BEHIND DATAGATE

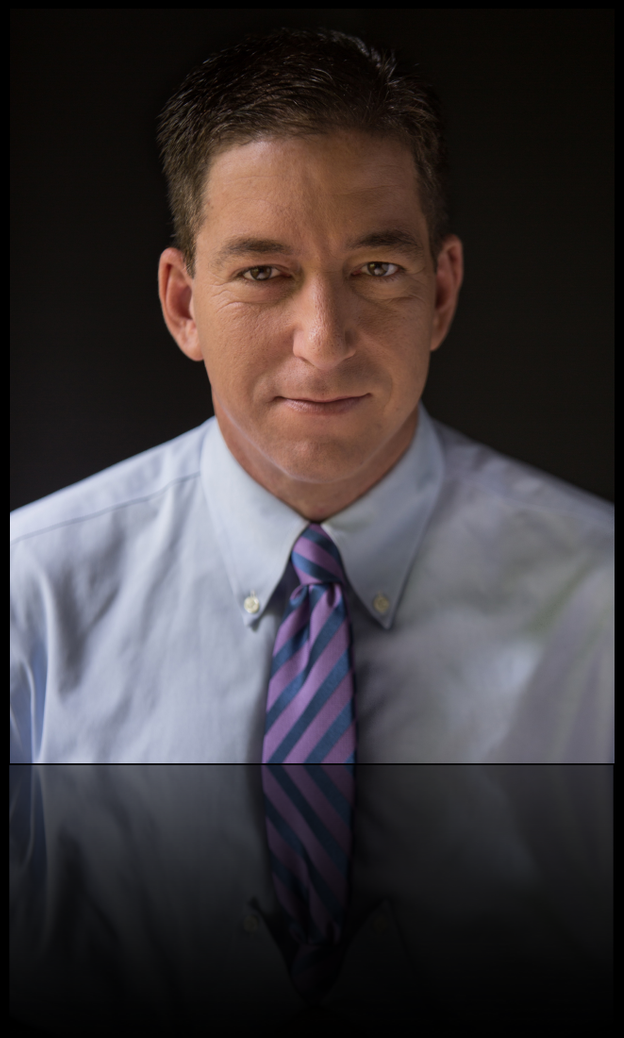
Chiara Marchetti e Matteo Longeri
Dipartimento di Informatica
Università degli Studi di Milano
Milano, Italia
chiara.marchetti1@studenti.unimi.it
matteo.longeri@studenti.unimi.it

“Il vero valore di una persona non si misura dalle cose in cui sostiene di credere, ma da che cosa è disposto a fare per proteggerle.”

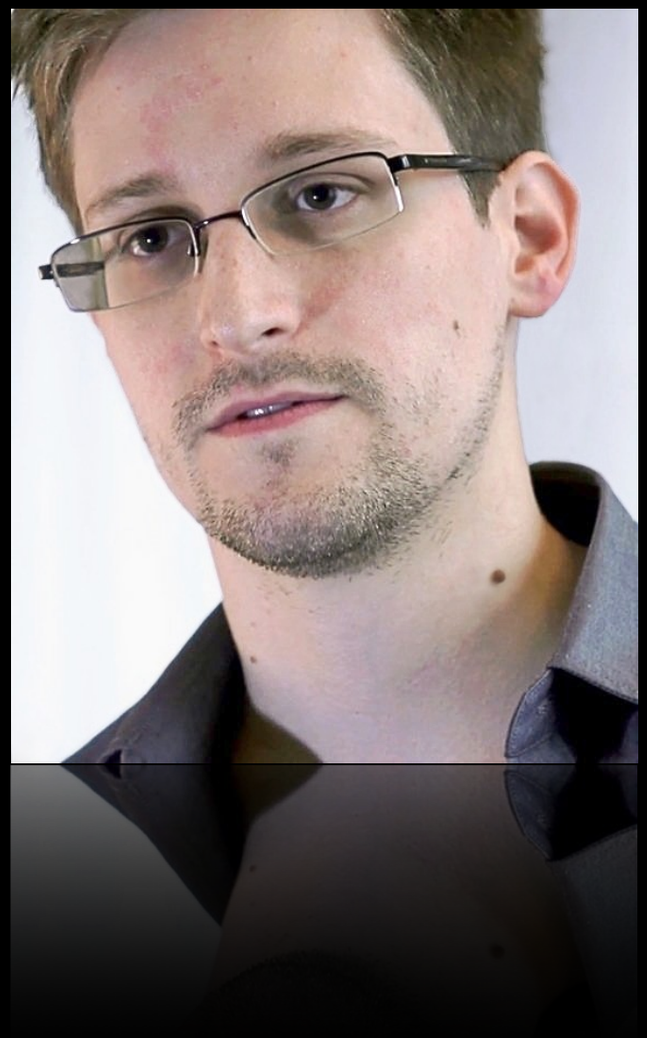
(Edward Snowden)

