
PRISM/US-984XN
Overview
The SIGAD Used Most in NSA Reporting
Overview
April 2013
PRISM Case Notations
Introduction
FAA702 Operations
Upstream
PRISM
Collection Details
PRISM Collection Details
PRISM Collection Overview
PRISM/US-984XN
Overview
The SIGAD Used Most in NSA Reporting
Overview
April 2013

TOP SECRET//SI//ORCON//NOFORN

PRISM/US-984XN
Overview

OR

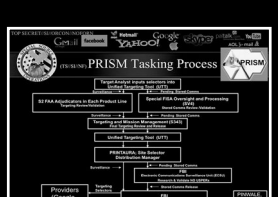
*The SIGAD Used **Most** in NSA Reporting*
Overview

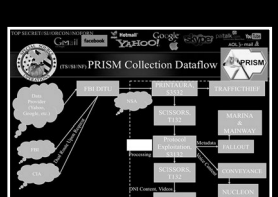
[redacted] PRISM Collection Manager, S35333

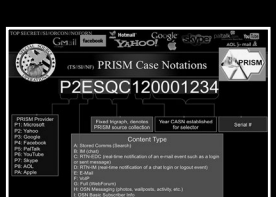
April 2013

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

TOP SECRET//SI//ORCON//NOFORN







On 6th June 2013, journalists[1] from The Guardian and Washington Post reported that the US National Security Agency[2] (NSA) was undertaking a portfolio of clandestine mass surveillance programs on a scale reminiscent of George Orwell's dystopian society of 1984. The NSA's initiatives supposedly ranged from the bulk collection of email and telephone records to infiltrating the data infrastructures of every leading Internet company and service provider.

In response to these allegations, the US government claimed that the NSA and other sections of its intelligence community were legally operating under the authority of laws such as the Foreign Intelligence Surveillance Act of 1978 (FISA) and the USA Patriot Act of 2001 that had been amended[3] in the post-9/11 political landscape to support the nation's continuous "War on Terror". However, the surveillance activities in question were not targeted at specific individuals or groups of interest, but rather focused on amassing personal data from millions of unsuspecting citizens indiscriminately and without clear jurisdiction or transparent oversight[4].

The first NSA program to be disclosed in these reports was PRISM – a "special source operation"[5] responsible for collecting stored data and live Internet transmissions obtained from a consortium of technology giants including Apple, AOL, Facebook, Google, Microsoft and Yahoo. Collaborating with the Five Eyes[6] network and major European allies, the NSA used PRISM and other related programs[7] to data mine the world's electronic communications systems in order to create vast information repositories that would give analysts the ability to "select" and "target" any individual in the world.

Given the increasingly connected digital nature of society, any proclaimed gains from such all-pervasive methods of surveillance must be weighed against the costs to personal freedom and privacy. With this in mind, perhaps it is useful to consider the story of the person who brought these revelations to the public's attention, Edward Snowden[8] – an everyman who might now be the Winston Smith[9] of this information age.

1. The reporters included Glenn Greenwald (political journalist, US) and Laura Poitras (documentary filmmaker, US) – Edward Snowden's original press contacts and (according to Greenwald) the only two people with full archives of his global surveillance disclosure.

2. The NSA is the organisation responsible for the production and management of signals intelligence (SIGINT) and information assurance for the US government. The agency is tasked with the global monitoring, collection, decoding, translation and analysis of information and data for foreign intelligence and counterintelligence purposes.

3. Section 702 of the FISA Amendments Act of 2008 and Section 215 of the USA Patriot Act (last extended by the PATRIOT Sunsets Extension Act of 2011) are often cited as the legal basis for many of the mass surveillance programs in the US.

4. The NSA's requests for surveillance warrants are overseen by the United States Foreign Intelligence Surveillance Court – a secret federal court whose hearings and records are closed to the public.

5. Special Source Operations is a division in the NSA which is responsible for all programs aimed at monitoring US communications systems through corporate partnerships.

6. The "Five Eyes" refer to an anglophonic alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States. These countries are bound by the multilateral UKUSA Agreement – a treaty for joint cooperation in signals intelligence. Documents leaked in 2013 revealed that the Five Eyes have been intentionally spying on one another's citizens and sharing the collected information with each other in order to circumvent restrictive domestic regulations on spying.

