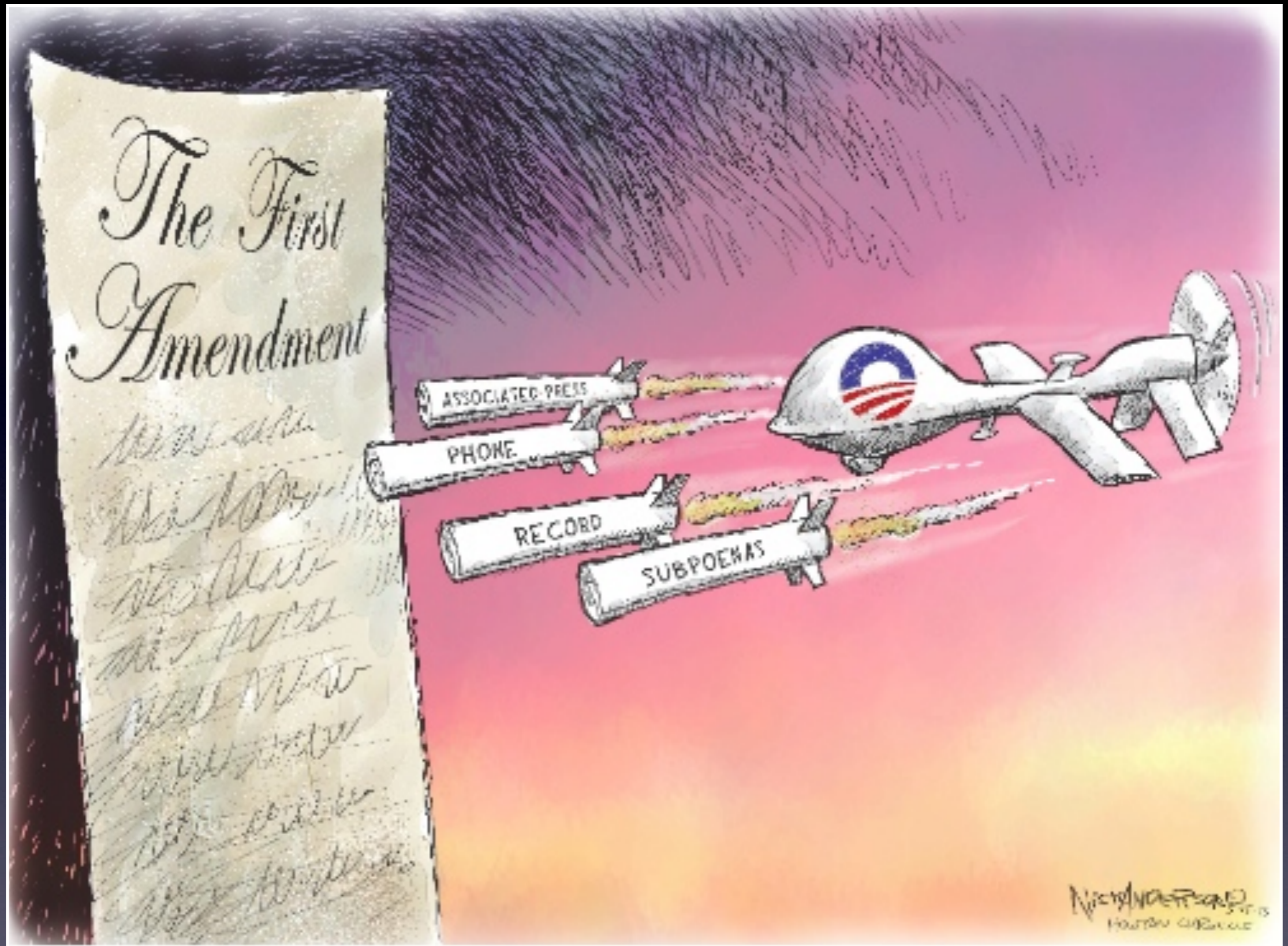


## What Will You Receive in Collection (Surveillance and Stored Comms)?

It varies by provider. In general:

- E-mail
- Chat – video, voice
- Videos
- Photos
- Stored data
- VoIP
- File transfers
- Video Conferencing
- Notifications of target activity – logins, etc.
- Online Social Networking details
- **Special Requests**

Complete list and details on PRISM web page:  
Go PRISMFAA



Q&A

# Grazie!

Monica A. Senior - Carlo Blengino  
[www.penalistiassociati.it](http://www.penalistiassociati.it)  
@MASenior - @CBlengio

Tutto è in C.C. 3.0 IT