NSA

GLENN GREENWALD



EDWARD SNOWDEN



GCHQ

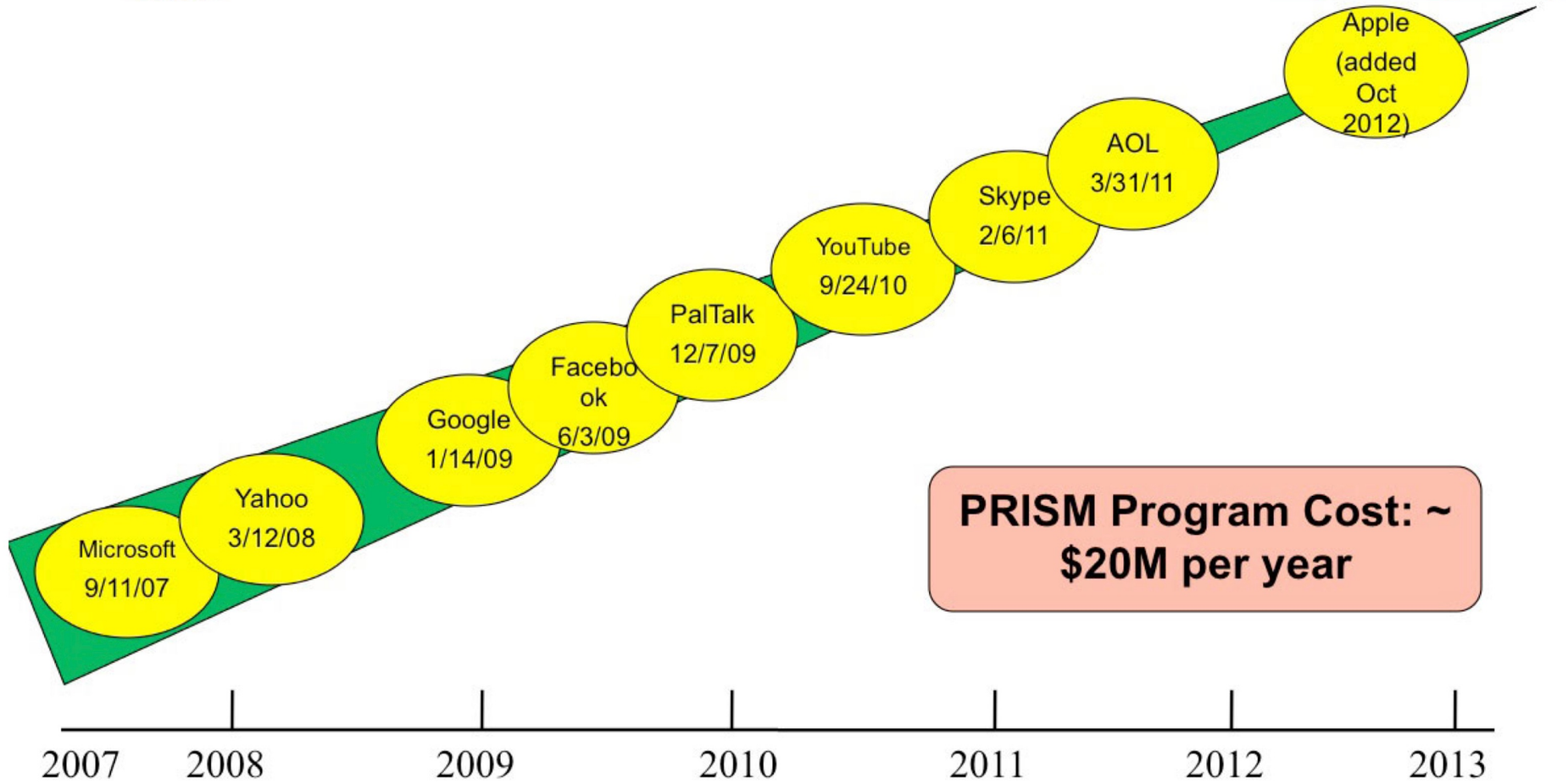
I PROGRAMMI DI SORVEGLIANZA

PRISM

- È **nato nel 2007** e ha visto nel tempo l'aggiunta di nuove aziende alla lista delle cooperanti
- Lo scopo del programma era l'**implementazione di backdoor nei sistemi dei principali colossi IT statunitensi** per permettere alla NSA un accesso diretto ai dati degli utenti
- Attraverso PRISM l'agenzia ha potuto **raccogliere qualsiasi tipo di contenuto generato in rete dagli utenti**: e-mail, chat, conversazioni VoIP, foto, ecc.
- **Dal 2010** è stato fornito l'**accesso al GCHQ** e **dal 2012** anche **a FBI e CIA**

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider



PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

Slide complete: https://s3.amazonaws.com/s3.documentcloud.org/documents/813847/prism.pdf

- **BOUNDLESS INFORMANT**: programma **ideato per quantificare e mappare con precisione le attività di sorveglianza quotidiane effettuate nei paesi stranieri** attraverso reti telefoniche ed Internet
- **BLARNEY**: programma di **raccolta dei metadati nei punti di congestione che si formano lungo la dorsale di Internet**. Viene attuato grazie alla collaborazione con le società che gestiscono le apparecchiature di rete costituenti i nodi nevralgici del web
- **XKEYSCORE**: **software** utilizzato dal 2007 **per gestire i dati raccolti attraverso gli altri programmi di sorveglianza**, permettendo agli analisti dell'agenzia di ricercare qualsiasi informazione in vasti database. Il sistema mantiene registrata l'integralità dei dati per alcuni giorni, permettendo di analizzare e memorizzare in maniera definitiva quelli di interesse
- **MUSCULAR**: **programma del GCHQ** in collaborazione con la NSA realizzato **per intercettare le informazioni in chiaro che transitavano attraverso le fibre ottiche che collegano i data center di Google e Yahoo** senza che questi ne fossero al corrente