7. Other NSA and Five Eyes mass surveillance programs include: BOUNDLESSINFORMANT, BLARNEY, BULLRUN, DROPMIRE, FAIRVIEW, MUSCULAR, MYSTIC, OAKSTAR, PINWALE, STATEROOM, STORMBREW, TEMPORA and XKEYSCORE.

8. Edward Joseph Snowden (born 21 June 1983 in Elizabeth City, North Carolina, US) is an American computer specialist, former employee of the Central Intelligence Agency and former contractor for the NSA. He came to international attention when he disclosed thousands of classified documents to several media outlets, which he had acquired while working for the American consulting firm Booz Allen Hamilton. A subject of controversy, Snowden has been variously called a hero, a whistleblower, a dissident, a traitor and a patriot. Snowden's "sole motive" for leaking the documents was, in his words, "to inform the public as to that which is done in their name and that which is done against them."

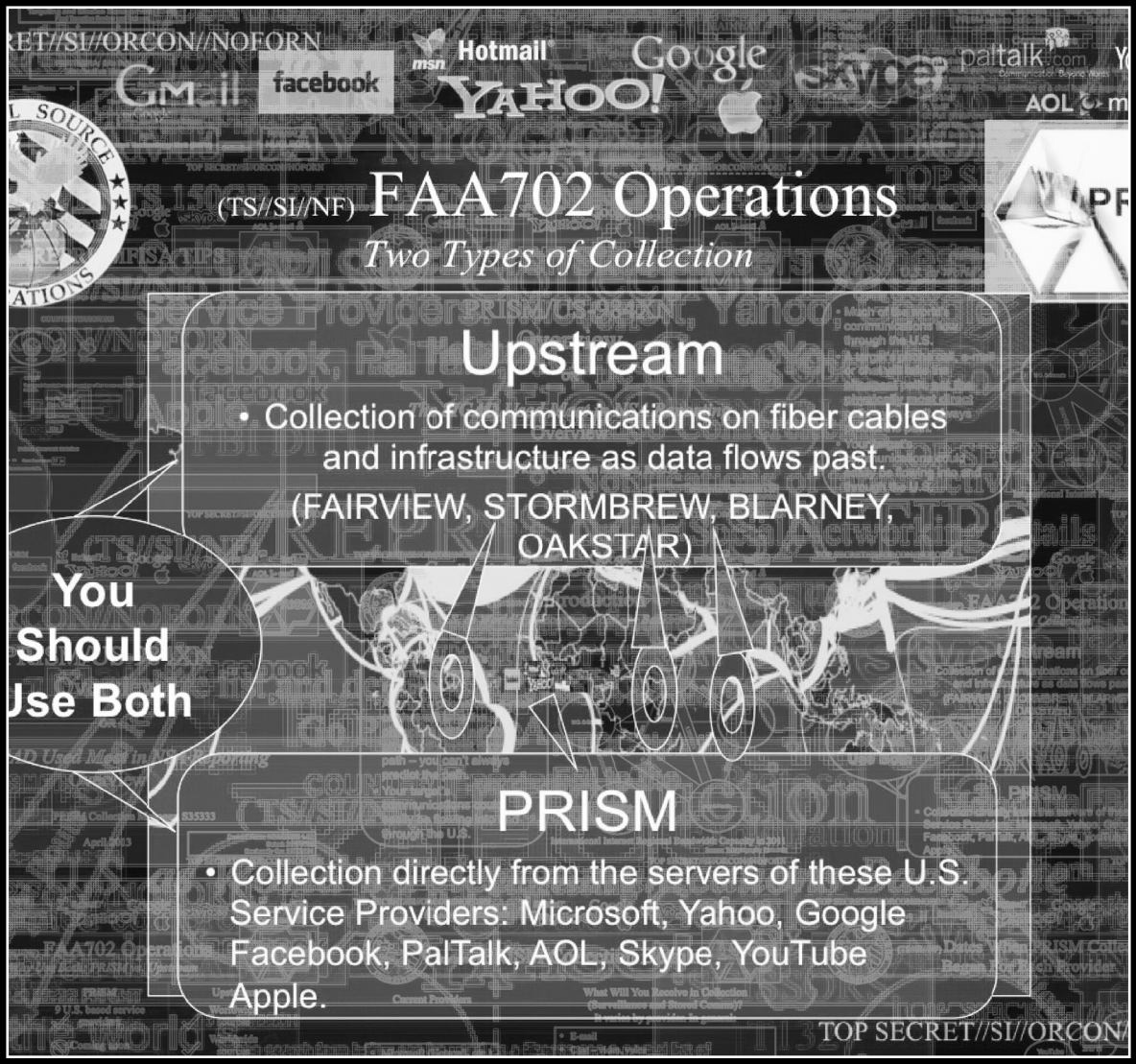
9. Winston Smith is a fictional character and the protagonist of George Orwell's novel 1984. The character was employed by Orwell as an everyman in the setting of the novel, a "central eye ... [the reader] can readily identify with".

