Západočeská univerzita v Plzni

Fakulta filozofická

Bakalářská práce

Kauza PRISM

Petr Pěkný

Plzeň 2015

Západočeská univerzita v Plzni

Fakulta filozofická

Katedra politologie a mezinárodních vztahů

Studijní program Mezinárodní teritoriální studia

Studijní obor Mezinárodní vztahy – britská a americká studia

Bakalářská práce

Kauza PRISM

Petr Pěkný

Vedoucí práce:

doc. PhDr. Přemysl Rosůlek, Ph.D.
Katedra politologie a mezinárodních vztahů
Fakulta filozofická Západočeské univerzity v Plzni

Plzeň 2015

Prohlašuji, že jsem práci zpracoval samostatně a použil jen uvedených pramenů a literatury.

Plzeň, duben 2015 ……

Chtěl bych poděkovat vedoucímu své bakalářské práce doc. PhDr. Přemyslu Rosůlkovi, Ph.D. za odborné vedení, věcné připomínky, za pomoc a rady při jejím zpracováním.

Obsah

SEZNAM POUŽITÝCH ZKRATEK

ARPANET – Advanced Research Projects Agency Network (počítačová síť, předchůdce dnešního internetu)

ASD – Australian Signals Directorate (Australská zpravodajská služba)

CIA – Central Intelligence Agency (Ústřední zpravodajská služba)

CSEC – Communications Security Establishment Canada (Kanadská zpravodajská služba)

FBI – Federal Bureau of Investigation (Federální úřad pro vyšetřování)

FISA – Foreign Intelligence Surveillance Act (zákon o špehování zahraničních agentů)

FISC – Foreign Intelligence Surveillance Court (Soud pro dozor nad zahraniční špionáží)

GCSB – Government Communications Security Bureau (Novozélandská zpravodajská služba)

GCHQ – Government Communications Headquarters (Vládní komunikační ústředí - zpravodajská služba Velké Británie)

GPS – Global Positioning Systém (Globální polohovací systém)

IP – Internet Protocol

NSA – National Security Agency (Národní bezpečnostní agentura)

NSL - *National Security Letters* (Národní bezpečnostní dopisy)

NT4 – New Technology (Později Microsoft od tohoto značení operačních systémů Windows opustil)

PRISM – Planning Tool for Resource Integration, Synchronization and Management (Nástroj pro plánování, integraci a řízení zdrojů)

STASI – Ministerium für Staatssicherheit (Ministerstvo státní bezpečnosti)

USA PATRIOT ACT – Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (Sjednocování a posilování Ameriky poskytováním vhodných pomůcek potřebných pro stíhání a bránění terorismu*)*

VoIP – Voice over Internet Protocol (Přenos hlasu prostřednictvím internetového protokolu)

1 ÚVOD

Ještě pod Bushovou administrativou roku 2007 spustila *National Security Agency* (NSA) program na tajné sbírání elektronických dat. Cílem programu PRISM je sbírat informace z internetové a telefonní komunikace uživatelů, jak ve Spojených státech, tak ve světě. Existenci tohoto programu prozradil Edward Snowden, bývalý pracovník CIA (Ústřední zpravodajská služba) a dodavatel NSA. Snowden poukázal na to, že NSA nezískává data pouze o zločincích a potencionálních hrozbách pro USA, ale i o běžných uživatelích či dokonce vysokých politických činitelích. Právě odposlechy např. německé kancléřky Angely Merkelové vyvolaly velký rozruch nejen mezi obyčejnými lidmi, ale i na mezinárodní politické scéně. Od uveřejnění Snowdenových dokumentů britským deníkem *The Guardian* se stala kauza PRISM jednou z nejsledovanějších bezpečnostních kauz.

Cílem mé práce bude zjistit, jaké důsledky měla kauza PRISM. Výzkumné otázky pro mne budou, zda odhalení kauzy PRISM mělo vliv na změnu jednání Obamovy administrativy a jaký vliv to mělo na konkrétní postupy NSA při sběru dat a informací. Dále budu zkoumat vliv kauzy PRISM na veřejné mínění a dopady na změnu chování uživatelů na internetu a na sociálních sítích.

Moje práce je koncipována do pěti kapitol. První kapitola se zabývá internetovým soukromím. Nejdříve definujeme tento pojem a poté představíme soukromí na internetu v digitální éře a také potencionální hrozby, kterým jsou uživatelé vystaveni. Rovněž se budeme zabývat spojením soukromí a technologií, mezi které patři GPS, mobilní telefony, *cloud computing* nebo šifrování dat. V kapitole druhé se budeme zabývat dějinami tajných služeb. V této kapitole jsou uvedeny důvody vzniku tajných služeb, jejich cíle, oblasti, kterými se zabývají. Dále jsou zde příklady tajných služeb napříč věky. Třetí kapitola pojednává o programu PRISM. Zde nejdříve definujeme pojem PRISM, poté se zaměříme na data, která jsou shromažďována prostřednictvím tohoto programu. Také

uvedeme společnosti, které spolupracují nebo spolupracovaly s programem PRISM. Dále uvedeme zákony, např. Vlastenecký zákon, které přinesly zvýšení určitých pravomocí zpravodajských agentur a vlády, částečný rozbor a kritiku. V kapitole čtvrté představíme aktéry zapojené do kauzy PRISM. Nejdříve uvedeme postavu Edwarda Snowdena, jehož čin názorově rozděluje společnost ve dví, kdy polovina společnosti má Snowdena za hrdinu a ta druhá za vlastizrádce. Uvedeme motivy, které vedly Snowdena k vynesení a zveřejnění tajných dokumentů. Poté navážeme, dalo by se říci, nejdůležitější aktérem, a to Národní bezpečnostní agenturou (NSA). Tato agentura je, co se týče získávání informací, pro Spojené státy americké nepostradatelná, ale v očích veřejnosti po celém světě vnímána spíše negativně. Rovněž představíme sledovací alianci *Five Eyes*, které je NSA součástí. Jako další uvedeme největší sociální síť současnosti – Facebook, která je díky množství uživatelských informací „pokladem“ pro tajné služby. V závěru této kapitoly představíme softwarového giganta, společnost Microsoft, která se jako vůbec první firma připojila k programu PRISM a rovněž firmy Apple a Google.

V praktické části se budeme zabývat dopady kauzy PRISM. Praktická část bude rozdělena na dvě části. Ta první se bude zabývat politickými důsledky, kde uvedeme reakci Obamovy administrativy a reformy NSA, které provedl Barack Obama. Dále uvedeme možné obavy spojené s prodloužením platnosti Vlasteneckého zákona, o kterém se bude hlasovat letos v červnu. V druhé části pak ukážeme dopady na jednání veřejnosti a veřejné mínění. Dále budeme zkoumat, jaké dopady měla kauza PRISM na internetové uživatele a na jejich soukromí.

V bakalářské práci jsem primárně vycházel z internetových zdrojů a to především proto, že téma PRISM je poměrně nové a tištěné literatury je zatím relativně malé množství. V teoretické části byl pro mne hlavním internetovým zdrojem *The Guardian*, který měl k dispozici dokumenty přímo od Edwarda Snowdena. V části o Edwardu Snowdenovi jsem primárně vycházel z knihy Glenna Greenwalda, který se osobně setkal se

Snowdenem v Hong Kongu, kde s ním dělal rozhovory. Dále jsem čerpal z odborných článků z online databáze EBSCO. V praktické části jsem vycházel především z průzkumů, které provedlo *Pew Research Center.*

2 INTERNETOVÉ SOUKROMÍ

Internetové soukromí je soukromí, úroveň bezpečnosti a osobních dat zveřejněných prostřednictvím internetu. Internetové soukromí, pro které se rovněž používá pojem online soukromí, je pojem, který se vztahuje k celé řadě faktorů, technických postupů a technologiím, které jsou používány k ochraně citlivých a soukromých dat, komunikace a preferencí (Janssen).

Internetové soukromí a anonymita jsou věci, které jsou pro uživatele internetu nejdůležitější, obzvláště v dnešní době, kdy se neustále rozvíjí online nakupování. Porušování soukromí a rizika jsou standardní kritéria, která nesmí brát žádný web na lehkou váhu (Janssen).

Dle Technopedie je internetové soukromí věc, o kterou se bojí každý uživatel internetu, ať už se jedná o online nakupování, sociální sítě, online hry nebo diskusní fóra. Pokud dojde k prozrazení a odhalení hesla, může být identita oběti podvodně zneužita nebo ukradena (Janssen).

2.1 Soukromí na internetu v digitální éře

Implementace přenosu mezi http klientem a serverem začala v roce 1990 a od té doby následoval prudký růst. Dle *Internet World Stats* z roku 2014 zaznamenal Internet od roku 1995 exponenciální růst. Ve zmíněném roce 1995 užívalo internet zhruba šestnáct milionů uživatelů (Chiru 2014: 141), v roce 2015 pak odhadem tři miliardy (Internet live stats). Internet mění naše zvyky a online aktivity jsou stále více a více přítomny v našich životech (Chiru 2014: 141).

Světová ekonomika, společně s globalizací, má nový aspekt „e“. V dnešní době tak existují e-platby, e-vláda, e-nákupy apod. Distribuční

systém a online prodeje se staly právě tím „e“ a moderní společnost si už neumí představit život bez těchto služeb (Chiru 2014: 141).

Prudký vývoj softwaru, hardwaru a technologií obecně umožnil použití v mnoha oblastech a službách, např. ve vzdělání, výzkumu, ekonomice, zdraví, obchodu, turismu, obraně apod. Byl vyvinut software pro online finanční transakce, online komerci, multimédia, knihovny a neustále se zlepšující online vyhledávače (Chiru 2014: 141).

2.1.1 Sociální sítě

Sociální sítě jako komunikační médium na internetu jsou online služby, které umožňují vytvoření vztahů mezi různými lidmi. Tyto vztahy jsou založeny na společných zájmech, aktivitách či sdílených myšlenkách. Zavedení takového systému do provozu vyžaduje webovou stránku, která poskytne uživatelům nástroje, pomocí kterých mohou organizovat své informace, nahrávat a stahovat soubory, chat, úložný prostor atd. (Chiru 2014: 142).

Ze všech sociálních sítí, které jsou dnes na internetu dostupné jako komunikační médium, převyšuje Facebook ostatní služby. Ať už se jedná o větší počet uživatelů nebo velké množství informací, které lidé dobrovolně zobrazují na stránkách Facebooku (Chiru 2014: 142).

2.2 Potencionální hrozby ohrožující internetové soukromí

Mezi bezpečnostní rizika, která ohrožují internetové soukromí, patří např. *Phishing*. *Phishing* je technika, která se používá ke zcizení soukromých uživatelských dat, včetně uživatelských jmen, hesel, čísel bankovních účtů, PIN kódů nebo čísla kreditních karet. *Phishing* se pokouší získat tato uživatelská data přesměrováním na podvodnou stránku, která se tváří jako ta oficiální (TechTerms).

Spyware je, jak název napovídá, software, který sleduje uživatelovo chování na jeho počítači. *Spyware* zachycuje informace o pohybu uživatele na webu, e-mailu, informace o uživatelských jménech, heslech, o kreditních kartách. Pokud nedojde k detekci *spywaru* v počítači, může dojít k zasílání těchto dat třetí straně. *Spyware* se do počítače může dostat např. otevřením e-mailové přílohy, která obsahuje škodlivý software (PC.net 2015).

2.2.1 Zadní vrátka v hardwaru a softwaru

Tzv. zadní vrátka, anglicky *Backdoor*, je v počítačovém systému zkratka k různým zdrojům. Může se jednat například o složky, hesla, práva. Použitím zadních vrátek získá neoprávněný uživatel přístup k datům v počítači bez klasického ověření (Chiru 2014: 146).

Lidé, kteří mají starost o svou počítačovou bezpečnost, se většinou omezují pouze na používání složitých hesel, instalaci antivirových programů, firewally apod. Většina z nich ale netuší, že existuje jednodušší cesta k jejich datům, která obchází všechny ověřovací mechanismy (Chiru 2014: 146).

Operační systém Windows, který je jedním z nejpoužívanějších operačních systémů (Nichols – Vaughan 2015), má zabudovány speciální přístupové kódy, které připravila NSA, a které byly tajně integrovány do všech systémů Windows s výjimkou verze 95 a jejich předchůdců (Campbell 1999). První odborník, který objevil možná zadní vrátka ve Windows, je dr. Nicko van Someren. Someren analyzoval ovladač ADVAPI a objevil dva klíče (Chiru 2014: 146). Jeden z nich sloužil k ovládání kryptografických funkcí ve Windows. Tento klíč úzce spolupracuje s aplikací Internet Explorer a šifruje pouze data, která mají být odeslána americké vládě (Campbell 1999). Druhý klíč zůstává tajemstvím (Chiru 2014: 146).

Další vědec ze Spojených států amerických, Andrew Fernandez, hlavní vědec ve společnosti Cryptonim, objevil a objasnil význam těchto dvou klíčů. Zkontroloval *Service Pack 5* pro Windows *NT4* a zjistil, že programátoři Microsoftu „zapomněli“ odstranit „ladící symboly“, které se používají k testování softwaru. Tyto dva klíče byly „KEY“ a „NSAKEY“. Fernandez prezentoval svá zjištění na konferenci Crypto 99, která se konala v Santa Barbaře. Programátoři Windows, kteří byli přítomni na konferenci, odmítli hovořit o významu těchto klíčů (Washingtons Blog 2013). Německý server *Zeit Online* získal od německého ministerstva hospodářství dokumenty, které ukazují, že německá vláda se obává, že technologie *Trusted Platform Module* (TPM), která je zabudována ve stále rostoucím počtu počítačových a mobilních verzích Windows 8, vytváří *backdoor* pro možné vzdálené sledování NSA (Beuth 2013).

2.3 Technologie a soukromí

V dnešní době většina lidí ve Spojených státech amerických a v dalších státech světa u sebe neustále nosí mobilní telefon, který používají na všechno. Na telefonování, posílání SMS a e-mailů, k pořizování fotografií, GPS, surfování na internetu nebo k hraní her. To vše v zásadě dělá z mobilního telefonu perfektní přístroj ke sledování a odposlouchávání. Vládní agentury v čele s NSA získávají data týkající se komunikace Američanů a jejich aktivit od poskytovatelů služeb a to vše dělají pod záštitou Vlasteneckého zákona a *Foreign Intelligence Surveillance Act* (Coats 2014).

Nejen, že zpravodajské služby shromažďují informace prostřednictvím mobilních společností, ale objevily se i případy, kdy může být telefon zpřístupněn útočníkovi prostřednictvím *spyware*. I když je telefon vypnut, stále může být zpřístupněn na dálku a použit k nahrávání konverzací nebo pořizování fotek. Tyto informace jsou pak zpřístupněny jakékoliv vládní agentuře. Se vzrůstajícím zájmem veřejnosti o běžně

nositelné technologie, jako jsou například chytré hodinky, další na řadě budou informace týkající se pohybu obyvatelstva (Coats 2014).