LE AZIENDE COINVOLTE

GOOGLE

- **Collaborazione con la NSA nel 2010** a seguito degli **attacchi a Gmail in Cina**
- Partecipazione al programma ***PRISM*** della NSA **dal 2009**
- **Violazione** delle **connessioni tra i data center** da parte del GCHQ e della NSA col progetto ***MUSCULAR***
- Attuale **sviluppo** della funzionalità di **crittografia End-to-End per Gmail** basata sullo standard *OpenPGP*
- Sentenza **Corte di giustizia dell'Unione Europea** sul ***Diritto all'Oblio*** nel **maggio 2014**

FACEBOOK

- **Dal 2009** partecipazione ai programmi ***PRISM* e *BLARNEY*** della NSA
- Coinvolgimento nel **progetto della NSA *TURBINE*** per infettare le macchine degli utenti con un'**attacco *One-Man-on-the-Side* chiamato *Quantumhand***. A seguito di ciò Zuckerberg ha chiamato Obama per lamentarsi
- **Nel 2013** è stato introdotto il **protocollo *HTTPS*** e **nel 2014** è stato aggiunto il **dominio *.onion* per gli utenti *Tor***
- **Nel 2014** sono state introdotte le **opzioni *Privacy Basics* interattive** per aiutare gli utenti nella gestione della propria privacy
- **Nel 2015** è stata realizzata una ***Class Action* europea per la gestione della privacy** relativa ai dati

WHATSAPP

- **Il creatore** Jan Koum **ha sempre combattuto per la difesa della privacy dei propri utenti**, promettendo di non modificare le politiche a seguito dell'acquisizione

- **Nel 2014 viene acquistata da Facebook** per 19 miliardi di dollari

- Sempre **nel 2014** è stata **integrata la crittografia *End-to-End* per** la versione **Android** dell'applicativo

- **Nel 2015 Facebook nei suoi ToS ha dichiarato di ricevere informazioni sugli utenti da tutte le aziende di sua proprietà.** Questo ha aperto dubbi sull'effettivo mantenimento delle politiche originali di WhatsApp

TWITTER

- Non è **mai entrata a far parte del progetto *PRISM***, tuttavia **ha fornito dati nel caso di richieste esplicite** del Tribunale FISA

- **Ha sporto denuncia alla Corte Federale della California** circa le limitazioni di trasparenza relative alle richieste governative

- **Nel 2013** ha integrato il **protocollo *HTTPS***

APPLE

- **Nel 2008** accuse sul ***malware Dropout Jeep*** sviluppato dalla NSA **per** il sistema **iOS**
- È stata l'**ultima** delle aziende **ad aderire al *PRISM* nel 2012**
- Ha ricevuto **accuse** sulla funzionalità di **salvataggio automatico** per il servizio ***iCloud Drive***
- **Nel 2014** integrazione della **crittografia in locale per iOS e Mac OSX**, **accusata dalla FBI** di oltraggio alle indagini
- Sempre **nel 2014** realizzazione di una **sezione del sito dedicata alla privacy**, con la **pubblicazione di una lettera di Tim Cook** ai clienti. A seguito di questo viene tenuto un **discorso del CEO di Apple al *Vertice sulla Sicurezza Informatica e la Tutela dei Clienti* indetto dalla Casa Bianca**

MICROSOFT

- **Nel 1999** ha ricevuto l'accusa di avere integrato la **backdoor *NSA Key* nei sistemi Windows** a partire **dalla versione *'95***
- È stata la **prima azienda ad aderire al programma *PRISM* nel 2007**, quando il suo motto era: *"your privacy is our priority"*
- Ha ricevuto accuse anche da ex dipendenti come ad esempio Caspar Bowden
- **Dal 2014** ha rimarcato in diverse occasioni la **necessità di ristabilire la fiducia** degli utenti **attraverso** una **maggior trasparenza** del governo
- A seguito del **caso Alex Kibkalo**, l'azienda ha **rivisto** le sue **politiche interne relative all'intercettazione** di messaggi dei propri dipendenti

SKYPE

- È stata **acquistata nel 2011 da Microsoft** per 8,5 miliardi di dollari. A seguito di ciò l'**architettura è passata da *Distribuita* a *Centralizzata***

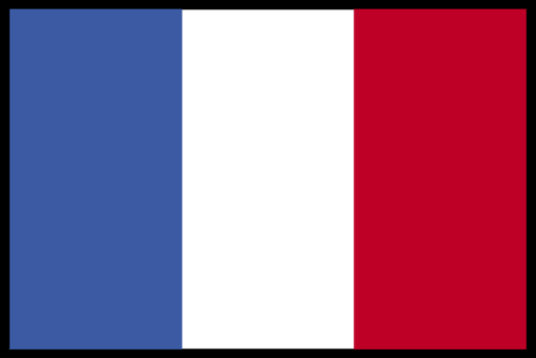
- Prima dello scoppio del Datagate, diversi ricercatori avevano evidenziato falle nella sua struttura