PUBLIC NOTES collected from _ en.wikipedia.org _ 01/04/2014

GOVERNMENT control..?

“...Every time you pick up the phone, dial a number, write an email, make a purchase, travel on the bus carrying a cell phone, swipe a card somewhere, you leave a trace and the government has decided that it’s a good idea to collect it all, everything, even if you’ve never been suspected of any crime. Traditionally the government would identify a suspect, they would go to a judge, they would say we suspect he’s committed this crime, they would get a warrant and then they would be able to use the totality of their powers in pursuit of the investigation. Nowadays what we see is they want to apply the totality of their powers in advance - prior to an investigation...”

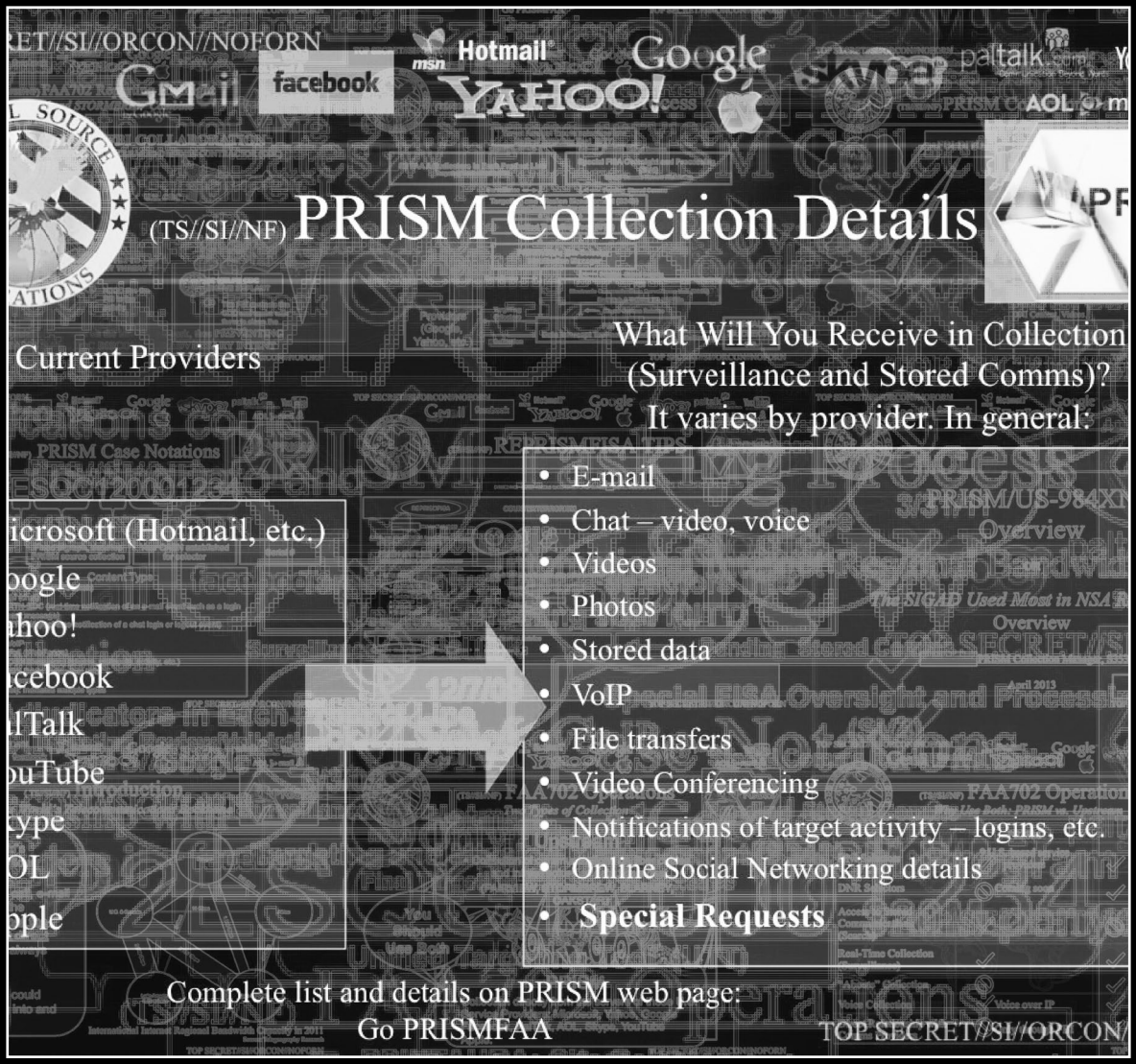
ARTICLE tinyurl.com/guardian-prism-whistleblower
COMMENT www.ndr.de/ratgeber/netzwelt/snowden277.html