V zásadě dnes existuje několik hlavních zařízení, pomocí kterých vládní agentury získávají a shromažďují data o amerických občanech. Prvním je GPS, neboli *Global Positioning System*, který má dnes téměř každý telefon nebo automobil. GPS byl a je projekt financovaný vládou, pomocí kterého může sledovat pohyb osob v reálném čase. Dalším zařízením je veřejný kamerový systém. Ten se v posledních letech stává stále rozšířenějším a pozorovat ho můžeme nejen ve městech, sousedstvích nebo podél dálnic. Kamery jsou dalším opatřením, které bylo implementováno z důvodu zvýšení bezpečnosti obyvatel (Coats 2014).

Telefony jsou v podstatě „zařízení pro všeobecné shromažďování dat“. Prostřednictvím rozhovorů s vládními zdroji, které provedl bezpečnostní zpravodaj CNET Declan McCullagh, se zjistilo, že FBI (Federální úřad pro vyšetřování) tlačí na společnosti, jako jsou AT&T nebo Verizon, aby vybavily telefony svých zákazníků *port reader* softwarem, který by vládním agenturám umožnil zachytávat komunikaci v reálném čase. FBI se opět odvolává na Vlastenecký zákon (Coats 2014).

2.3.1 Cloud Computing

Cloud, je zjednodušeně řečeno, ukládání, zpracování a používání dat, která jsou vzdáleně přístupná přes internet (European Commission 2013). Slovo *cloud* je užito jako metafora pro internet, kdy *cloud computing* by se dalo vysvětlit jako „práce s počítačem přes internet“, kde různé služby, např. servery, uchovávání (dat) a programy jsou přes internet zpřístupněny uživatelům počítačů a dalších zařízení (Beal). Obvykle se jedná o sdílení počítačových dat v rámci agentur, poboček či

oddělení jednotlivých firem, ale rovněž se může jednat i o sdílení mezi třetími stranami. Díky *cloudu* mohou uživatelé naplnit své počítačové potřeby a mohou mít přístup ke svým datům odkudkoliv, kde je internetové připojení (European Commission 2013). Místo toho, aby si uživatel software koupil a instaloval na vlastní počítač, tak si vlastně pronajme online software. Díky *cloud computingu* mohou celé společnosti a stovky zaměstnanců používat pronajaté online počítačové nástroje. Všechny procesy a ukládání dat probíhá „*v cloudu*“, kam se můžou uživatelé každý den připojit, aby mohli pracovat (Gil).

Cloud computing zahrnuje tyto hlavní oblasti. Tou první je online ukládání dat, které již funguje několik let, ale až v dnešní době se začíná rozšiřovat. Způsobeno je to i cenou, kdy gigabyte v *cloudu* stojí méně než dolar. Google Docs, Microsoft Skydrive, Dropbox a stovky další jsou dnes známými službami, které zdarma nebo za symbolický poplatek nabízí online úložiště (Gil).

Software a Platforma jako služba popisuje obchodní model, kdy se uživatel přihlásí do centrální sítě, kde získá přístup k (např. firemnímu) softwaru. Uživatel k otevření vlastních souborů a softwaru musí být online a k přístupu musí použít příslušný webový prohlížeč a vlastní heslo (Gil).

2.3.2 Šifrování dat jako možná ochrana osobních dat

Když na to přijde, tak v dnešní době je prakticky nemožné utéct před potenciálním sledováním a znovu získat soukromí. Možné by to bylo snad jen v případě, že by jedinec přestal používat jakékoliv elektronické zařízení, čímž by se ve skutečnosti stáhnul ze společnosti (Coats 2014).

Nicméně však existuje celá škála šifrování a kryptologických služeb, které mohou zvýšit osobní soukromí. Různé společnosti poskytují zakódování e-mailových služeb, které jsou populární mezi aktivisty, žurnalisty a diplomaty. Avšak tyto společnosti jsou v ohrožení, stejně jako

služby typu Silent Circle nebo Lavabit, které byly pozastaveny nebo ukončeny na základě vládního příkazu (Coats 2014).

Lavabit poskytoval svým uživatelům e-mailové služby, které zahrnovaly velmi silné šifrování a jeho služby využíval i Edward Snowden. Zakladatel Ladar Levison tak učinil, aby ochránil data svých uživatelů. Lavabit byl projekt, který byl zastaven roku 2013 na základě příkazu americké vlády[1] (Ackerman 2013).

Stejný osud jako Lavabit postihl i program TrueCrypt. TrueCrypt je kryptografický software, který vznikl roku 2004 a byl šířen jako freeware, tedy zdarma. Tento software umožňuje vytvoření virtuálních disků, které jsou chráněny šifrováním AES, Serpent, Twofish apod. Jelikož je při vytváření virtuálního disku disk zaplněn náhodnými daty, je nemožné zjistit, kolik souborů se na disku nachází nebo zdali na něm nejsou skryté oddíly. Právě nemožnost rozeznat od sebe prázdný a TrueCryptový plný disk patří mezi jednu z nejsilnějších vlastností tohoto softwaru (Rybka 2014).

Ukončení vývoje a podpory TrueCryptu je přinejmenším podivné. I přes to, že byli autoři TrueCryptu anonymní, jejich nadace TrueCrypt Foundation sídlila v Nevadě, což znamená, že byla pod jurisdikcí Spojených států amerických. Nadace přijímala dary od uživatelů přes platební systém PayPal, díky kterému byli dohledatelní. Možnost „návštěvy“ např. z FBI je tedy velmi vysoká a i pravděpodobná. Stejně jako v případě Lavabitu, i zde autoři raději ukončili vývoj programu, než aby zradili svou původní myšlenku, se kterou celý projekt založili. Uvalení příkazu o mlčenlivosti (*gag order*) ve formě *National Security Letter* (NSL) by vysvětloval, proč se autoři nevyjádřili k celé kauze a na nově vytvořené

[1] Celé vyjádření autora programu Lavabit, Ladara Levisona, k dispozici na (http://lavabit.com/, 15. 4. 2015).

webové stránce TrueCryptu se objevily pouze zvláštní argumentace[2] (Rybka 2014).

Dosažení zašifrování veškeré komunikace nebo „vymazání se“ ze sítě není něco, čím by se většina Američanů měla zabývat. Pokud se někdo nebaví o vysoce citlivých materiálech, zájem vlády o práva jednotlivce je víceméně otázkou morálky. Přiznejme si, že většina z nás není pro výzvědné služby zajímavá (Coats 2014).

3 DĚJINY TAJNÝCH SLUŽEB

Dějiny tajných služeb prošly velmi dlouhým vývojem, nicméně základní politické principy a často i vojenské akce v rozvinutých antických státech a v současnosti se dají označit jako srovnatelné. Ať už se jedná o výplod fantazie nebo realitu, pocit vnitřního nebo vnějšího ohrožení, nedůvěra tvoří i nadále základní veličiny politické moci. Právě z těchto pocitů pramení potřeba sledovat potencionální nepřátele, zjistit včas jejich úmysly, schopnosti a plány. Poté na tyto podněty adekvátně reagovat (Krieger 2011: passim).

Již odedávna sloužily tajné služby jako nástroj ponížení a útlaku. Tento přístup se uplatňuje nejen v diktaturách, ale i v dějinách demokratických zemí. Dostupnost pramenů ke studiu novodobé historie 20. a 21. století je obtížnější, ale řada informací byla postupně zveřejněna. Lze nalézt informace k teroristickým útokům v USA z 11. září 2001 či k válce v Iráku z roku 2003. Ruský prezident Boris Jelcin umožnil, aby bylo uvolněno rozsáhlé množství spisů, jeho nástupci však v této politice otevřenosti nepokračují. Ostatní státy bývalého východního bloku částečně odhalily spisy státních služeb z období komunistické nadvlády. Spisy východoněmecké Státní bezpečnosti byly rovněž dány badatelům

[2] Na nynější oficiální stránce TrueCryptu můžeme v současné době najít pouze informace o tom, že byl projekt ukončen a není nadále bezpečné ho používat. Více na (http://truecrypt.sourceforge.net/, 15. 4. 2015).

k dispozici, nicméně poslední vedení STASI nejen zničilo část spisů, ale byla vydána i určitá omezení z důvodu ochrany osobních práv. Německá spolková zpravodajská služba a dokonce i Čínská republika rovněž zahájily zpřístupňování spisů k výzkumným účelům. Předsudek, že se nelze dějinami tajných služeb vědecky zabývat z důvodu neexistence veřejně přístupných pramenů, je již tedy překonán (Krieger 2011: 9-10).

Úroveň polního zvěda z doby Alexandra Makedonského samozřejmě nejde stavět na tu samou úroveň jako dnešní zpravodajské služby, které mají k dispozici moderní techniku, nicméně, základní principy, ať už politické, často dokonce i vojenské, jsou si často podobné. Oproti materiálnímu prostředí, které lidstvo po celou dobu obklopuje, se chování člověka změnilo pouze minimálně. Právě způsob agresivního chování a lidské vlastnosti, zejména ty špatné, mezi které se řadí prolhanost, nevěrnost, závist a nepřejícnost, vedou k násilí a válkám (Krieger 2011: 13).

Mezi hlavní činnosti tajných služeb patří následující oblasti. Tou první je získávání informací o nepřátelích i přátelích, ale třeba i konkurenci. Druhou oblastí je infiltrace do tajných služeb protivníka. Třetí činností, kterou tajná služba musí vykonávat, je vytvořit zabezpečení pro vlastní vládnoucí aparát proti útokům ze strany cizích tajných služeb. Poslední činností je pak skryté ovlivňování (Krieger 2011: 14).

3.1 Důvody vzniku tajných služeb ve starověkých dějinách

Všechny starověké říše Blízkého a Středního východu usilovaly o vytvoření univerzální říše. Udržení trvalé stability těchto mnohonárodnostní říší bylo možné pouze za předpokladu, že panovník měl k dispozici obsáhlé a včasné informace o potencionální možné hrozbě. Stručně řečeno, bez tajné služby není impéria (Krieger 2011: 19).

Královští poslové společně s úředníky a vojáky křižovali říši a kromě daní shromažďovali zprávy o vlastních obyvatelích říše, hraničních oblastech i sousedních národech. Pro sběr informací se proto pravděpodobně udržovaly styky s lodními kapitány, obchodníky a přepřahajícími stanicemi karavan. Dalším důležitým zdrojem vojenských informací byli i váleční zajatci, u kterých ovšem, stejně jako v dnešní době, bylo těžké zjistit skutečnou loajalitu (Krieger 2011: 24). Části dochovaných deníků, jež patřily královským poslům, ukazují, že právě poslové zaznamenávali veškeré důležité vládní dokumenty, kontakty nebo dopisy (Kriger 2011: 20).

3.2 Tajné služby v historii

Zajímavou postavou v historii byl mongolský panovník Čingischán, kterému se podařilo vládnout říši o rozloze 33 milionů kilometrů čtverečních, což je více jak trojnásobek plochy Spojených států amerických. Schopnost diplomacie a zejména pak preventivní práce zpravodajských služeb doplňovaly krutost a sílu. To vše stálo za mongolskými vítězstvími. Vláda nad takto nebývale rozsáhlou říší vyžadovala perfektní komunikační sítě a informační základnu, která shromažďovala zprávy o cizích národech a reagovala na nově vzniklé změny. Práce tajných služeb byla důležitou příčinou úspěchu mongolské expanze, k jejímuž přerušení došlo roku 1260 v Palestině (Krieger 2011: 44-45).

Dvůr Elizabeth I. byl úrodnou půdou pro intrikaření a špehování. Prací Francise Walsinghama bylo držet královnu o krok napřed před jejími odpůrci. V květnu 1582 se Walsinghamovi podařilo zachytit dopis napsaný španělským velvyslancem v Anglii, týkající se spiknutí k invazi do Anglie a uvedení do úřadu Mary, královny Skotska. Zatímco Mary byla zavřena v Chartley Manor, Walsingham přišel s nápadem, jak dokázat to, že je hrozbou pro královnu (Zurcher 2013).

Během Francouzské revoluce Maximilien Robespierre a jeho stoupenci bedlivě sledovali obyvatelstvo a nemilosrdně zakročili proti odporu. V roce 1793 revoluční vláda zřídila dvanáctičlennou sledovací komisi napříč zemí. Komise byla oprávněna identifikovat, sledovat a zatýkat jakéhokoliv podezřelého bývalého šlechtice, cizince, občana státu, který se v poslední době vrátil ze zahraničí apod. Historici odhadují, že více než půl milionu lidí bylo cílem sledovací komise, která byla nemilosrdná zejména v menších francouzských městech (Zurcher 2013).

V 18. a 19. století se vlády napříč Evropou ujaly sledování s byrokratickým nadšením. Zavedly oddělení nazvaná „černé komory“ (z francouzského *cabinet noir*), které sloužily ke čtení dopisů vybraného jedince. Úřad, který se obvykle nacházel v poštovní budově, využíval celou škálu technik k tajnému otevření, kopírování a znovu zapečetění korespondence, která poté byla poslána nic netušícímu příjemci. Praktika zapletla britskou vládu do skandálu v roce 1840, když došlo k odhalení, že londýnská černá komora tajně čte dopisy vyhoštěného italského autora a aktivisty Giusseppe Mazziniho. Velká část britské veřejnosti byla pobouřena tím, že jejich vláda předávala informace do Neapole, kde bylo těchto informací využito k popravě Mazziniho revolucionářů (Zurcher 2013).

Roku 1922 Spojené státy americké pořádaly ve Washingtonu námořní konferenci o odzbrojení, kde dohlížely na jednání mezi devíti národy, včetně Spojeného království, Francie, Itálie a Japonska. Rovněž tajně sledovaly japonské a další vyjednávací týmy. Docházelo k zachytávání komunikace mezi delegacemi a jejich domovskými zeměmi. Částečně i díky americkému šifrovacímu úřadu byly Spojené státy schopny úspěšně vyjednat několik nadnárodních smluv a dohod, které odřízly cestu námořnímu závodu ve zbrojení. Roku 1929 byl šifrovací úřad zavřen tajemníkem Henry Simsonem, který uvedl, že

džentlmeni si navzájem poštu nečtou. Nicméně po druhé světové válce se Američané rozhodli, že trvalou sledovací síť potřebují (Zurcher 2013).

Spojené státy americké vstoupily do sledovacího odvětví v brzkých letech po druhé světové válce. Začalo to projektem Shamrock, který zahrnoval shromažďování a sledování telegrafních informací, které přicházely a odcházely ze země. Rovněž byl vytvořen „watch list“, v tomto případě seznam cizinců, podezřelých z podvratné činnosti. Komunikace těchto cizinců byla sledována v rámci projektu Minaret. Tuto operaci převzala NSA, která spolupracovala s FBI a CIA. Oba programy byly ukončeny po vyšetřování americkým Kongresem v roce 1975. Třicet let poté NSA obnovila projekt Shamrock s využitím technologií informačního věku (Zurcher 2013).