- **Accuse al brevetto *Legal Intercept*** depositato da Microsoft

- **Coinvolgimento** nel **programma** della **NSA** denominato ***Project Chess* e** nel programma ***RAMPART-A*** per le intercettazioni delle conversazioni *VoIP*

- A seguito dello scandalo sono state proposte soluzioni alternative come *Tox* e *MegaChat*

LA RISPOSTA DELL’EUROPA



FRANCIA

- **Intercettazione di 70 milioni di chiamate** dei cittadini francesi **dal 10 dicembre 2012 all'8 gennaio 2013**
- **Nel 2013 proposta al *Vertice UE di Bruxelles***, unitamente alla Germania, di un ***"codice etico di spionaggio"***
- **Nel marzo 2015** avvio definizione di un ***Patriot Act* francese** per offrire **libertà di spionaggio anti-terroristico illimitata**

GERMANIA

- **Nel 2013** notizia sull'**intercettazione del cellulare privato** della Cancelliera Angela **Merkel**
- Sempre **nel 2013 proposta al *Vertice UE di Bruxelles***, unitamente alla Francia, di un ***"codice etico di spionaggio"***
- **Nel 2014** la Merkel voleva **proporre** ad Hollande la **creazione** di un ***Network Europeo di Comunicazione***
- Sempre **nel 2014 arresto di un membro dei servizi segreti tedeschi in combutta con gli Stati Uniti**
- **Tra il 2014 e il 2015 adozione di *macchine da scrivere, cellulari anti-intercettazioni* e scioglimento del contratto del governo con Verizon**

ITALIA

- **Nel 1998** la **NSA** richiese alla **Telecom Italia** di poter **accedere agli snodi siciliani della dorsale** in fibra ottica sottomarina
- **Tra il 10 e il 28 dicembre 2012** sono stati **intercettati 46 milioni di metadati attraverso** il programma ***BOUNDLESS INFORMANT***. A seguito l'Italia ha inviato negli USA una delegazione del *COPASIR*
- A seguito di un **incontro tra** l'allora premier **Letta e** il sottosegretario USA **John Kerry**, l'ex presidente del consiglio dichiarò che la privacy degli italiani non era stata compromessa

REGNO UNITO

- È stato coinvolto nello scandalo Datagate essendo il GCHQ britannico il principale partner della NSA
- **David Cameron e Charles Farr** sono sostenitori **dell'operato del GCHQ** e difendono le intercettazioni mediate da questo
- **Nel febbraio 2015 l'*Investigatory Powers Tribunal* ha definito "illegale" l'attività di spionaggio del GCHQ e della NSA**