CORPORATE collusion..?

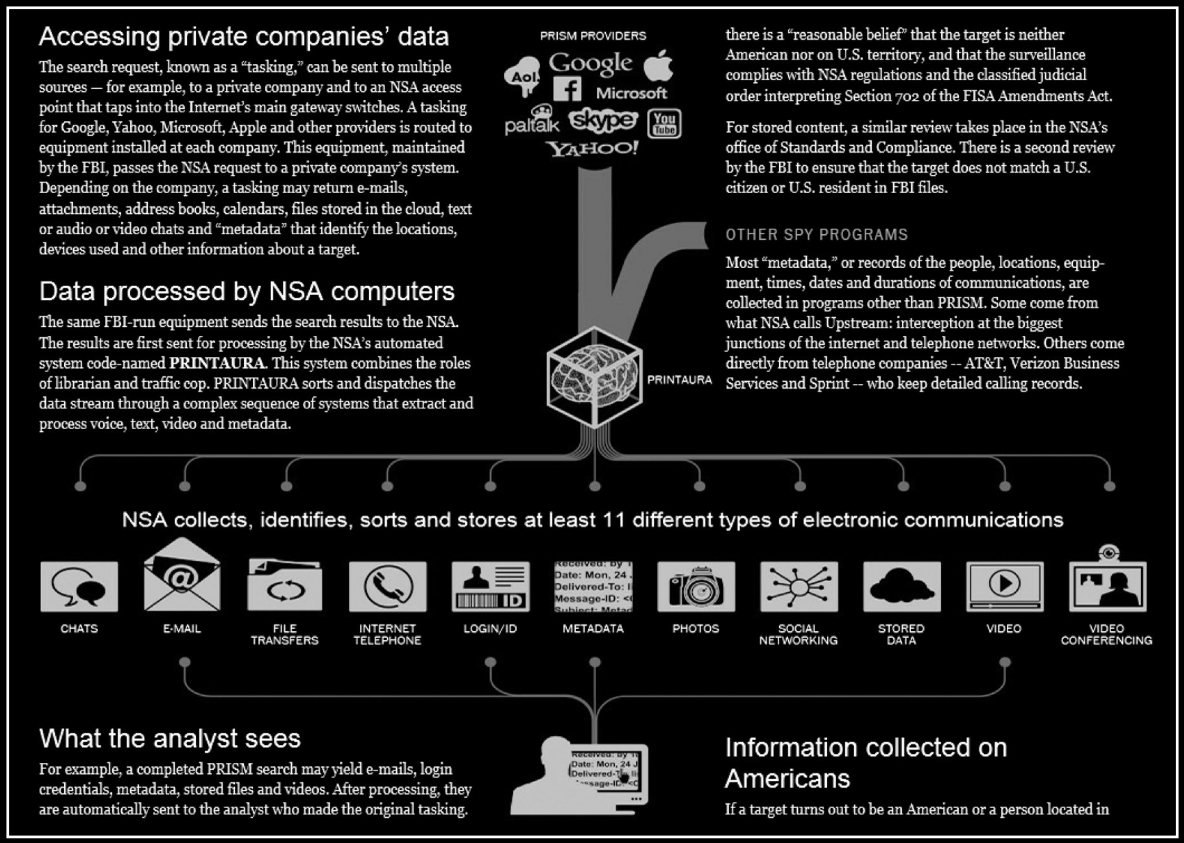
“...‘Direct Access’ didn’t mean no access. ‘Back door’ didn’t mean no door. ‘Only in accordance with the law’ didn’t mean PRISM is illegal. And you didn’t need to have heard of a codename to have participated. Larry [Page], [Mark] Zuck[erberg], you didn’t spell out your denials of the NSA’s data spying program in plain English, and now we know why. You were obligated to help the government in its spying, but were muzzled. The New York Times says you knowingly participated in the NSA’s data monitoring program. In some cases, you were asked to create ‘a locked mailbox and give the government the key’, to allow it to peer into private communications and web activity. Even if the exact words of your denials were accurate, they seemed to obscure the scope of your involvement with PRISM. Outlining as clearly as possible exactly what kind of data the government could attain would have gone a long way. [...] The terms you used disguised what was going on. Direct access means unrestricted access with no intermediary, but the government didn’t need to be standing in the server rooms to get what it wanted. A back door means access to data without its host’s knowledge or consent, but you were well aware of the NSA’s snooping. The NSA’s actions are likely protected by law, so saying you’re only honoring prying that’s legal didn’t mean no prying. And why would the government tell you the juicy codename or details of its data spying program? All it had to say is it needed your data. Now these excuses ring hollow. The average citizen doesn’t know the difference. They heard ‘we didn’t help the NSA’, and you did, so their trust in you has disintegrated. That’s a threat to your business, and our way of life. I like that all my friends use Google Docs. I like that I can invite any of my friends to a Facebook Event. Seeing them ditch the building blocks of the web you’ve developed because they don’t believe anything you say anymore will be a great inconvenience. And that inconvenience pales in importance to the actual liberty PRISM strips away from us...”