Americkou zpravodajskou komunitu, tak jak ji známe dnes, oficiálně založil prezident Ronald Reagan v roce 1981. V roce 2012 se americká zpravodajská komunita skládala ze 17 agentur. Každá z nich pak operuje nezávisle na ostatních. Nicméně cíl mají všechny stejný – zlepšit národní a domácí bezpečnost. Mezi těch 17 agentur patří např. CIA, FBI nebo NSA (Chesbro).

Tyto agentury mají za cíl shromažďovat a analyzovat informace o zahraničních národech, identifikovat nepřátelské organizace, mezi které patří např. teroristické organizace. Rovněž musí sledovat možné hrozby, mezi které se řadí např. obchod s narkotiky (Chesbro).

Za železnou oponou studené války bylo sledování obyvatel nedílnou součástí každodenního života. Nikde to neplatilo tolik jako ve Východním Německu, kde skoro čtyřicet let zpravodajská služba STASI sledovala a informovala o aktivitách vlastních obyvatel. Tyto informace pak byly využívány k potlačování nepokojů. V době pádu Berlínské zdi, tedy roku 1989, se STASI rozrostla o více než devadesát jedna tisíc

úředníků a celková informační síť čítala skoro dvě stě tisíc informátorů. Východoněmecké sledování využívalo moderních technologií a obrovské pracovní síly a rozšířila vládní špehování do dříve nevídaných rozměrů (Zurcher 2013).

Krádeže dopisů, zachytávání komunikace nebo odposlechy úředníků jsou některé z příkladů špehování napříč věky (Zurcher 2013).

4 PRISM

PRISM (*Planning Tool for Resource Integration, Synchronization and Management*), v překladu znamená Nástroj pro plánování, integraci a řízení zdrojů (Murse). Tento program slouží jako nástroj pro shromažďování a zpracování dat. První detaily o programu PRISM zveřejnil britský deník *The Guardian* a americký *The Washington Post*. Oběma médiím dodal informace 29 letý Edward Snowden, který pracoval jako externí dodavatel pro Národní bezpečnostní agenturu (NSA) (Sottek – Kopstein 2013).

Program PRISM byl spuštěn v roce 2007, tehdy ještě pod administrativou bývalého amerického prezidenta George Walkera Bushe ml. Právě George Bush ml. podepsal v roce 2001 *USA Patriot Act* (česky Vlastenecký zákon), který novelizoval zákon z roku 1978, tzv. *The Foreign Intelligence Surveillance Act* of 1978 (FISA) a který byl reakcí na zářijové útoky. Program PRISM je zatím poslední produkt, který americká vláda používá ke kontrole elektronické komunikace po událostech z 11. 9. 2001 (Sottek – Kopstein 2013).

Další zákon, tzv. *The Protect America Act* z roku 2007, který nahradil *Terrorist Surveillance Act* z roku 2006, byl podepsán také prezidentem Georgem W. Bushem ml. Tento zákon vedl k vytvoření tajného programu pod vedením NSA. Vznikl program, který nesl označení US-984XN, rovněž nazývaný jako PRISM. Program byl označován jako

zefektivněná verze ve sledovacích praktikách, které Spojené státy používaly po 11. září (Sottek – Kopstein 2013).

The Protect America Act umožňuje generálnímu prokurátorovi a řediteli národní zpravodajské služby vyjádřit se v dokumentu, který podléhá utajení, jak budou každý rok Spojené státy získávat informace o cizincích v zámoří. Současně ovšem nevyžaduje, aby byla uvedena konkrétní místa či jména. Jakmile je v tajném řízení jednou návrh schválen federálním soudcem, může si NSA vyžádat data od společností, kterými jsou např. Google nebo Facebook. Tato data jsou pak předána vládě (Sottek – Kopstein 2013).

Cílem programu PRISM je sbírat informace z internetové a telefonní komunikace uživatelů, a to jak ve Spojených státech, tak jinde po světě. Jedná se o elektronická data uživatelů, kteří používají služby hlavních internetových firem, mezi které patří např. Gmail, Facebook, Outlook apod. (Sottek – Kopstein 2013).

Data, která NSA shromažďuje, se dají rozdělit do dvou kategorií. První skupinou jsou *upstream*[3] odposlechy, které stahují data přímo z podmořských telekomunikačních kabelů. Tou druhou jsou programy jako např. PRISM, které získávají data od amerických poskytovatelů služeb. Na snímku z uniklé prezentace (viz příloha č. 1) jsou analytici instruováni, aby využívali obou zdrojů. PRISM shromažďuje dva typy dat: metadata a obsah. Metadata jsou citlivý vedlejší produkt komunikace, kdy například metadata telefonních nahrávek prozrazují účastníky komunikace, časy a celkovou dobu trvání hovorů. Komunikace shromážděná programem PRISM zahrnuje obsah e-mailů, rozhovorů, VoIP hovorů, dat uložených v *cloudových* úložištích atd. Americké úřady

[3] *Upstream data* jsou data, která jsou odesílána z počítače nebo sítě (e-maily, zprávy nebo nahraná data) (Christensson 2010).

se pokoušely vyvrátit obavy ohledně bezhlavého sběru metadat zpravodajskou službou NSA tím, že poukazovaly na to, že tato metadata neobsahují obsah konverzací. Nicméně metadata mohou odhalit závažné informace, které obsahují např. e-mailové záznamy, data o poloze (IP adresy) nebo historii webového vyhledávání. Metadata ve Spojených státech jsou díky starým zákonům mnohem méně chráněná než obsah (Sottek – Kopstein 2013).

V prohlášení, které potvrzuje existenci programu PRISM, ředitel národní zpravodajské služby, James R. Clapper, prohlásil, že informace, které získávají pomocí programu PRISM, jsou těmi nejdůležitějšími a nejcennějšími zahraničními informacemi. Tyto informace jsou pak použity k ochraně vlastní národní bezpečnosti, která je ohrožována celou škálou hrozeb. Neoprávněné vyzrazení informací, které se týkají tohoto důležitého a zcela legálního programu, je trestuhodné. Vyzrazení těchto tajných informací může znamenat závažná rizika pro bezpečnost Američanů (Clapper 2013).

4.1 Vlastenecký zákon

USA Patriot Act[4] je americkým zákonem, který byl schválen krátce po teroristických událostech 11. září 2001. Hlavním cílem tohoto zákona je posílit vnitrostátní bezpečnost a rozšířit pravomoci agentur, které mají za úkol identifikovat a eliminovat teroristické hrozby. Přijetí a prodloužení zákona bylo neobyčejně kontroverzní. Zastánci tvrdí, že byl nespočetněkrát nápomocný při vyšetřování a zatýkání teroristů, zatímco kritici tvrdí, že zákon dává vládě až moc kompetencí, ohrožuje civilní svobody a podkopává právě tu demokracii, kterou usiluje chránit (Grabianowski 2007a).

[4] USA Patriot Act je zkratka pro *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism* (Investopedia).

Vlastenecký zákon je rozdělen do deseti částí, neboli hlav a týká se mnoha oblastí. Uvedeny jsou ty nejdůležitější.

Hlava jedna, která nese název Posílení domácí bezpečnosti proti terorismu, se zabývá ochranou civilních svobod. Součástí Hlavy jedna je i vytvoření separátního fondu pod názvem Protiteroristický fond, který je například využíván k podpoře obrany, vyšetřování a stíhání domácího nebo mezinárodního terorismu (The Library of Congress). Dále prezident získává pravomoc zkonfiskovat majetek kteréhokoliv cizince, který je podezřelý, že pomáhal ve válce nebo v útoku na Spojené státy. Tyto konfiskace mohou být tajně použity a předloženy soudu jako důkaz (Grabianowski 2007a).

Hlava dva, neboli Posílení procedur dozoru, rozšiřuje schopnost agentur provádět sledování zahraničních agentů. Je umožněno zachytávat komunikaci, pokud má co do činění s teroristickými aktivitami. Tyto agentury umožňují sdílet informace, které se týkají teroristických aktivit s federálními orgány. Kromě toho hlava dva povoluje „toulající se“ sledování, což je situace, kdy soud povolí sledování konkrétní osoby. Při tomto sledování je možné použít jakékoliv dostupné prostředky k zachycení komunikace dotyčné osoby bez ohledu na to, kam osoba jde. Dříve to bylo tak, že soud mohl povolit pouze odposlech telefonu na konkrétní lince a v konkrétním místě. Dále je vládě umožněno vyžádat si záznamy s detaily o tom, jak a jaké služby zákazník používá a to přímo od poskytovatele, který zprostředkovává komunikační službu. Například tak může být internetový poskytovatel vyzván, aby poskytl informace o IP adresách, časech přihlašování a stránkách, které dotyčný navštívil. Hlava dva také umožňuje opožděné oznámení o domovní prohlídce, což znamená, že dům podezřelého může být prohledán i v době, kdy podezřelý není přítomen. Rovněž podezřelý nebude upozorněn, že byla provedena domovní prohlídka (Grabianowski 2007a).

Hlava tři, Redukce mezinárodního „praní špinavých peněz“ a výnos proti financování terorismu z roku 2001, se zaměřuje na odříznutí finanční podpory teroristickým organizacím. Jsou zavedena opatření, která vyžadují od bank, aby podnikly kroky, které by byly prevencí před praním peněz. Současně povoluje agenturám, aby shromažďovaly informace od bank a vytváří delší tresty za praní špinavých peněz a pašování (Grabianowski 2007b).

Na Hlavě pět, neboli Odstranění překážek pro stíhání terorismu, je nejdůležitější použití *National Security Letters* (NSL). NSL je obsílka nejčastěji vystavená FBI a používá se v případě hledání „relevantních“ informací během oprávněného bezpečnostního vyšetřování, které slouží k ochraně před mezinárodním terorismem nebo ilegální zpravodajskou činností. Vlastenecký zákon posílil NSL a umožňuje jejich použití proti americkým občanům. NSL mohou obsahovat i tzv. *gag order*, neboli zákon o mlčenlivosti, který dotyčnému objektu zabraňuje, aby o tom mluvil s někým dalším. V případě vyžádání a použití není potřeba soudního přezkoumání ani udání příčiny (Electronic Frontier Foundation).

Hlava šest pojednává o poskytnutí finančních kompenzací obětem terorismu a jejich rodinám, Hlava sedm se zabývá oprávněním a sestavováním rozpočtu pro zvýšení sdílení informací mezi agenturami a jurisdikcí (Electronic Frontier Foundation). Hlava osm pak přidává několik trestných činů, které jsou považovány za teroristický čin. Mezi tyto činy například patří napadení hromadné dopravy, použití biologických zbraní, podpora terorismu a počítačového *hackingu*[5]. Tresty za teroristické činy rovněž vzrostly (Electronic Frontier Foundation). Hlava devět vytváří způsob, na základě kterého dojde ke sdílení informací mezi zpravodajskou službou a vládními agenturami. Do desáté hlavy jsou pak zařazeny další předpisy (Electronic Frontier Foundation).

[5] *Hacking*, neboli nabourávání se do počítačových systémů apod.

4.1.1 Vlastenecký zákon a jeho použití v boji proti terorismu

Od té doby, kdy byly zničeny budovy světového obchodního centra, bylo třeba začít myslet jinak a to, jak těmto útokům předcházet (Ridge 2004: 266).

Pod administrativou prezidenta Bushe došlo ke schválení Vlasteneckého zákona, který obsahuje mechanismy, pomocí kterých je možné předcházet budoucím útokům. Jedním z těchto mechanismů je sdílení informací, díky kterému mohly Spojené státy rychle získávat informace o možných teroristických útocích. Tyto informace jsou klíčové pro americké domácí zpravodajské agentury. Druhým nástrojem jsou pak vyšetřovací prostředky, které kdysi byly použity k dopadení hlav mafie a drogových bossů. Dnes jsou tyto nástroje používány zpravodajskými službami a dalšími bezpečnostními orgány v zemi i v zámoří k identifikaci, zadržení a zastavení teroristů ještě před tím, než uskuteční svoje plány (Ridge 2004: 266).

Tom Ridge, první ministr vnitřní bezpečnosti Spojených států amerických tvrdí, že lepší sdílení informací mezi agenturami je klíčovou částí nového myšlení, stejně tak prevence je nejvyšším cílem. Aby těchto cílů bylo dosaženo, je potřeba, kromě jiných věcí, i nových technologií a nových nástrojů. Rovněž jsou vyžadovány i komplexní operace zpravodajských služeb za účelem sběru informací (Ridge 2004: 266).

Když to vše dáme do kontextu, tak před 11. září často nemohly zpravodajské agentury a ostatní vyšetřovatelé mezi sebou sdílet informace. V mnoha případech nemohli ani pracovníci FBI sdílet informace mezi sebou uvnitř FBI i přes to, že pracovali na stejném případu. Schopnost bojovat s terorismem byla omezena neschopností zkoordinovat práci uvnitř. Vlastenecký zákon pomohl vše změnit a vybavil orgány vymáhající právo nástroji, kterých bylo potřeba k zahájení efektivní kampaně proti teroristům (Ridge 2004: 266).

Pracovníci zpravodajských služeb mohou nyní konzultovat s federálními agenty postup při řešení nebo ochraně proti hrozbám ze zahraničí. Tato spolupráce mezi zpravodajskými agenturami a orgány prosazujícími právo je nezbytná k ochraně národní bezpečnosti (Ridge 2004: 267).

Zvýšená schopnost sdílení informací přímo vedla k přerušení několika teroristických akcí a rovněž vedla k četným zatčením, trestním stíháním a odsouzením v případech terorismu. Příkladem může být *Lackawanna Six* na severu Buffala nebo *Portland Seven* v Oregonu. Obě tyto teroristické organizace byly zapleteny do případu, kdy obžalovaní odjeli do Afghánistánu nebo se o to pokusili, aby zde bojovali na straně Al-Kajdy proti Spojeným státům americkým (Ridge 2004: 267).

Vlastenecký zákon však neřeší pouze možné teroristické útoky, ale pomáhá chránit i americké rodiny. V Pensylvánii bylo roku 2002 nahlášeno zmizení třináctileté dívky. Byla vylákána z domu svých rodičů a poté, co byla unesena, byla držena v řetězech dva státy od domova. Unesl ji osmatřicetiletý muž, kterého poznala online. Díky sekci 212 Vlasteneckého zákona dokázali federální agenti v Pittsburghu získat důležité internetové důkazy, které pomohly lokalizovat pachatele a zachránit dívku. Muž byl shledán vinným a dostal dvacetiletý trest (Ridge 2004: 268).