ANALISI DEI QUESTIONARI

IL CAMPIONE ANALIZZATO

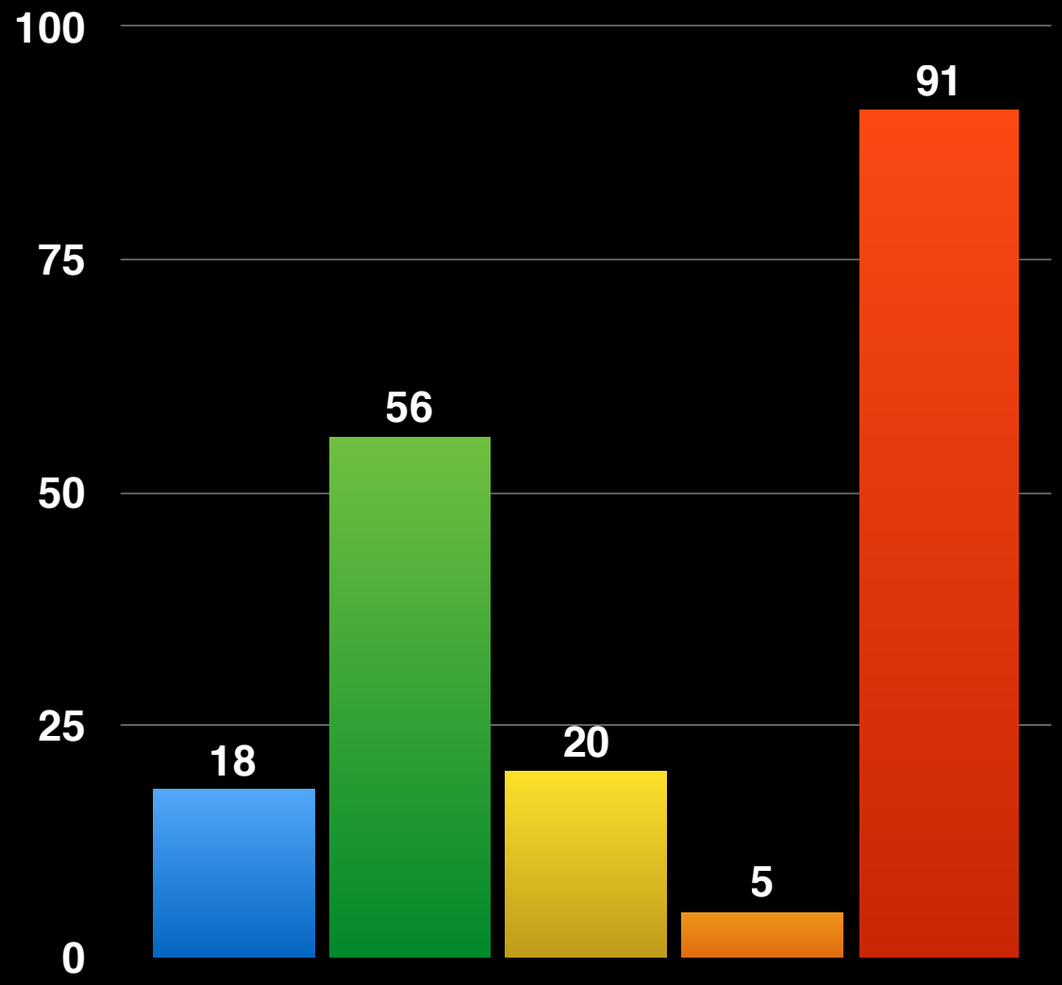
48 femmine

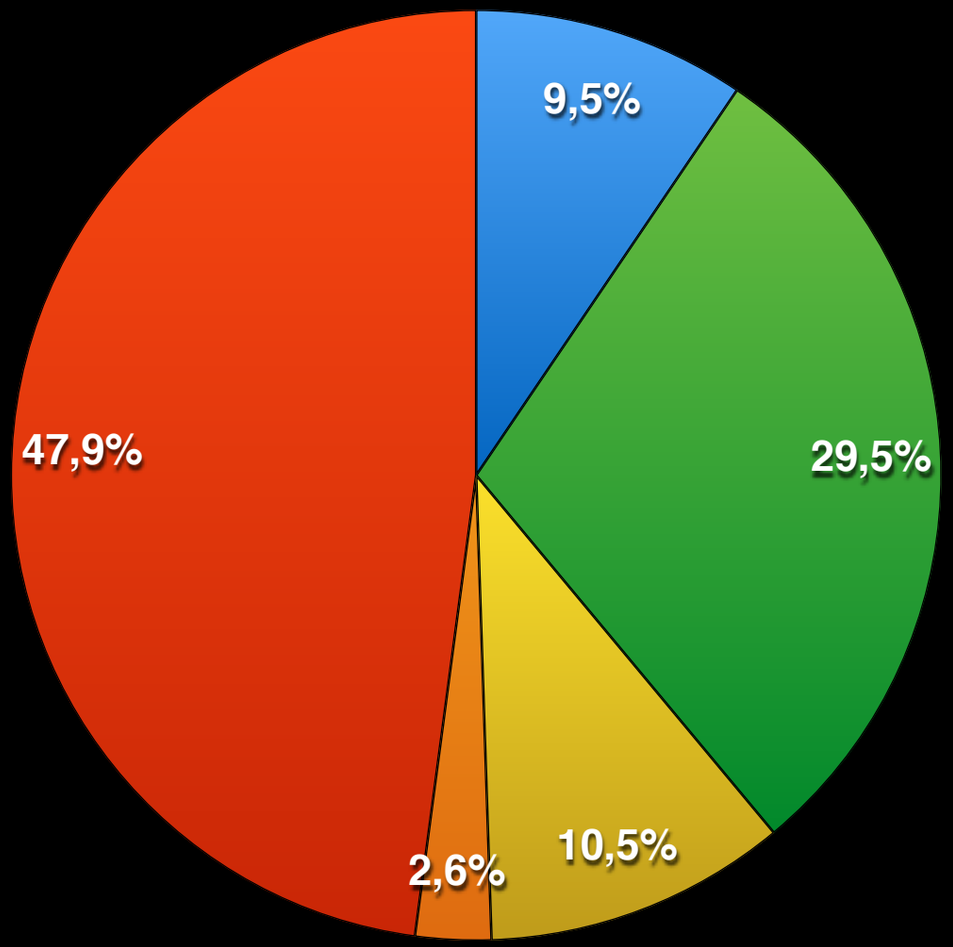
142 maschi

- **68,4%** degli intervistati appartengono alla fascia d’età **18-30**
- La quasi totalità del campione ha dichiarato di avere la **licenza media superiore** (**48,4%**) o la **laurea** (**46,3%**)
- Il **41,1%** sono **studenti**, i restanti si distribuiscono tra: **insegnanti/educatori** (**12,1%**), **esperti IT** (**10,5%**), **impiegati** (**9,5%**), **liberi professionisti** (**7,9%**) e **altro** (**18,9%**)