ARTICLE tinyurl.com/nytimes-prism-companies
COMMENT techcrunch.com/2013/06/07/doublespeak-denials-and-broken-hearts



PUBLIC

vulnerability..?



"...Because even if you're not doing anything wrong you're being watched and recorded. And the storage capability of these systems increases every year consistently by orders of magnitude to where it's getting to the point where you don't have to have done anything wrong. You simply have to eventually fall under suspicion from somebody - even by a wrong call. And then they can use this system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with. And attack you on that basis to sort of derive suspicion from an innocent life and paint anyone in the context of a wrongdoer..."

ARTICLE tinyurl.com/washingtonpost-prism-workings
COMMENT www.youtube.com/watch?v=0hLjuVyIIrs

PRISM

Michael Takeo Magruder

produced in dialogue with: Dr. Sarah Grochala (curation)

with thanks to: Angelo Petsas & William Warrener (production)
Dr. Btihaj Ajana (discourse)

commissioned by: Headlong (www.headlong.co.uk)
for the Cultural Institute at King's College London

published by: School of Arts & Humanities, King's College London
ISBN 978-1-897747-30-8

on the occasion of: the 1984 Digital Double Project
(www.digital-double.com)

about the artist:

Michael Takeo Magruder (1974, US/UK) is an artist and researcher based in the Department of Digital Humanities, King's College London. In the last 15 years, his projects have been showcased in over 250 exhibitions in 30 countries, and his art has been widely supported by numerous funding bodies and public galleries within the UK, US and EU. His practice explores concepts ranging from media criticism and aesthetic journalism to digital formalism and computational aesthetics, deploying Information Age technologies and systems to examine our networked, media-rich world.

FURTHER INFORMATION www.takeo.org


PRISM
PRISM/US-984XN
Overview
The SIGAD Used Most in NSA Reporting
Overview
April 2013