Prezident Bush prohlásil, že skutečná síla země leží v srdcích a duších občanů. Tom Ridge mu dává za pravdu. Federální vláda nemůže zvládnout dohlédnout na kompletní ochranu Ameriky. Místo toho, státní bezpečnost se musí stát prioritou v každém městě, v každém sousedství, v každé domácnosti a u každého jedince (Ridge 2004: 268).

4.1.2 Kritika Vlasteneckého zákona

Vlastenecký zákon byl terčem kritiky a to hned z několika důvodů. Byl přijat velmi rychle (měsíc po útocích z 11. září) a Kongres jeho čtením a projednáváním strávil jen krátkou chvíli. Dle některých trvalo méně než 48 hodin mezi představením návrhu, jeho finální podobou a přijetím oběma komorami Kongresu. To vyneslo pochyby o tom, zdali většina členů Kongresu vůbec takto rozsáhlý návrh zákona četla. Jediným senátorem, který volil proti přijetí zákona, byl demokrat z Winconsinu, Russ Feingold (Grabianowski 2007c).

S přijetím Vlasteneckého zákona začaly panovat obavy, že odstraní mnoho občanských svobod, které Spojené státy garantovaly konstitucí. Právo na soukromí (není přímo zmíněno v ústavě, ale v mnoha kauzách podpořeno Nejvyšším soudem) a na svobodu naruší neodůvodněné prohlídky a zadržení, které vláda bude moci vykonávat, stejně jako provádět odposlechy a uplatňovat NSL. Dále například zadržování klíčových svědků a osob podezřelých z terorismu bez možnosti přístupu k právnímu zástupci, soudnímu slyšení nebo k jakékoli oficiální žalobě. Všechny tyto uvedené obavy jsou vnímány jako úpadek pátého a šestého dodatku, tedy práva na řádný právní a soudní proces (Grabianowski 2007c).

Kritici také obviňují Vlastenecký zákon z nespravedlivého rozšiřování pravomocí moci exekutivní, která s sebou nese narušení klíčových aspektů systému brzd a rovnovah. Nedostatek kontroly ze strany justice, uzavřená jednání a přísný zákon o mlčenlivosti jsou hlavními příčinami kritiky. Rovněž panují obavy, že zákon bude nevhodně používán proti neteroristickým zločincům. Zákon byl například použit k odstranění bezdomovců z vlakových nádraží, ke stíhání překupníků drog a k získání finančních informací o náhodných návštěvnících v Las Vegas (Grabianowski 2007c).

Když se podíváme na výsledky vnitřního auditu FBI, který byl vydán roku 2007, o kterém informoval např. *The Washington Post,* zjistíme, že od 2002 agentura zneužila NSL ve více než tisíci případech. Je však pravděpodobné, že toto číslo představuje pouze zlomek skutečného čísla. V drtivé většině odevzdávaly telefonní společnosti a internetoví poskytovatelé informace agentům bez příslušného oprávnění (Solomon 2007).

Jeffren Rosen, profesor práv na Washingtonské univerzitě, ve svém článku pro deník *New York Times* napsal, že již od počátku kritici z řad Demokratů a Republikánů varovali, že mimořádná sledovací práva by mohla být použita k vyšetřování politických neshod či k menším trestným činům, než ve vyšetřování terorismu. Např. roku 2007 se objevila rozsáhlá a vážná zneužití pravomocí FBI. Mnoho z případů FBI zahrnovalo lidi, u kterých nebylo zjištěno žádné spojení s terorismem. Co se týče dodatků k Vlasteneckému zákonu, tak např. roku 2011 navrhoval senátor Ron Wyden dodatek, který by omezil nejvíce kontroverzní část Vlasteneckého zákona, a to sekci 215, která vládě umožňuje zabavit všechny hmotné věci, ať už jde o e-maily, historii prohlížeče nebo záznamy z knihovny, to vše bez soudního povolení. Waydenův dodatek navrhoval, aby složky vymáhající právo musely prokázat, že zabavené záznamy byly spojeny s teroristickou činností. Naneštěstí prezident Obama, který podobný návrh podporoval, když byl ještě senátorem, podepsal další prodloužení Vlasteneckého zákona bez ohledu na návrhy dodatku. Podobný návrh přednesli i další demokratičtí senátoři, Dick Durbin a Patrick Leahy, kteří navrhovali omezení odposlechů jen na vyšetřování spojená s terorismem a větší soudní dohled (Rosen 2011).

Dá se tedy přijetí Vlasteneckého zákona brát jako úspěch nebo spíše jako selhání? Je to těžké, jako vše má i Vlastenecký zákon dvě strany, pozitivní a negativní. Jeho hlavní klad je určitě zvýšení bezpečnosti, které napomohlo k tomu, aby se již neopakoval žádný útok

podobný tomu z 11. září. Samozřejmě to má i co do činění se zvýšením bezpečnosti na letištích nebo se soustředěním se na konflikt na Blízkém východě (Grabianowski 2007d).

Ministerstvo spravedlnosti označilo za klíčové v boji proti terorismu použití „toulajícího se“ sledování a odposlechů, rozšíření oprávnění ke sledování, opožděná upozornění na domovní prohlídky a také integrované sdílení informací mezi agenturami. Konzervativní analytici dokonce tvrdí, že bylo přerušeno na patnáct teroristických akcí, právě díky pravomocem nabytých z Vlasteneckého zákona (Grabianowski 2007d).

Na druhou stranu může docházet k různému zneužití těchto pravomocí, následkem čehož může dojít ke křivému obvinění bez možnosti řádného soudního procesu apod. Dalším problémem, na který kritici upozorňují, je zásah do soukromí, i když se veřejně hovoří o tom, že se netýká běžných amerických občanů (Grabianowski 2007d). V roce 2004 byl Brandon Mayfield, právník v Portlandu, který konvertoval k Islámu, zatčen za údajné spojení s událostmi z 11. března, kdy došlo k madridským bombovým útokům, při nichž zemřelo 191 lidí. Mayfield byl držen po dobu dvou týdnů jako klíčový svědek. Propouštěn byl poté, co FBI přiznala, že jeho otisk prstu byl chybně zaměněn s tím, který byl odebrán na místě činu. FBI tento incident popsala jako ojedinělý. Nicméně vláda přiznala, že byl Mayfieldův dům, na základě zvláštního soudního rozkazu (za účelem zajištění informací), tajně prohledán. Americký odbor pro civilní práva tvrdí, že se jednalo o zneužití Vlasteneckého zákona, kdy vše bylo prováděno tak, jako by se jednalo o špionáž tajné služby, když ve skutečnosti agenti hledali důkazy, které chtěli využít k trestnímu stíhání osob. Mayfield podal žalobu na ministerstvo spravedlnosti za porušení jeho osobních svobod. Tvrdí, že byl podezřelý pouze proto, že je muslim (Abramson 2005).

4.2 *Protect America Act of 2007* a FISA

Od té doby, co byla přijata výchozí část *Foreign Intelligence Surveillance Act* (FISA), pokročila technologie o velký kus dopředu a učinila tak mnoho bodů zákona zastaralými. Původně zákon FISA povoloval sledování pouze zahraničních hovorů, které byly vysílány bezdrátově. Nicméně, od té doby je skoro 90 % mezinárodní komunikace primárně vedeno přes optické kabely, které nebyly zahrnuty v původním znění zákonu FISA. NSA došla k závěru, že je legální monitorovat a odposlouchávat zahraniční komunikaci, která prochází skrze vysílače, které se nachází na území Spojených států. V lednu 2007 Bushova administrativa odsouhlasila dozor instituce *Foreign Intelligence Surveillance Court* (FISC) nad odposlouchávacím programem. Zpočátku soud odposlechy nechal dále probíhat. V březnu však byla vznesena námitka v otázce legality odposlechů, v květnu bylo usneseno, že vláda musí pro odposlouchávání získat soudní povolení, kdykoliv se to týká pevné linky. Výsledkem toho bylo, že NSA byla nucena žádat *Foreign Intelligence Surveillance Court* o soudní příkaz, který jí umožnil monitorovat a odposlouchávat zahraniční komunikaci tak často, že došlo k nahromadění žádostí o povolení. Úředníci amerických zpravodajských služeb uváděli, že došlo až k 25 % úpadku zahraničních odposlechů. Tato prodlení, tzv. *intelligence gap*, která způsobil FISC, přiměla Bushovu administrativu lobbovat u Kongresu za přepracování FISA (OpenCongress).

Dle kanceláře ředitele Národní zpravodajské služby není PRISM utajeným programem na shromažďování a zpracování dat, ale jedná se o interní vládní počítačový systém, který slouží k usnadnění získávání zahraničních informací. Tato data získává vláda od poskytovatelů elektronických komunikačních služeb, to vše probíhá pod dohledem soudu, který jedná na základě sekce 702 *Foreign Intelligence*

Surveillance Act, který byl přijat roku 2007/08 (Office of the Director of National Intelligence 2013).

Podle sekce 702 zákonu FISA, nezískává vláda Spojených států data od amerických poskytovatelů elektronických služeb unilaterálně. Všechny tyto informace získává se souhlasem FISA soudu a s vědomím poskytovatele. To vše na základě písemného pokynu od generálního prokurátora a ředitele Národní zpravodajské služby (NSA) (Office of the Director of National Intelligence 2013).

Stručně řečeno, sekce 702 usnadňuje cílené získávání zahraničních informací, které se týkají cílů mimo území Spojených států, to vše pod dohledem soudu. Poskytovatelé komunikačních služeb jsou povinni, v souladu s tímto zákonem, poskytnout vládě informace, pokud si tak vyžádá (Office of the Director of National Intelligence 2013).

Vláda si ovšem nemůže vybrat za cíl, koho chce. Učinit tak může pouze v případě, že se jedná o „příslušně zdokumentovaný účel“, jako je např. prevence terorismu, prevence nepřátelské kybernetické činnosti nebo šíření jaderných zbraní. Nemůže rovněž cílit na osoby v zámoří bez opodstatněného účelu. Kromě toho, sekce 702 nemůže být použita k záměrnému zaměření se na občana Spojených států či jinou americkou osobu nebo úmyslně zaměřenou osobu, která pobývala či pobývá v USA (Office of the Director of National Intelligence 2013).

Kongres přijetím *Protect America Act* v roce 2007 a FISA dodatky v roce 2008 uložil soukromým společnostem dobrovolnou povinnost spolupracovat s americkým shromažďováním informací. Jako prvního partnera (viz příloha č. 2) si program PRISM vybral amerického giganta, společnost Microsoft, čímž začal šestiletý sběr dat, který každým dnem rostl. Tato spolupráce pomalu otevírala debaty na národní úrovni o dohledu a soukromí (Gellman – Poitras 2013).

Soudem schválený program se zaměřuje na zahraniční data z komunikací, které proudí přes americké servery. A to i tehdy, jedná-li se o komunikaci mezi zeměmi, které jsou obě v zámoří. Mezi roky 2004 a 2007 přesvědčili právníci Bushovy administrativy federální (FISA) soudce, aby dostal program na sledování novou podobu. Do té doby musela vláda dokázat, že oba, jak dotyčný objekt, tak „zařízení“, byly zapojeny do terorismu nebo špionáže (Gellman – Poitras 2013).

5 AKTÉŘI ZAPOJENÍ DO KAUZY PRISM

5.1 Edward Snowden

Edward Joseph Snowden se narodil roku 1983 v Elizabeth City, v Severní Karolíně, do rodiny, kde všichni pracovali pro federální vládu (ExpressVPN 2015). Když byl ještě dítě, celá rodina se přestěhovala do Marylandu, což je blízko hlavního sídla NSA (Ray 2014). V desáté třídě Snowden přerušil studium z důvodu mononukleózy. Místo toho, aby se vrátil a dokončil školu, začal navštěvovat technickou školu a začal se zabývat počítači, technologií, internetem (ExpressVPN 2015).

Po 11. září Snowden, stejně jako velké množství Američanů, značně změnil své politické názory. Stal se více patriotem (Greenwald 2014: 40). V roce 2003 Spojené státy americké vedly invazi do Iráku, což bylo pro Snowdena podnětem k tomu, aby přemýšlel o kariéře v armádě. „Chtěl jsem bojovat v Iráku, protože jsem jako lidská bytost cítil povinnost pomoci osvobodit irácký lid z útlaku“, říká Snowden (Harding 2014). Nicméně už po několika týdnech základního tréninku viděl, že se jedná spíše o zabíjení Arabů, než o osvobození (Greenwald 2014: 40).

Armáda nabízela to, co bylo pro Snowdena na první pohled velmi atraktivní, a to možnost stát se elitním vojákem i bez předchozích zkušeností. V roce 2004 se pak rozhodl narukovat (Harding 2014). Poté,

co si během pětiměsíčního výcviku speciálních jednotek zlomil obě dolní končetiny, byl nucen armádu opustit (ExpressVPN 2015).

Po odchodu z armády byl, co se války týče, zbaven iluzí, nicméně i nadále věřil v podstatu dobrých úmyslů vlády Spojených států amerických. Po vzoru dalších členů rodiny se rozhodl jít v jejich stopách, tedy pracovat pro federální vládu (Greenwald 2014: 40).

V roce 2005 začal pracovat jako ostraha v Centru pro pokročilé studium jazyků na univerzitě v Marylandu, která byla tajně spravována a používána NSA (Greenwald 2014: 41). Navzdory nedostatku vzdělání a zkušeností projevil Snowden nadání a talent v práci s počítači, na základě čehož byl v roce 2006 najat CIA (Ray 2014). Díky kombinaci inteligence a počítačových schopností rychle povýšil na technického experta CIA (Greenwald 2014: 41).

Snowden se stal v agentuře ceněným členem jejího IT týmu a značně převyšoval většinu svých starších kolegů, kteří měli vysokoškolské vzdělání. Snowden cítil, že našel přesně to pracovní prostředí, které ocení jeho dovednosti a kde nedostatek akademického vzdělání bude ignorován (Greenwald 2014: 41).

Roku 2006 se stal zaměstnancem CIA na celý úvazek, rok poté se dozvěděl o možnosti pracovat v zahraničí. Na základě velmi dobrých hodnocení od manažerů získal práci ve Švýcarsku (Greenwald 2014: 41). Tam pracoval v Ženevě jako bezpečnostní síťový technik s identitou diplomata (Ray 2014). Náplní jeho práce bylo spravovat bezpečnost sítě, kterou využívaly počítače CIA a dohlížet na bezpečnost počítačů amerických diplomatů (Harding 2014). Snowden ovšem popisuje, že náplní jeho práce bylo mnohem více než být pouze systémovým administrátorem. V té době byl považován za jednoho z největších expertů ve Švýcarsku, co se týče kybernetické bezpečnosti. Jako

počítačový expert měl přístup k mnoha tajným informacím, z nichž mnohé byly znepokojivé (Greenwald 2014: 41-42).