*Dati completi in fondo alla presentazione

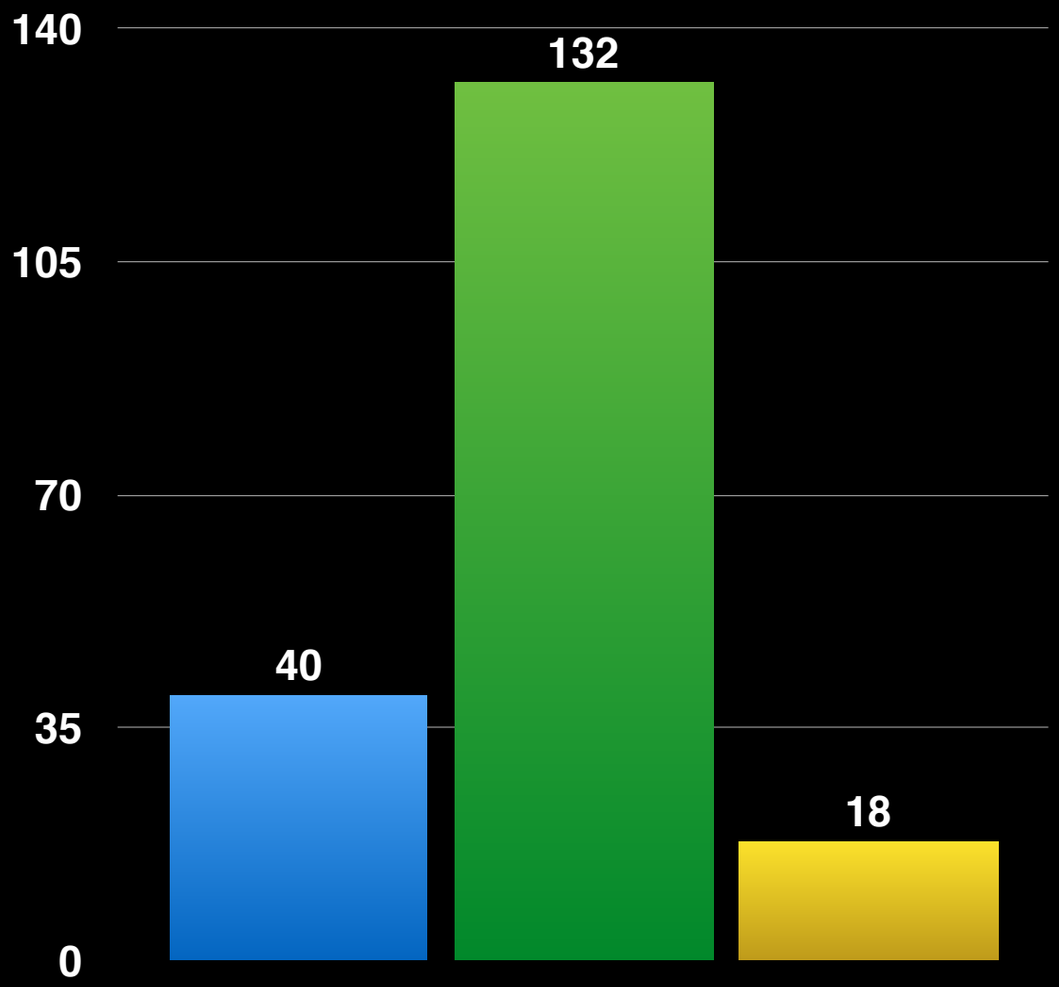
Come consideri il suo operato?

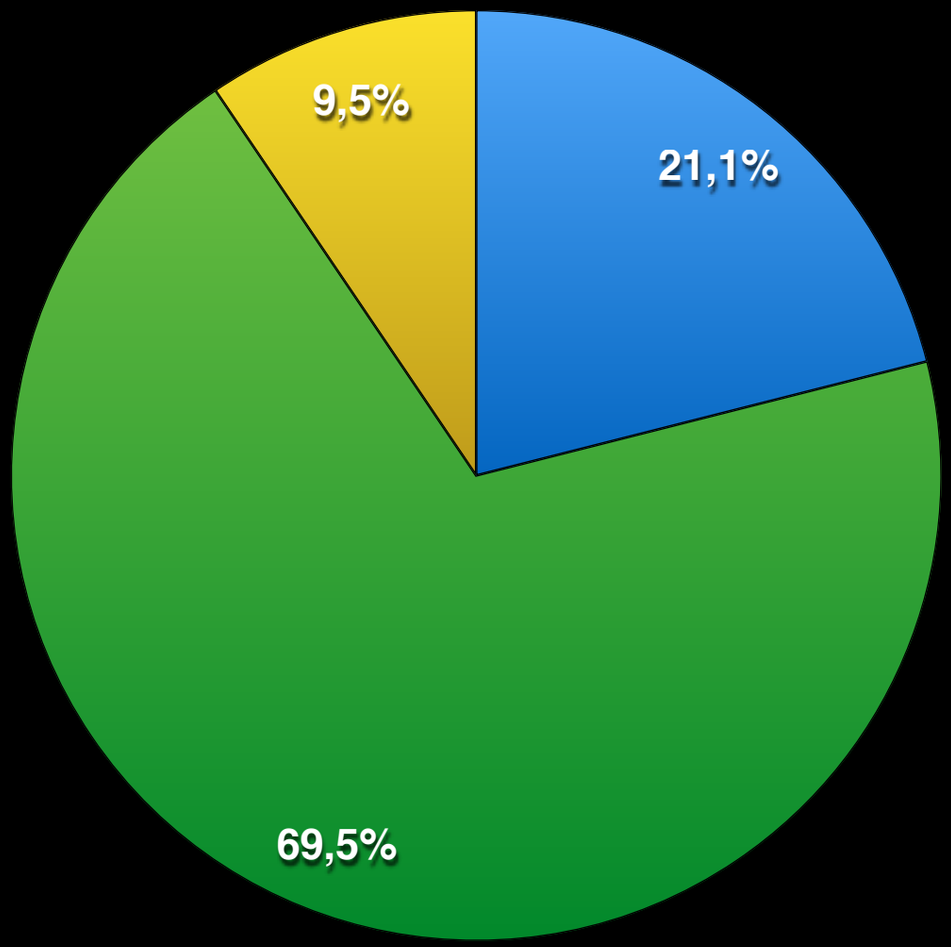




- Sconsiderato (ha messo in pericolo la sua Nazione)
- Eroico (ha messo la trasparenza davanti alla sua libertà personale)
- Esibizionista (voleva la notorietà, e l’ha avuta)
- Esagerato (ha ingigantito di molto le notizie che ha reso pubbliche)
- Una conferma (ha solo dato conferma a ciò che già immaginavo)

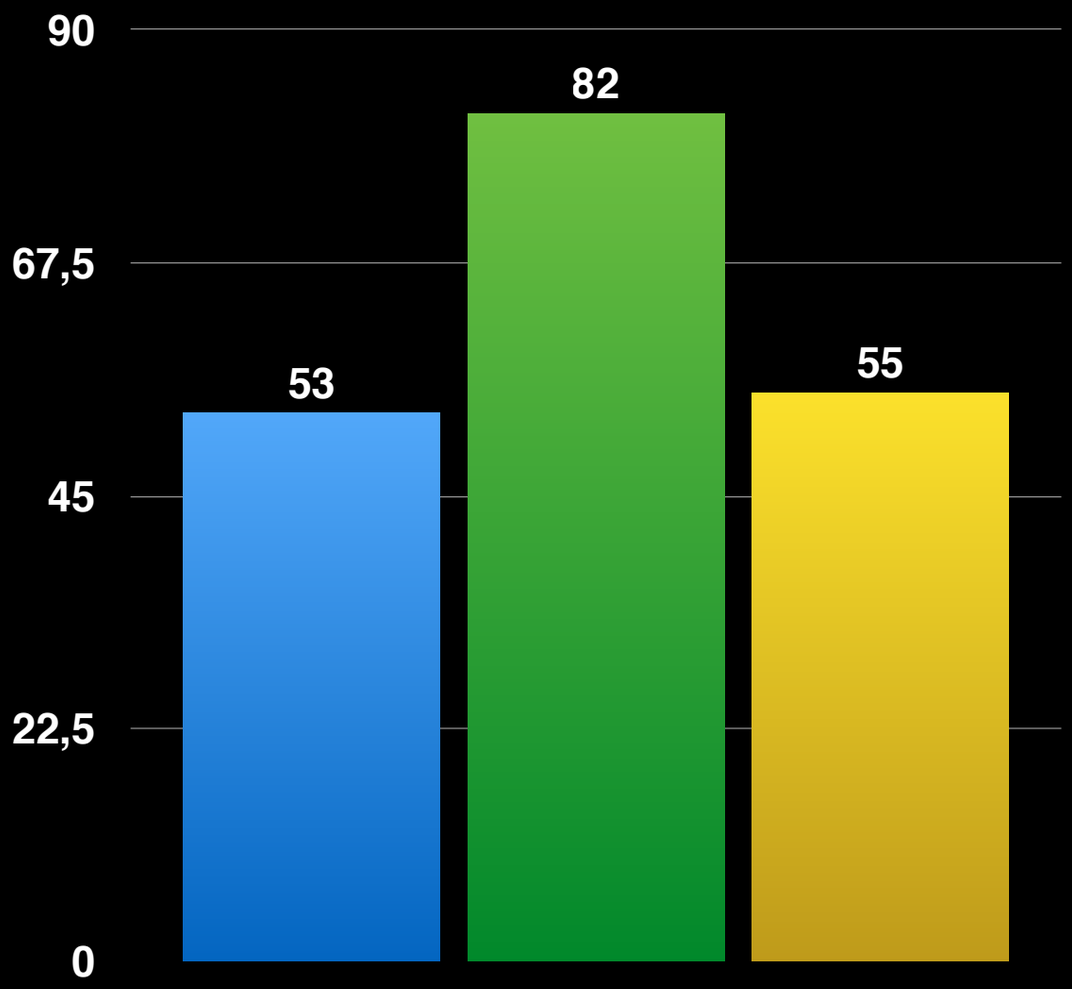
L’NSA ha giustificato il suo operato facendo riferimento alla lotta al terrorismo. Ritieni che la privacy individuale possa essere sacrificata a favore di questa giustificazione?