Právě v Ženevě začal Snowden chápat, že to, co jeho vláda opravdu dělá, se velmi liší od toho, co mu bylo zpočátku řečeno (Greenwald 2014: 42). Tyto události ho zbavily iluzí a uvědomil si, že je součástí něčeho, co přináší více škody než užitku (Harding 2014). S přijetím tohoto faktu se začal na věci dívat jinak (Greenwald 2014: 42).

Další věcí, která Snowdena frustrovala, byl postoj jeho nadřízených. Pokaždé, když se snažil upozornit na problémy spojené s počítačovou bezpečností nebo překračováním morálních mezí, byl rázně odmítnut. Téměř vždy mu bylo řečeno, že toto není jeho práce, nebo že nemá dostatečné informace k tomu, aby dělal závěry. Těmito postoji si mezi spolupracovníky vytvořil pověst někoho, kdo vzbuzuje příliš mnoho obav, což nebyla vlastnost, díky které by si získal přízeň nadřízených (Greenwald 2014: 42).

Na konci roku 2009 se rozhodl ze CIA odejít a začal pracovat pro společnost Dell a Booz Allen Hamilton. Během práce ve společnosti Dell byl pracovně umístěn do Japonska, kde pracoval jako subdodavatel pro NSA (Bio. 2015). V Japonsku již měl mnohem větší přístup k informacím o sledování a věci, které viděl, ho začaly velmi znepokojovat. „Mohl jsem sledovat v reálném čase *drony*, jak sledují lidi, které by mohly zabít. Mohli jste sledovat celé vesnice a dívat se, co kdo dělá. Viděl jsem, jak NSA sleduje aktivity lidí na internetu, které právě probíhaly. Uvědomil jsem si, jak americké schopnosti sledovat narušují lidské soukromí“ (Greenwald 2014: 43). Po odchodu ze CIA poprvé začal zvažovat možnost stát se informátorem a vyzradit tajemství, o kterých si myslel, že jsou přestupkem. Tajemství ovšem v tuto chvíli nevyzradil, protože doufal, že zvolení prezidenta Baracka Obamy do úřadu prezidenta alespoň částečně změní zneužívání moci. Po svém nástupu do úřadu Obama

přísahal změnit nepřiměřené zneužívání pravomocí národní bezpečnosti, která se k těmto pravomocem dostala po vyhlášení válce s terorismem (Greenwald 2014: 42-43).

Po nějakém čase se ovšem ukázalo, že Obama nejen pokračoval, ale v mnoha případech zneužívání pravomocí ještě do větší míry rozšířil. Snowden si uvědomil, že nemůže čekat na vůdce, který bude jednat jako první a který bude sloužit jako příklad pro ostatní (Greenwald – MacAskill – Poitras 2013). Současně měl obavy ze škod, které by způsobil prozrazením utajovaných dokumentů CIA. V případě, že by tyto informace prozradil, ohrozil by životy lidí, např. agenty v utajení, nebo informátory, ale v případě NSA by poškodil pouze nekorektní systém (Greenwald 2014: 43).

Dalším místem, kde Snowden pracoval (stále pro společnost Dell), byl ostrov Oahu – Hawai. Zde pracoval v kryptologickém centru NSA, které bylo jedním ze třinácti hlavních středisek zaměřených na špionáž zahraničních zájmů, zejména těch čínských (Harding 2014). Část roku 2012 strávil stahováním dokumentů, o kterých si myslel, že by o nich svět měl vědět. Část dokumentů nebyla určena pro širokou veřejnost, nýbrž pro novináře, aby byli schopni pochopit kontext. Na počátku roku 2013 si Snowden uvědomil, že mu chybí část dokumentů, kterou nebyl schopen získat prostřednictvím společnosti Dell. Získání těchto informací bylo možné, pouze pokud by získal jinou pozici, ve které by byl oficiálně přiřazen jako analytik infrastruktury. Tato pozice by mu umožnila přístup k prvotním informacím z archívu NSA (Greenwald 2014: 48).

Rovněž jako subdodavatel pracoval Snowden v roce 2013 pro firmu Booz Allen Hamilton. Během práce na Havaji byl Snowden stále více znepokojen tím, jak NSA sleduje obyčejné občany prostřednictvím jejich mobilního telefonu nebo Internetu (ExpressVPN 2015).

V květnu 2013 Snowden požádal o zdravotní dovolenou a odletěl do Hong Kongu, kde během následujících měsíců poskytl několik rozhovorů redaktorům z novin *The Guardian* (Ray 2014).

Aktuálně Snowden, který využívá tříletého azylu, který mu poskytlo Rusko, by byl rád, kdyby Švýcarsko vyhovělo jeho žádosti na azyl. Dle Snowdena je Švýcarsko správnou politickou volbou a to především kvůli neutralitě. Do této doby požádal Snowden o azyl již dvacet jedna států, žádný z nich ale jeho prosbu nevyslyšel. Snowden si myslí, že je to především díky zásahu administrativy prezidenta Obamy. I nadále pokračuje Snowden v práci se svými právníky na tom, aby mu byl zařízen spravedlivý soud, který mu americká justice není ochotna dopřát. Snowden dodává, „že jediné, co mu americká justice odvětila na jeho žádost na spravedlivý soud, bylo, že mě nepopraví, což není zrovna spravedlivý soud“ (Neuman 2015).

5.2 Národní bezpečnostní agentura

Národní bezpečnostní agentura je vysoce specializovaná a pro Spojené státy americké nepostradatelná zpravodajská agentura, která se zabývá vytvářením a lámáním tajných kódů, známých jako kryptologie. NSA podává informace ministerstvu obrany. Práce NSA je prováděna v tajnosti, ve jménu národní bezpečnosti. Této agentuře se často přezdívá „*No Such Agency*“. Národní bezpečnostní agentura shromažďuje informace pomocí sledování protivníků skrze telefonní rozhovory, e-maily a internet. Tato zpravodajská agentura má dva primární úkoly. Tím prvním je předcházet krádežím citlivých a tajných informací, týkajících se národní bezpečnosti Spojených států. Tím druhým je pak shromažďování, zpracovávání a šíření informací ze zahraničních signálů pro kontrarozvědku a pro podporu vojenských operací (Murse 2015).

Národní bezpečnostní agentura byla vytvořena roku 1952 prezidentem Harry Trumanem za účelem konsolidovat vládní schopnost šifrování a dešifrování (Risen 2006: 42). Základy agentury mají původ v práci amerických sil, které prováděly dešifrování německých a japonských kódů během druhé světové války. Tyto akce byly klíčové a stály za úspěchem Spojenců proti německým ponorkám v Severním Atlantiku a stejně tak za vítězstvím v bitvě o Midway v Tichém oceánu (Murse 2015).

Součástí agentury je i *Central Security Service*, založený roku 1972 za účelem podpory partnerství mezi NSA, kryptologickými prvky ozbrojených sil a *National Cryptologic School*. Hlavní středisko ve Fort Meade, Maryland, je největším zaměstnavatelem matematiků v zemi. Ředitel musí být vojenský důstojník (Infoplease).

Zpočátku zde bylo pouze několik právních omezení ohledně schopnosti NSA provádět elektronické sledování uvnitř Spojených států amerických. V roce 1978 Kongres schválil zákon, který vyžadoval, v případě vnitrostátních odposlechů za účelem národní bezpečnosti, povolení k domovní prohlídce. Toto povolení musel schválit tajný soud. Zákon FISA, společně s dalšími novými zákony a omezeními uvalenými na zpravodajskou agenturu, ukončily hlavní roli NSA ve vnitrostátních sledovacích operacích. Po zavedení těchto pravidel byla vnitrostátní role NSA z velké části omezena na specializované výzvědné služby, mezi které patřily odposlechy zahraničních ambasád a diplomatických misí ve Washingtonu, New Yorku a v dalších městech. Nicméně, všechny tyto operace stále vyžadovaly povolení (Risen 2006: 42).

Po 11. září vláda Spojených států amerických musela přijít na to, jak se nabourat do komunikační sítě Al-kajdy. John Yoo, právník ministerstva spravedlnosti, řekl, že zbraně i zákony NSA jsou produkty minulého století. Yoo dále argumentoval, že nelze říct, že některá

telefonní linka je vyhrazena Usamu bin Ládinovi, prostřednictvím které hovoří se svými poručíky. Dle něj je toto dobrý příklad toho, že existující zákony neplnily svou funkci, protože pod zákony, mezi které patří i FISA, musíte mít jméno někoho, musíte předpokládat, že ten někdo je terorista před tím, než získáte oprávnění. Musíte mít jméno, které zadáte do povolení k tomu, abyste mohli odposlouchávat telefon, ale jména lidí, kteří tyto hovory uskutečňují, nikdo nezná. Získání těchto informací z telefonních hovorů, e-mailů není pod FISA možné (Bamford 2009: 115).

Bamford ve své knize uvádí, že deset dní po útocích napsal Yoo interní sdělení, ve kterém tvrdí, že NSA by mohla použít elektronické sledovací techniky a vybavení, která jsou mnohem silnější a sofistikovanější než ty, které používají agentury vynucující zákon k zachytávání komunikace a sledování pohybu osob. To vše bez soudního povolení (Bamford 2009: 115).

Několik měsíců po útocích prezident Bush tajně povolil NSA, aby tajně odposlouchávala Američany a ostatní osoby uvnitř Spojených států. Tyto odposlechy měly vést k hledání důkazů o teroristické činnosti. Probíhaly bez soudně schváleného povolení, které je jinak nutné k vnitrostátní špionáži. Na základě tohoto povolení začala NSA monitorovat mezinárodní hovory, e-mailové zprávy stovek, možná tisíců lidí uvnitř Spojených států (Risen – Lichtblau 2005). Prezident ve svém sdělení oznámil, že povolil „specifické elektronické sledování“, které bude probíhat po „omezenou dobu“ a má sloužit k objevení a zmaření terorismu uvnitř Spojených států amerických (O’Harrow – Nakashima 2013: 753).

Agentura běžně operuje pod omezením, že nesmí sledovat a šířit informace o amerických občanech a to ani v případě, že se nachází v zámoří. Krátce po 11. září začal program, který agentura nazývá „mimořádné shromažďování informací“. Program nabral na rychlosti na

začátku roku 2002 poté, co CIA začala v zámoří zatýkat představitele Al-kajdy. CIA zajistila teroristické počítače, mobilní telefony a telefonní adresáře. Úmyslem NSA bylo plně využít těchto čísel a adres tak rychle, jak jen to bylo možné. Vedle odposlechů těchto telefonních čísel a čtení e-mailů Al-kajdy, začala NSA monitorovat ostatní, kteří jsou na ni napojeni. Začal tak vznikat rozšiřující se řetěz kontaktů. Většina čísel a adres byla ze zámoří, nicméně stovky z nich pocházely z USA (Risen – Lichtblau 2005).

Několik dnů po teroristických útocích nabídly telefonní společnosti přístup NSA k vnitrostátním hovorům. K tomu nabídly i vlastní metodu pro analýzu hovorů. Zpočátku NSA tuto nabídku přijmout nemohla, protože neměla soudní povolení ke sběru domácích dat. To se změnilo poté, co George Bush ml. odsouhlasil tzv. Prezidentský sledovací program (PSP). NSA okamžitě začala rozvíjet několik soukromých partnerství, do kterých bylo zahrnuto několik telefonních společností, internetových poskytovatelů služeb a společnostní poskytující webové služby. Na základě těchto partnerství začali soukromí partneři v říjnu 2001 posílat NSA telefonní a internetový obsah (O'Harrow – Nakashima 2013: 713).

5.2.1 Která data NSA sbírá?

Boundless informant program byl prvním důkazem toho, že NSA počítá všechny telefonní hovory a e-maily z celého světa s matematickou přesností. Snowdenovy dokumenty ukazují, že se jednalo o miliardy hovorů a e-mailů a rovněž ukazují, že Keith Alexander, bývalý ředitel NSA, a další představitelé opakovaně lhali Kongresu o tom, že nejsou schopni poskytnout přesná čísla. Jak ukazuje snímek (viz příloha č. 3), tak od března 2013 po dobu jednoho měsíce bylo shromážděno více než tři miliardy telefonních hovorů a e-mailů, které prošly americkým komunikačním systémem. To převyšuje sběr informací z Ruska, Mexika

a prakticky všech zemí v Evropě. Pouze množství dat shromážděných v Číně bylo zhruba stejné (Greenwald 2014: 92).

Navzdory tomu, že se NSA ze zákona má soustředit na informace ze zahraničí, Snowdenovy dokumenty ukazují a potvrzují, že americká veřejnost byla stejně důležitým cílem. To nejlépe ukázala kauza Verizon, kdy Snowdenovy dokumenty dokazují, že poprvé pod administrativou Baracka Obamy byly ve velkém shromažďovány záznamy komunikace milionů amerických občanů a to bez ohledu na to, zda byli podezřelí nebo ne (Greenwald 2013).

Mezi programy vytvořené za účelem sběru dat patří kromě PRISM (který zahrnuje shromažďování dat přímo ze serverů největších světových internetových společností) i *Project Bullrun*. *Project Bullrun* je společnou snahou NSA a britské *GCHQ* zničit nejpoužívanější formy šifrování, které se používá např. při bankovních transakcích. Program NSA *Bullrun* byl pojmenován po důležité bitvě v americké občanské válce, zatímco britský *Edgehill* nese jméno po bitvě v anglické občanské válce. Dle dokumentů, které poskytl Edward Snowden, se *Bullrun* zaměřuje na zničení šifrování používané v určitých síťových komunikačních technologiích. Naproti tomu se *Edgehill* zaměřuje na rozšifrování čtyř největších internetových komunikačních společností: Hotmail, Google, Yahoo a Facebook (Neal 2013a). Dalším programem je pak EGOTISTICAL GIRAFFE, který se zaměřoval na webový prohlížeč Tor a jeho uživatele. Tor poskytoval nástroje, které umožňovaly anonymní surfování (Greenwald 2014: 94). Kanadský program OLYMPIA za podpory Spojených států tajně sledoval brazilské ministerstvo energií. Shromážděná data pak byla sdílena mezinárodní špionážní sítí *Five Eyes* (RT 2013).

Některé ze sledovacích programů se údajně věnovaly cílům podezřelým z terorismu, ale velké množství z nich zcela zjevně nemělo

nic společného s otázkou národní bezpečnosti. Dokumenty nenechávají na pochybách, že NSA byla zároveň zapojena i do ekonomické a diplomatické špionáže, stejně tak do sledování celé populace. Celkově vzato, informace ze Snowdenových dokumentů vedou k velmi jednoduchému závěru. Americká vláda vytvořila systém, jehož cílem je kompletní eliminace celosvětového elektronického soukromí. Dalo by se říci, že je to snaha o „policejní stát“, kdy stát shromažďuje, ukládá, sleduje a analyzuje veškerou elektronickou komunikaci všech lidí napříč světem (Greenwald 2014: 94).