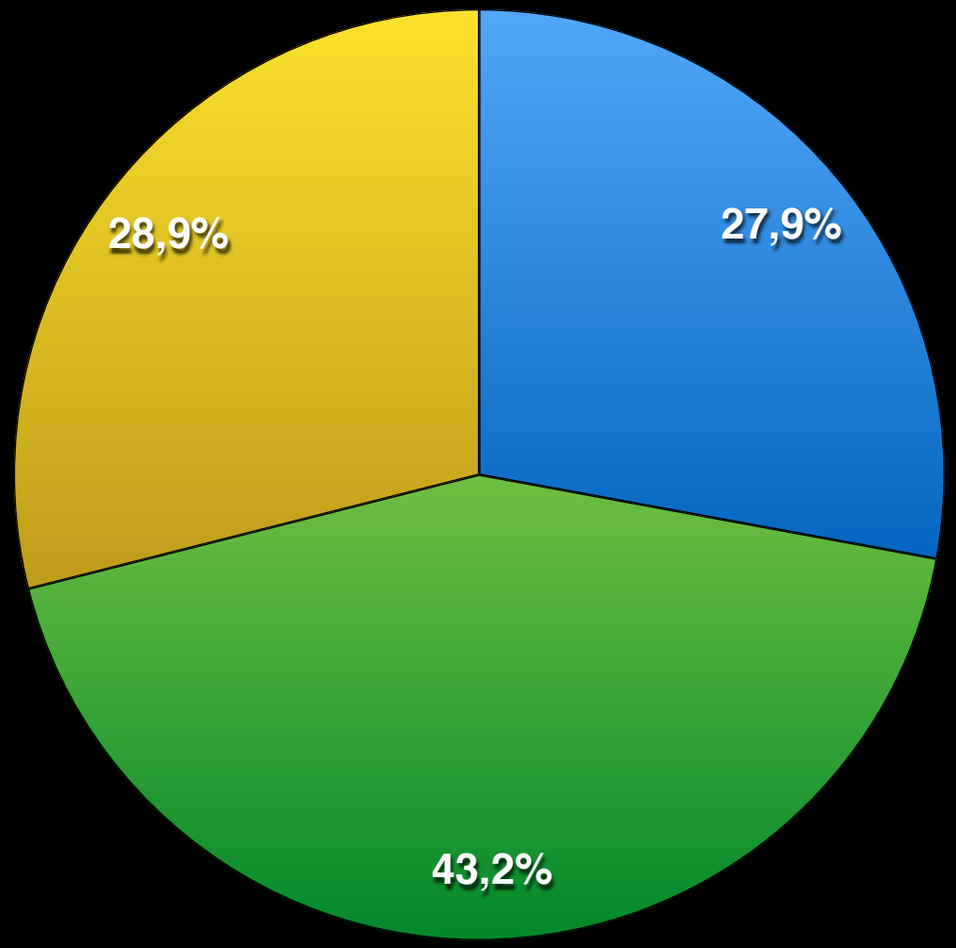




- Si, sono disposto ad essere intercettato se questo permette di garantire maggiore sicurezza alla popolazione
- Credo che le intercettazioni andrebbero eseguite solo nei confronti di sospetti reali e non a macchia d’olio
- No, un governo non dovrebbe mai poter monitorare la vita privata dei suoi cittadini

Come già accennato, lo scandalo non è restato confinato ai soli USA, ma si è dimostrato aver coinvolto molti paesi esteri. Alla luce di ciò, ti senti coinvolto dall'operato del NSA o pensi che la tua vita online non venga considerata dall'agenzia di sicurezza americana?





- Si, mi sento vittima delle attività di sorveglianza dell'agenzia
- No, ritengo che l'NSA sia più interessata ai vertici (politici ed economici) dei paesi esteri che non ai comuni cittadini
- No, non ho nulla da nascondere, non mi interessa dell'operato dell'agenzia

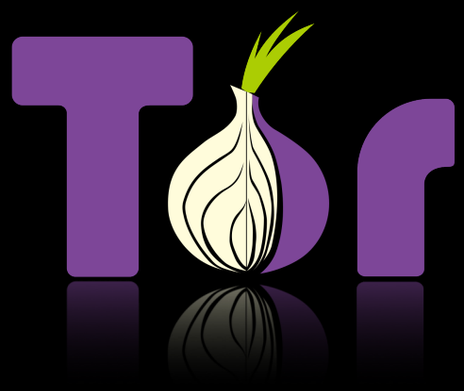
GLI STRUMENTI PER DIFENDERSI

CryptoCat

GNUPG

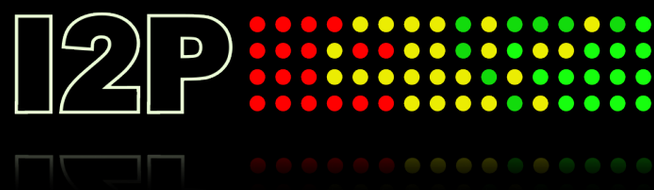
Tox

Telegram



GNUnet

Freenet



www.prism-break.org

File-System Crittografici

CONCLUSIONI

- Risulta **difficile dare un giudizio** su quanto accaduto senza avere a disposizione ogni singolo tassello collegato all'intera vicenda
- Il fatto che **Snowden** sia un **"Eroe" o** un **"Traditore"** è in bilico sulla sottile linea che divide cosa è giusto e cosa è sbagliato
- È **aumentata l'attenzione** da parte delle **aziende e** degli **sviluppatori** a tutti quegli elementi connessi a funzionalità di protezione della privacy, anche se questo apre il dubbio sulle finalità di ciò (**sentimento pro-privacy o mero profitto?**)
- È **impossibile esercitare il Diritto all'Oblio per ogni singola traccia** lasciata da ognuno di noi nella "Rete"
- Gli **utenti** hanno dimostrato una **maggior attenzione alle tematiche relative alla privacy**, dichiarando **però:** ***"non ho niente da nascondere"***, senza comprendere le reali implicazioni della Sorveglianza di Massa
- Nonostante quasi ogni giorno escano nuove notizie, **trascorsi quasi 2 anni** dalle dichiarazioni l'**attenzione dei cittadini comuni** verso l'argomento è **calata**

Q & A ?

GRAZIE PER L’ATTENZIONE