5.2.2 NSA a Aliance *Five Eyes*

Aliance *Five Eyes* je tajné globální sledovací společenství, které je složeno z tajných služeb pěti zemí. Mezi tyto země patří USA (NSA), Velká Británie (GCHQ), Kanada (CSEC), Austrálie (ASD) a Nový Zéland (GCSB) (Privacy International). Alianci *Five Eyes* původně tvořily pouze dva státy – Velká Británie a Spojené státy americké. Spolupráce započala ke konci druhé světové války a cílem bylo sdílet informace. Austrálie, Kanada a Nový Zéland se připojily v roce 1955. Těchto pět anglicky mluvících zemí vytvořilo několik bilaterálních dohod, které jsou známy pod názvem dohody „UKUSA“ (Tucker 2015).

Aliance vznikla za účelem sdílení informací (*SIGINT*). Přes sedmdesát let tato tajná aliance buduje globální sledovací infrastrukturu k „řízení internetu“ a k tajnému sledování světové komunikace (Privacy International).

I přesto, že je tato organizace sedmdesát let stará, je o ní a dohodách mezi státy velmi málo známo. Ve skutečnosti např. australský předseda vlády údajně nebyl o existenci této aliance informován až do roku 1973 a žádná z vlád oficiálně nepřiznala dohodu až do roku 1999. Z toho, co je veřejnosti známo, dochází v souladu se

smlouvou k získávání, shromažďování, analýze a dešifrování informací a to každým státem v jeho vlastní části světa. Tyto informace jsou pak automaticky sdíleny s ostatními členy aliance (Privacy International).

Skupina těchto států byla např. zapojena do příprav CIA na svržení chilského prezidenta Salvadora Allendeho. Od útoků z 11. září schopnosti *Five Eyes* značně vzrostly a skupina začala tajně sledovat všechny od světových vůdců až po studentské účty na Facebooku. Státy, které nejsou členy *Five Eyes*, mohou být cílem i přes to, že jsou spojenci (Tucker 2015).

5.3 Korporace zapojené do kauzy PRISM

5.3.1 Facebook a sběr informací

Jak bylo již zmíněno, Facebook se stal největší sociální sítí s téměř miliardou a půl registrovaných uživatelů (viz příloha č. 4). Mezi těmito uživateli je také mnoho organizací, společností a firem (Statista 2015).

Nicméně existuje mnoho názorů, které tvrdí, že je Facebook nástrojem pro shromažďování a sledování (Chiru 2014: 145). Ve své studii z roku 2006 Alessandro Acquisti a Ralph Gross došli k závěru, že většina uživatelů Facebooku nemá strach o bezpečnost svých osobních informací. Ze studie například vyplynulo, že téměř 77 % respondentů uvedlo, že nečetlo zásady ochrany osobních údajů (skutečné číslo je ale pravděpodobně vyšší) nebo že 56 % respondentů věří, že Facebook nesdílí informace o uživatelích s třetími stranami (Acquisti – Gross 2006: 13).

Dle Marka Zuckerberga vzestup sociálních sítí znamená, že lidé již dále neočekávají vysokou míru soukromí. Zakladatel Facebooku dále prohlásil, že soukromí již nadále není sociální normou a lidé si zvykli sdílet informace otevřeněji a s více lidmi (Johnson 2010).

Nicméně Facebook je organizace, která funguje v současné kapitalistické společnosti, kde je jasně dáno, jak vydělávat. Profitu je dosaženo prostřednictvím reklam, které jsou cíleny na uživatele Facebooku. Zásady ochrany osobních údajů jsou na této sociální síti velmi komplikované a předpokládá se, že jen pár jedinců je dočetlo až do konce. Nicméně, po důkladném přečtení těchto zásad a podmínek si uvědomíme, že Facebook shromažďuje značné množství osobních dat o svých uživatelích, které následně prodává inzerentům. Facebook má tak dvě tváře. Ta jedna ujišťuje uživatele, že jejich osobní data jsou v bezpečí, zatímco ta druhá tato data shromažďuje a prodává reklamním společnostem (Chiru 2014: 145).

Andrew Brown ve svém článku *Facebook is not your friend* tvrdí, že uživatelé Facebooku nejsou klienti, ale produkty Facebooku. Brown přímo píše „zákazníci jsou inzerenti, kterým Facebook prodává informace, které předali uživatelé, ať už s jejich vědomím nebo ne“ (Brown 2010).

5.3.2 Microsoft a sběr dat

Deník *The Guardian* zveřejnil informace o blízké spolupráci mezi společností Microsoft a americkými zpravodajskými službami. Microsoft umožnil agenturám zachytávat komunikaci uživatelů a rovněž pomohl NSA obcházet vlastní šifrování (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Dokumenty, které poskytl Edward Snowden, ukazují rozsah spolupráce mezi Silicon Valley a zpravodajskými agenturami za poslední tři roky. Dokumenty ukazují, že Microsoft pomohl NSA obcházet vlastní šifrování a umožnil tak zachytávání komunikace na novém portálu Outlook.com. Dále měla agentura přístup k e-mailům, a to jak na Outlook.com, tak na Hotmail.com (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Microsoft též spolupracoval s FBI, což mělo za následek usnadnění přístupu, skrze program PRISM, k vlastnímu *cloudovému* úložišti SkyDrive (dnes OneDrive), který celosvětově používá něco kolem 250 milionů uživatelů (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

V červnu minulého roku, devět měsíců po tom, co Microsoft koupil Skype, se NSA pochlubila novou schopností, díky které dokáže ztrojnásobit množství video hovorů skrze Skype, v rámci programu PRISM. Materiály shromážděné prostřednictvím programu PRISM jsou běžně sdíleny s FBI a CIA. NSA program PRISM v tomto případě označuje jako „kolektivní sport“ (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Poslední odhalení ukazují nárůst napětí mezi Silicon Valley a Obamovou administrativou. Všechny velké firmy lobbují, aby jim vláda umožnila prozradit kompletní míru jejich spolupráce s NSA, která se týká soukromí uživatelů (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Ve svém prohlášení Microsoft uvedl, že v případě vylepšení nebo aktualizování produktů není (Microsoft) zproštěn povinnosti dodržet existující nebo budoucí požadavky dané zákonem. Společnost také zopakovala svůj výrok, že uživatelská data poskytuje pouze v reakci na vládní požadavky. Microsoft vždy poskytne pouze data, která se týkají specifických účtů (Microsoft News Center 2013).

Celoplošné rozkazy od tajného dozorčího soudu umožňují shromažďování informací z komunikačních prostředků bez soudního povolení v případě, že pracovník NSA má 51 % jistotu, že cílem není americký občan, který se momentálně nachází na americké půdě. Aby se terčem sledování mohl stát americký občan, je již nutné mít soudní

povolení. Ale NSA je schopna shromažďovat americkou komunikaci i bez soudního povolení v případě, že cílem je cizinec, který se nachází v zámoří (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Od doby, kdy se existence programu PRISM dostala na veřejnost, Microsoft a všechny další velké společnosti, které se objevily jako dodavatelé na seznamu v dokumentech NSA, popřely, že by si byly vědomy existence programu a trvaly na tom, že zpravodajské služby nemají *backdoor* v jejich systémech (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Předloňská dubnová kampaň Microsoftu pak zdůrazňovala oddanost k soukromí uživatelů se sloganem *Your privacy is our priority*[6]*.* Současně zásady ochrany osobních údajů společnosti Skype uvádí, že Skype respektuje soukromí uživatelů a důvěrnost osobních dat, odeslaných dat a obsahu komunikací (Skype/Microsoft 2014).

Dokumenty ukazují, že NSA začalo zajímat zachytávání šifrovaných rozhovorů již od okamžiku, kdy Microsoft začal testovat portál Outlook.com. Testování této služby začalo v červnu 2012. Během pěti měsíců, jak ukazují dokumenty, přišel Microsoft a FBI na řešení, které umožňovalo NSA obcházet šifrování komunikace na Outlook.com. Během testování se řešení ukázalo jako úspěšné a začalo se používat od prosince 2012. O dva měsíce později pak Microsoft oficiálně spustil službu Outlook.com (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Microsoft se ve spolupráci neomezil pouze na Outlook.com. Záznam z 8. dubna 2013 popisuje, jak společnost „po mnoho měsíců“ spolupracovala s FBI, která fungovala jako prostředník mezi zpravodajskými službami a Silicon Valley v rámci programu PRISM.

[6] Kampaň lze najít na oficiální stránce Microsoftu: (http://www.microsoft.com/security/online-privacy/overview.aspx, 15. 4. 2015).

Tato spolupráce se týkala *cloudové* služby SkyDrive a umožnila programu PRISM přístup bez zvláštní autorizace. Dokument dále popisuje, že analytici již nebudou muset speciálně žádat divizi NSA *Special Source Operations* (SSO). NSA vysvětluje, že nová schopnost se projeví v mnohem kompletnější a rychlejší odezvě při shromažďování dat. Dále NSA uvádí, že tento úspěch je výsledkem mnohaměsíční spolupráce mezi Microsoftem a FBI (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Během posledních dvou let NSA věnovala značné úsilí spolupráci s Microsoftem zejména kvůli zajištění většího přístupu ke Skypu, jehož uživatelská základna se odhaduje na 663 milionů celosvětových uživatelů (Greenwald 2014: 113).

Jeden z dokumentů ukazuje, že pod projektem PRISM se sledování video přenosů přes Skype ztrojnásobilo od doby, kdy byla tato možnost přidána. Před červnem 2012 bylo možné zpracovat zvukové části bez možnosti doprovodného videa. Nyní mají analytici možnost mít kompletní audio i video (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Skype se připojil ke spolupráci s programem PRISM v únoru 2011, tedy osm měsíců před tím, než Skype koupila společnost Microsoft. Dle dokumentů NSA však postupná práce na integraci Skypu do programu PRISM začala již v listopadu 2010, samotné shromažďování dat začalo 6. února 2011. V dokumentu se můžeme dočíst, že zpětná vazba ukázala, že shromážděné Skype hovory byly velmi čisté a *metadata* vypadala kompletní. Stejně tak byla pochválena spolupráce mezi týmy NSA a FBI, která byla klíčová k přidání dalšího poskytovatele s programu PRISM (Greenwald – MacAskill – Poitras – Ackerman – Rushe 2013).

Taylor Soper ve svém článku pro *Geekwire* cituje technologického experta ALCU, Chrise Soghoiana, který prohlásil, že „pokud uživatelé nechtějí, aby stát odposlouchával jejich komunikaci, tak se obávám, že jim program Skype nemůžu doporučit“ (Soghoian cit. dle Sopera 2015).

5.3.3 Google, Apple a vyšetřování *The Wall Street Journal* ve světě digitálního soukromí

Chytré telefony společnosti Apple a Google pravidelně vysílají svou polohu zpět svým tvůrcům, respektive, dle dat a dokumentů analyzovaných deníkem *The Wall Street Journal*, se zvyšují obavy nad soukromím a nad rozšiřováním obchodu s osobními daty (Angwin – Valentino-DeVries 2011).

Apple a Google shromažďují informace o poloze v rámci jejich snahy vytvořit rozsáhlé databáze, které budou schopné velmi přesně určit polohu lidí skrze jejich telefon. Tyto databáze by jim mohly pomoci využít 2.9 miliardového trhu se službami zaměřujícími se na určení polohy (Angwin – Valentino-DeVries 2011).

V případě Google, dle výzkumu bezpečnostního analytika Samy Kamkara, shromažďují telefony HTC se systémem Android informace o vlastní poloze každých několik sekund a tato data posílají zpět do Googlu několikrát do hodiny. Data obsahují jméno, polohu, sílu signálu blízkých wifi sítí, stejně jako jedinečný identifikátor telefonu (Angwin – Valentino-DeVries 2011).

Existují způsoby, jak mohou uživatelé blokovat přenos udávání polohy na svém Android zařízení, stejně tak na zařízení iPhone. Nicméně, pokud tak uživatel učiní, omezí tím některé důležité funkce, mezi které například patří mapy (Angwin – Valentino-DeVries 2011).

Jennifer Valentino z *The Wall Street Journal* vysvětluje, že do minulého roku shromažďoval Google podobná data pomocí StreetView automobilů, za pomocí kterých mapoval a fotografoval ulice po celém světě. Společnost vypnula StreetView wifi sbírku minulý rok, poté, co neúmyslně shromažďovala e-maily, adresy, hesla a další osobní informace z wifi sítí. Data, která byla odesílána prostřednictvím zařízení se systémem Android a která pan Kamkar sledoval, neobsahovala žádné osobní informace (Angwin – Valentino-DeVries 2011).

Apple se pak stal terčem kritiky poté, co výzkumníci zjistili, že iPhone skladuje nešifrované databáze obsahující informace o umístění, které byly staré i několik měsíců. *The Washington Street Journal* dále zjistil, že některé z nejpopulárnějších aplikací pro chytré telefony používají údaje o poloze a další osobní informace sofistikovaněji a v některých případech tato data sdílejí se společnostmi třetí strany bez souhlasu nebo vědomí uživatele (Angwin – Valentino-DeVries 2011).

Rozšíření shromažďování informací o poloze je v poslední době ve velkém rozmachu. Do této doby byla většina dat o chování lidí shromažďována z osobních počítačů. Tato data jsou všeobecně spojena s městem nebo poštovním směrovacím číslem, takže bližší určení je komplikovanější. Vzestup mobilních telefonů s internetem umožňuje shromažďování dat s mnohem větší precizností, co se týče bližšího určení polohy. S touto novou formou sledování vyvstává otázka od vlády a soukromých advokátů. Ve svém dopisu se poslanec Markey táže společnosti Apple, proč se údaje o poloze uživatelů ukládají a uchovávají v telefonu (Angwin – Valentino-DeVries 2011). Ve svém dopisu Markey píše, že Apple potřebuje zabezpečit informace týkající se polohy uživatele a měl by se ujistit, že se z iPhonu nestane iTrack (Reardon 2011).

Google již dříve prohlásil, že data z wifi sítí, která sbírá, jsou anonymní a jsou mazány informace o začátku a konci trasy každé cesty

v případě využití cestovních map. Nicméně, data, která exkluzivně deníku *The Wall Street Journal* poskytl Kamkar, obsahovala jedinečný identifikátor, který je spjatý s individuálním telefonem (Angwin – Valentino-DeVries 2011).

Kamkar má ovšem za sebou kontroverzní minulost. V roce 2005, když mu bylo devatenáct let, vytvořil počítačový vir, který způsobil pád portálu MySpace. Vrchní soud v Los Angeles ho shledal vinným za hackerství a Kamkar souhlasil, že tři roky nebude používat počítač. Od roku 2008 dělá nezávislé bezpečnostní výzkumy a konzultace. Před čtyřmi lety vyvinul sledovací soubor tzv. *evercookie*, aby tak poukázal na zranitelnost webových prohlížečů (Angwin – Valentino-DeVries 2011).

Dle Kamkarova posudku jsou data o poloze odesílána bez ohledu na to, jestli aplikace běží. Stejně tak jsou tato data vázána na unikátní identifikátor telefonu (Angwin – Valentino-DeVries 2011).

Deník *The Wall Street Journal* najal nezávislého konzultanta, Ashkana Soltaniho, aby přezkoumal Kamkarovy závěry ohledně zařízení se systémem Android a sledování polohy. Soltani potvrdil Kamkarovy závěry (Angwin – Valentino-DeVries 2011).

Přenosy dat s polohou uživatelů s sebou nesou otázku, kdo má přístup k citlivým informacím o poloze a pohybu uživatele telefonu. Mluvčí Úřadu komisaře pro ochranu a soukromí v Kanadě sdělila své obavy ohledně užívání mobilních telefonů ke sběru wifi dat společností Google. Podle ní celá záležitost kolem schopnosti sledování mobilních telefonů vyvolává vážné otázky ohledně ochrany osobních údajů (Angwin – Valentino-DeVries 2011).

6 PRAKTICKÁ ČÁST

V této části práce se zaměříme na některé reformy, které navrhoval reformní výbor a porovnáme je se změnami, které provedl prezident Obama. Vzhledem k tomu, že 1. června vyprší platnost Vlasteneckého zákona, představíme možné problémy a obavy panující v případě, že by nedošlo k jeho prodloužení, zejména jeho problematických částí. Dále se budeme zabývat dopady kauzy PRISM na veřejnost a její mínění. Zde ukážeme výsledky celosvětového průzkumu, průzkumu mezi občany Spojených států a porovnáme postoje ke sledování mezi americkými a evropskými obyvateli. Poté představíme dopad kauzy PRISM na *cloudové* služby a alternativní prohlížeče.

6.1 Politické důsledky kauzy PRISM v USA

6.1.1 Reakce Obamovy administrativy

Podle Úřadu ředitele národní zpravodajské služby americké zpravodajské služby omezí využívání shromážděných informací o cizincích, a to včetně podkladů, které nejsou relevantní pro národní bezpečnost. Nová opatření jsou reakcí Obamovy administrativy na vlnu odporu proti špehování NSA, která se zvedla po zveřejnění dokumentů Edwardem Snowdenem (Strohm 2015).

Americké zpravodajské služby aktualizovaly jejich současnou politiku pro sběr a zadržování dat o Američanech a cizincích, která získávaly prostřednictvím elektronického sledování. Data o cizincích budou od nynějška mazána v průběhu pěti let, pokud ředitel národní zpravodajské služby neschválí prodloužení této lhůty (Strohm 2015).

Asistentka prezidenta pro národní bezpečnost a boj s terorismem Lisa Monaco v prohlášení uvedla, že jak Spojené státy i nadále čelí hrozbám z terorismu a kybernetickým útokům, tak musí použít schopnosti

zpravodajských služeb způsobem, který optimálně ochrání národní bezpečnost a podpoří zahraniční politiku a zároveň, který udrží důvěru veřejnosti a bude respektovat soukromí a občanské svobody (Strohm 2015).

Díky změnám v politice tajných služeb bude mít nyní Národní bezpečnostní rada větší dohled nad shromažďováním zahraničních informací za účelem řešení možných nebezpečí, která by mohla ohrozit národní zájmy, vynucení práva a diplomatické vztahy v zahraničí. Zpravodajská služba NSA vylepšila zpracování informací, aby zajistila, že jsou sledované cíle pravidelně přezkoumávány a v případě, že již neposkytují cenné informace, budou ze systému vymazány (Strohm 2015).

6.1.2 Obamovy reformy NSA

Prezident Obama oznámil velké změny vládního sledovacího programu, stejně tak slíbil přidat nové pojistky, které poslouží k ochraně amerického soukromí. Vytvořena rovněž budou nová omezení na používání a shromažďování informací zpravodajskou agenturou NSA, která se budou týkat obyčejných občanů.

6.1.2.1 Reforma shromažďování velkého objemu telefonních nahrávek

Bílý dům slíbil, že ukončí současný program a přesune telefonní nahrávky mimo přímý vládní dosah. Nezávislý revizní výbor doporučoval buďto dotazování telefonních společností, aby uchovávaly informace, nebo aby je vložily do rukou soukromé třetí strany. Obě tyto možnosti představují riziko týkající se soukromí, nicméně by to znamenalo ústup od centralizované sbírky. Obama provedl přímé změny programu, kdy si analytici od teď mohou vyžádat nahrávky pouze se souhlasem FISA

soudu a mohou vyhledat v limitu dvou čísel, namísto tří (Verge Staff 2014).

6.1.2.2 Konec zneužívání NSL

NSL jsou tajné vládní rozkazy, které přinucují společnosti jako Google a Facebook, aby předávaly informace o uživatelích do rukou FBI, aniž by to uživatelé tušili. Prezident prohlásil, že nařídil generálnímu prokurátorovi Ericu Holderovi poodhalit tajemství, která dopisy obklopují, aby uživatelé, kterých se to týká, byli informováni a společnosti aby mohly poskytnout více informací veřejnosti. Nicméně objem dopisů se nezmenšuje a FBI se snaží, aby NSL zůstaly lehce použitelné. Ale můžeme zde vidět značné reformy *gag orders* (Verge Staff 2014).

6.1.2.3 Vytvoření externího dohledu nad NSA

Kontrolní komise navrhovala kontrolní mechanismy, které by byly soustředěny v exekutivní moci, přidáním nového úřadu, který by jmenoval prezident a který by byl pod přísnějším dohledem prezidentského štábu. Obamova nařízení toto celé ignorují a dávají přednost soudnímu dohledu. V mnoha ohledech je toto lepší řešení, které nabízí důslednější kontrolu z odlišných úřadů vlády. Stejně tak je pravda, že justice je na tyto případy lépe připravena (Verge Staff 2014).

6.1.2.4 Zastavení oslabování šifrovacích standardů

Pro kryptografické nadšence a zastánce civilních svobod byl toto hlavní bod a důkaz toho, že americká vláda oslabovala nezbytné nástroje online soukromí. Naneštěstí se prezident Obama tohoto tématu ještě nedotknul, možná právě proto, že předpokládá, že většina Američanů se zajímá více o své telefony než o HTTPS. Prezident rovněž neudělal žádné kroky k oddělení NSA od americké *Cyber Command* ani se

nedotknul stavu NSA, která je v současné době vládním šifrovacím orgánem (Verge Staff 2014).

6.1.2.5 Ukončení špehování zahraničních vůdců

Neshody mezi Obamovou administrativou a ostatními zeměmi byly vyvolány Snowdenovými dokumenty, které ukázaly, že Spojené státy americké prováděly špionáž nejméně třiceti pěti zahraničních vůdců a to včetně osobního telefonu německé kancléřky Angely Merkelové a brazilské prezidentky Dilmy Rousseffové (Strohm 2015). Prezident jasně prohlásil, že nařídil zpravodajským službám, aby se vyhnuly sledování hlav spřátelených států. I přes to, že neexistuje žádný konkrétní program, který by zamezil tomu, aby se tento incident znovu opakoval, prezident požádal ministra zahraničí Johna Kerryho, aby jmenoval nového představitele do funkce koordinátora mezinárodních vztahů, který bude mít na starost řešení stížností ohledně jejich mezinárodního sledování zahraničních lídrů a hodnostářů (Verge Staff 2014).

6.1.3 Znovuobnovení Vlasteneckého zákona

K 1. červnu 2015 má vypršet platnost Vlasteneckého zákona. Přesněji jeho tří problematických částí: sekce 215, dále tzv. ustanovení *Lone Wolf* a „toulajících se“ odposlechů. Všechny tyto části jsou znepokojující, nicméně Sekce 215 nejvíce. Právě tato sekce opravňuje NSA, společně s FBI, k tomu, aby shromažďovala telefonní hovory milionů nevinných lidí. Dle Nadii Kayyali neexistuje lepší chvíle na reformu NSA, než je teď, protože hlas pro prodloužení zákona bez komplexní reformy NSA by byl jednoznačně hlasem proti Ústavě (Kayyali 2015).

Za poslední rok a půl proběhlo velké množství legislativních snah na reformu NSA, nicméně žádná z nich nebyla úspěšná. Jako poslední byla prosincová snaha Senátu, který se neúspěšně snažil předložit USA

FREEDOM Act (Svobodný zákon) k finálnímu hlasování. Jedním z těch, kteří byli proti, byl i senátor Rand Paul, který namítl, že zákon prodlužuje platnost sekce 215 o další dva roky. Paul byl kritikem Vlasteneckého zákona a špehování NSA a jasně vyjádřil své stanovisko hlasovat proti prodloužení zákona. Otázkou zůstává, jestli budou on a další kritici z řad Republikánů schopni protlačit skutečnou reformu (Kayyali 2015).

Zde by mohl nastat problém. Hlasování o Svobodném zákonu bylo ukázkou toho, jakou protireformní rétoriku můžeme očekávat v následujících měsících. Někteří zastánci občanských svobod si myslí, že zákon nebude dostatečně reformní, naproti tomu zákonodárci, kteří hlasovali proti, si myslí, že je až dostatečně inovující. Mitch McConnell na půdě Senátu prohlásil, že nyní není vhodná doba na to, aby se projednávala legislativa, která by odebrala přesně ten nástroj, který nyní Spojené státy potřebují v boji proti IS (Islámskému státu). Senátor Marco Rubio si myslí, že by platnost Sekce 215 neměla nikdy vypršet. Tvrdí, že svět je nebezpečným místem a že přijetí této legislativy by značně oslabilo Spojené státy a v některých případech by ukončilo nejdůležitější protiteroristickou schopnost, kterou mají Spojené státy k dispozici. Z těch důvodů bude hlasovat proti (Kayyali 2015).

Prezident Obama vyzval Kongres, aby schválil program, který ukončí hromadný sběr telefonních dat, ale který ponechá některé sledovací pravomoci netknuté a to z důvodu národní bezpečnosti. Pokud Kongres neobnoví zákon, nebude Obamova administrativa pokračovat v programu i přes to, že by mohla tato absence ohrozit americkou národní bezpečnost. Ned Price, mluvčí Národní bezpečnostní rady, tvrdí, že to, že skončí platnost Sekce 215, by mohlo mít za následek ohrožení bezpečnostního nástroje, který je využíván v celé řadě dalších událostí, které nejsou součástí hromadného sběru dat (Risen 2015).

Nicméně, dle Harleyho Geigera, nejvyššího právního zástupce Centra pro podporu demokracie a technologie, NSA může uplatnit další legální pravomoci, které jí umožní pokračovat ve shromažďovacích programech i bez Sekce 215 Vlasteneckého zákona. A to například prostřednictvím Sekce 214, která umožňuje využít tzv. *pen register/trap and trace devices*[7]. *Pen register/trap and trace devices* nemají dobu platnosti, tudíž by neměly být ovlivněny platností Sekce 215. Geiger tvrdí, že z těchto důvodů by byl zákon, který by ukončil hromadné shromažďování dat, daleko efektivnější, než pouhé ukončení platnosti Sekce 215. Proto věří, že Kongres by měl ukončit platnost Sekce 215, pokud není možná její efektivnější reforma (Risen 2015).

6.2 Dopady na veřejnost a veřejné mínění

6.2.1 Dopady na digitální soukromí

V dnešní době, kdy se digitalizuje čím dál více aspektů našich životů a přesouváme většinu věcí do *cloudu*, je spojena i velká pravděpodobnost, že vše, co děláme, může být sledováno (Smith 2013).

S tím, jak se stává šifrování obsahu čím dál tím častější a jeho popularita roste, roste i otázka, jak budou reagovat Spojené státy. Zdá se, že potřebou vlády Spojených států je mít přístup k šifrovanému obsahu, pokročilému zabezpečení a šifrovacím protokolům. Jak roste počet mobilních zařízení (chytré telefony, tablety apod.) a aplikací dostupných veřejnosti, stalo se šifrování jednodušším víc než kdy předtím. A co více, použití VPN umožňuje zašifrovat veškerá data a neponechat tak nic náhodě ve snaze uchovat si soukromí a anonymitu. Je zřejmé, že se vláda a NSA obávají šifrování a jeho použití zločinci, kteří by tak mohli jednat v utajení, aniž by si toho někdo všimnul (Paganini 2015).

[7] *Pen register/trap and trace devices*, jsou zařízení, která umožňují zachytávání informací o odesilateli a příjemci komunikace (Electronic Privacy Information Center 2005).

6.2.1.1 Celosvětový průzkum

Data, která Tom Smith poskytl *GlobalWebIndex,* ukazují, že více než 88 % internetových uživatelů užívá nějakou formu sociální sítě. Díky technologiím, které učinily přispívání a publikování na sociálních sítích jednodušším, se úplné soukromí stane pouhým pojmem v historii. Graf ukazuje (viz příloha č. 5) dvě rozdílné věkové skupiny. První, ve které se nachází lidé v rozmezí 16 – 24 let a druhá, kde jsou lidé mezi 55 – 64 lety. Nebylo překvapením, že 70 % v první skupině je ochotno publikovat fotky, 33 % rádo publikuje vlastní konverzace s přáteli a rodinou, 26 % je ochotno zveřejnit své telefonní číslo a 20 % poskytne svou historii nákupu. To je zřejmý rozdíl, protože ve druhé, starší skupině je ochotno publikovat osobní fotku pouze 32 % (Smith 2013).

Průzkum, který provedlo Centrum pro mezinárodní správu a inovace mezi uživateli ve 24 zemích ukázal, že 60 % internetových uživatelů slyšelo o Edwardu Snowdenovi a 39 % z nich podniklo kroky za účelem ochrany soukromí a bezpečnosti. Z průzkumu dále vyplynulo, že 73 % uživatelů chce mít svá online data a osobní informace fyzicky uložena na bezpečném serveru. Dále pak 72 % uživatelů chtějí mít svá online data a osobní informace fyzicky uložena na bezpečném serveru, který se nachází v jejich zemi (CIGI).

6.2.1.2 Průzkum mezi Američany

V dalším průzkumu se *Pew Research Center* ptalo dospělých Američanů, co si myslí o sledovacích programech a jestli tyto programy a odhalení s nimi spojená změnily jejich zvyky v komunikaci a online aktivitách (Rainie – Madden 2015).

Celkově téměř devět z deseti dotázaných odpovědělo, že zaslechli alespoň něco málo o vládních sledovacích programech. 31 % pak řeklo, že slyšeli hodně o vládních sledovacích programech a dalších 56 %

odpovědělo, že zaslechli pouze málo. Pouze šest procent řeklo, že o vládním sledování neslyšelo vůbec nic. Těm 87 %, kteří odpověděli, že zaslechli alespoň něco, byly dále položeny otázky týkající se jejich chování a soukromí (Rainie – Madden 2015).

Dále 34 % dotazovaných, kteří jsou si vědomi sledovacích programů (30 % všech dospělých), podniklo alespoň jeden krok ke skrytí nebo ochránění informací před vládou. Například 17 % z nich si změnilo nastavení soukromí na sociálních sítích, 15 % začalo používat sociální sítě méně, 15 % se vyhýbá užívání určitých aplikací, 14 % komunikuje více osobně místo komunikace prostřednictvím internetu nebo telefonu, dalších 13 % se pak vyvarovalo používání určitých výrazů v online komunikaci (Rainie – Madden 2015).

25 % těch, kteří jsou si vědomi sledovacích programů (22 % všech dospělých), tvrdí, že po Snowdenových odhaleních změnili své zvyky v používání různých technologických platforem. Například 17 % změnilo způsob, jakým používá vyhledávač. Dále značný podíl Američanů podnikl určitý krok ke zlepšení kontroly nad vlastním soukromím a bezpečím, i když většina udělala pouze jednoduché věci, kdy například 25 % si změnilo heslo na více složité (Rainie – Madden 2015).

Jedním z možných důvodů, proč lidé nezměnili své chování, je to, že 54 % z nich věří, že je „trochu“ nebo „velmi“ těžké najít správné nástroje, které by jim pomohly mít více soukromí, ať už online nebo při používání telefonu. Nicméně, značná část občanů prohlásila, že si neosvojili nebo nezvážili použití některých z běžně dostupných nástrojů, které jsou používány k tomu, aby udělaly online komunikaci a aktivity více soukromé. Když budeme konkrétnější, tak například 53 % si neosvojilo nebo nezvážilo používání vyhledávače, který by nesledoval uživatelovu aktivitu a historii hledání, 13 % pak vůbec netuší, že tyto nástroje existují. Dále 46 % si neosvojilo nebo nezvážilo použití e-mailových šifrovacích

programů, mezi které patří *Pretty Good Privacy* (PGP) a dalších 31 % o těchto programech neví. Průzkum dále ukázal, že 43 % si neosvojilo nebo nezvážilo použití přídavných zásuvných modulů (v prohlížeči), které zvyšují bezpečnost a soukromí. Sem patří zásuvné moduly typu *DoNotTrackMe* (dnes známé jako *Blur*) nebo *Privacy Badger,* dalších 31 % pak netuší, že takovéto moduly existují. Proxy servery, které pomáhají vyhnout se sledování, si neosvojilo nebo nezvážilo používání 41 % dotázaných, dalších 33 % o této možnosti neví (Rainie – Madden 2015).

Na otázku, zdali se na základě vývoje situace v médiích (ohledně vládních sledovacích programů v uplynulých měsících) stali spíše více nebo naopak méně přesvědčeni o tom, že programy slouží veřejným zájmům, odpovědělo 61 % negativně, tedy, že jsou méně přesvědčeni o tom, že tyto programy slouží v zájmu veřejnosti. Naproti tomu 37 % je více přesvědčeno o tom, že programy slouží v zájmu veřejnosti (Rainie – Madden 2015).

Americká veřejnost považuje sledování ostatních, včetně zahraničních občanů, zahraničních lídrů a amerických lídrů, za akceptovatelné. Výzkum *Pew Research Center* ukázal, že 82 % Američanů souhlasí se sledováním komunikace osob podezřelých z terorismu, dalších 60 % věří, že je přípustné sledovat komunikaci amerických lídrů, 60 % si myslí, že je v pořádku sledovat komunikaci zahraničních lídrů a 54 % zastává názor, že je přijatelné sledovat komunikaci zahraničních občanů. Nicméně 57 % tvrdí, že je neakceptovatelné, aby vláda sledovala komunikaci amerických občanů. Současně většina podporuje sledování konkrétních jedinců, kteří používají slova jako „výbušniny“ a „automatické zbraně“ v internetových vyhledávačích (to tvrdí 65 %) a ty, kteří navštěvují antiamerické stránky (to schvaluje 67 %) (Rainie – Madden 2015).

Když dojde na obavy ohledně sledování, jsou Američané rozděleni do dvou táborů. Celkově 52 % popisuje sebe jako „velmi znepokojené“ nebo „poněkud znepokojené“ ohledně vládního sledování dat elektronické komunikace amerických občanů. V porovnání s tím 46 % sebe, co se sledování týče, popisují jako „ne tak znepokojené“ nebo „vůbec neznepokojené“. 39 % dotázaných popisuje sebe jako „velmi znepokojené“ nebo „poněkud znepokojené“ co se týče sledování jejich aktivity při používání vyhledávačů. 38 % tvrdí, že jsou „velmi znepokojeni“ nebo „poněkud znepokojeni“ ohledně vládního sledování jejich e-mailových aktivit. 37 % vyjádřilo obavy týkající se sledování jejich mobilního telefonu. Dalších 31 % se pak obává vládního sledování jejich uživatelských aktivit na sociálních sítích (Facebook nebo Twitter) (Rainie – Madden 2015).

Průzkum mezi Američany, který provedl Will McCormick pro *Business Wire,* ukázal, že nejvíce se Američané bojí v oblastech online soukromí, které by mohly později způsobit finanční újmy. Nicméně se méně obávají možné osobní ostudy. Průzkum ukázal, že téměř tři ze čtyř Američanů (71%) se více obávají o své online soukromí, když přistupují na svůj bankovní účet nebo ke svým finančním údajům. Více než polovina (57%) pak jako druhé největší nebezpečí považuje online nakupování (viz Příloha č. 6) (McCormick 2014).

6.2.2 Porovnání postojů ke sledování mezi Evropany a Američany

Odhalení, které přinesly dokumenty získané Edwardem Snowdenem o špionáži NSA, odkryly jak rozdíly, tak podobnosti v přístupu veřejnosti ohledně soukromí mezi Evropany a Američany. Ředitel světových ekonomických postojů v *Pew Research Center*, Bruce Stokes, došel prostřednictvím průzkumů k závěru, že obě veřejnosti si cení soukromí, ale oproti Evropanům jsou Američané ochotni obětovat

své soukromí ve jménu národní bezpečnosti. Američané mají protichůdné názory ohledně aktivit, které NSA koná. Naznačují tím, že NSA zašla příliš daleko ve špionáži amerických spojenců. Dále jsou toho názoru, že NSA narušuje soukromí amerických občanů sběrem obrovského množství soukromých hovorů a e-mailů. Nicméně většina by vyměnila své soukromí za větší bezpečnost, které souvisí s honbou za terorismem (Stokes 2013).

Evropané si nemyslí, že národní bezpečnost opravňuje k narušení soukromí. Většina obyvatel Německa (70 %), Francie (52 %) a Švédska (52 %) si myslí, že jejich vlastní vláda nemá oprávnění ke shromažďování telefonních a internetových dat o občanech. A to ani v případě, jedná-li se o snahu ochránit národní bezpečnost. 44 % lidí ve Velké Británii s tím souhlasí (Stokes 2013).

Dalším rozdílem mezi Evropou a Spojenými státy je postoj ohledně špehování spojenců. Veřejnost na obou stranách Atlantiku si myslí, že národní bezpečnost není dostatečným důvodem k akci, ale je to sentiment, který silněji zastávají spíše někteří Evropané nežli Američané. Většina Němců (72 %) a více než polovina Francouzů a Švédů (oba 55 %) si myslí, že vlády nejsou oprávněny shromažďovat telefonní a internetová data občanů spojeneckých národů a to ani v případě, jedná-li se o otázku národní bezpečnosti. Dále průzkum TNS/GMF ukázal, že 43 % Britů toto považuje za neoprávněné (Stokes 2013).

6.2.3 Dopady na veřejnost

6.2.3.1 Alternativní vyhledávače

Poté, co se kauza PRISM a ostatní sledovací programy dostaly na veřejnost, vzrostla popularita alternativních internetových služeb. *IBTimes* uvádějí, že vyhledávač *DuckDuckGo* zaznamenal po kauze PRISM až tři miliony vyhledávání denně. Nicméně *DuckDuckGo* není jediným

vyhledávačem, který se dostal do popředí. Další dva soukromé vyhledávací *enginy StartPage* a *Inxquick*, které oba vlastní nizozemská společnost, zaznamenaly rovněž nárůst uživatelů. Jejich denní provoz vzrostl z 2.8 milionu vyhledávání na 4.2 milionu a tato stále čísla rostou. Stejně jako *DuckDuckGo*, ani *StartPage* nebo *Ixquick* neukládá IP adresy, nesleduje, co uživatel vyhledává nebo nepoužívá *cookies*. *StartPage*
a *Ixquick* navíc ještě poskytuje uživateli možnost vyhledávat s využitím proxy. Výsledky hledání jsou pak nahrávány skrze vlastní servery, což zabraňuje vytvoření přímého kontaktu mezi uživatelem a webovou stránkou. Dokonce ani internetový poskytovatel neví, co uživatel vyhledává. S tím, že se servery *StartPage* a *Ixquick* nenacházejí na půdě Spojených států, souvisí to, že nejsou součástí žádného sledovacího programu, což znamená, že se jich netýkají NSL nebo FISA soud (Neal 2013b).

Dle Dannyho Sullivana se ovšem moc nezměnilo. Dle něj většina lidí tvrdí, že nechce být sledována, nicméně pokud se podíváte na to, jak vyhledávají, tak nikdo z nich se nesnaží, aby jejich vyhledávání bylo bezpečnější a soukromější. Když pak porovnáme čísla, tak Google vyhledá třináct miliard dotazů denně, oproti tomu jsou 3 miliony (90 milionů měsíčně), které vygeneruje *DuckDuckGo,* opravdu zanedbatelné (Sullivan 2013).

6.2.3.2 Dopady kauzy PRISM na *cloudové* služby

Kauza PRISM rozvířila diskuze ohledně *cloudových* služeb. Poté, co se veřejnost dozvěděla o sledování, začaly pokládat organizace i jedinci otázky *cloudovým* poskytovatelům, jak mohou zlepšit bezpečnost jejich dat. Mezi další obavy pak patří např. fyzická lokace, tedy místo, kde jsou data uložena. Uchovávání dat v data centrech v zemi, kde je mohou autority sledovat nebo k nim mít přístup, znamenají značný risk pro

podnikání. Politici v Evropě se přidávají. Evropská komise prohlásila, že strach ze sledování, který vyvstal po odhalení kauzy PRISM, nesmí zastavit podniky v tom, aby se vzdaly výhod, které *cloud* poskytuje. Nicméně na škody, které kauza PRISM napáchala, reagoval např. německý internetový gigant *Deutsche Telekom*, který oznámil urychlení plánů, které mají za cíl udržet veškerá internetová data uvnitř Německa (Padilla 2014).

S odhalením kauzy PRISM vyjádřili členové Řídícího výboru obavy ohledně vlivu kauzy PRISM na přijetí *cloud computingu* v Evropě a volali po náležitých opatřeních. Obecně vyvstaly dva problémy. Tím prvním je neochota v použití *cloud computingu* mezi evropskými občany, firmami a veřejnou administrativou. Uživatelé již měli nějaké výhrady k bezpečnosti a důvěrnosti informací v *cloudu* a kauza PRISM tomu jen přitížila (European Commission 2013).

Za druhé, odhalení spojená s kauzou PRISM vedla po národních či regionálních *cloudových* iniciativách. Nicméně takováto fragmentace nebo segmentace *cloud computingového* trhu podle národní či regionální linie by naneštěstí bránila rozvoji *cloudu* v Evropě. Právě národní nebo regionální opatření platí pro většinu národních vlád, s tím souvisí fakt, že zákony zabraňují přenosům specifickým dat (především se jedná o data z veřejného sektoru) mimo hranice, a to dokonce i uvnitř Evropské unie. Každopádně, iniciativy na národní úrovni v případě softwarových systémů neumožní uvedení na trh v takovém měřítku, které by zpřístupnilo všechny výhody cloud-computingu. Větší trh zvýší konkurenci a cenu peněz, zatímco dojde k redukci nákladů. Taktéž by rozvoj *cloud computingu* otevřel nové možnost pro evropské *cloudové* poskytovatele (European Commission 2013).

Evropa, která není lídrem, co se týče poskytování *cloudových* služeb, je známá vysokými standardy zabezpečení dat, bezpečností,

vzájemnou spoluprací napříč platformami, transparentností a úrovněmi služeb a vládním přístupem k informacím. To vše jsou dobré základy pro pozdější rozvoj *cloud computingu* v Evropě (European Commission 2013).

Zpráva, kterou zveřejnil *The Information Technology & Innovation Foundation* (ITIF), ukázala, že vnitrostátní sledování může stát počítačové společnosti ve Spojených státech, zabývající se *cloudem,* částku mezi 22 až 35 miliardami dolarů během příštích tří let. Je to výsledek, za kterým stojí program PRISM a který bude i nadále růst s tím, jak si zahraniční společnosti budou pokládat otázku, zdali se jim ukládání dat ve Spojených státech vyplatí riskovat (Null 2013).

6.2.4 Shrnutí

Snowdenova odhalení změnila pohled uživatelů na bezpečnost a soukromí. Pro vládu se tak situace stává komplikovanější, protože se americké zpravodajské služby musí více vyhýbat veřejnosti, která ví o metodách, které služby používají a veřejnost si osvojuje protiopatření. Prvním jevem, který se dal pozorovat po rozšíření dokumentů ke kauze PRISM, byl vzrůstající počet uživatelů, kteří se začali zabývat anonymizací jejich internetové aktivity (Paganini).

Snowden, který ukázal světové veřejnosti obsedantní posedlost vlády ve sledování její aktivity, poznamenal, že za jistých podmínek je web stále schopný udržet anonymitu uživatelů. Šifrování a anonymizace jsou primárními nástroji v ochraně anonymity, které pomáhají chránit před dohledem vlády, která se nicméně neustále snaží snižovat místa na internetu, kde nemůže uživatele sledovat (Paganini).

Chování uživatelů na internetu se po Snowdenových odhaleních změnilo. Především se znatelně snížila důvěra ve vládní instituce a velké IT společnosti, poskytující např. *cloudové* služby. Na internetu roste

množství internetových stránek, které zdarma nabízejí „soukromí – přívětivý“ software. Stránka prism-break.org je jedním z příkladů reakce na kauzu PRISM. Nicméně lze s jistotou konstatovat, že sledovací programy budou i nadále pokračovat a výdaje na sledovací aktivity jen porostou. Z tržního pohledu dává pokles důvěry v americké prodejce výhodu jiným subjektům (Paganini).

Co se týče využívání alternativních vyhledávačů, tak i přes to, že vzrostlo jejich využívání, si Sullivan nemyslí, že by mohl *DuckDuckGo* ohrozit vyhledávač *AOL Search*. Dle něj může být *DuckDuckGo* vynášející byznys, ale s omezeným počtem pracovníků a výdaji není pro Google vážnou hrozbou a to ani v dnešní době, kdy je otázka soukromí na internetu aktuální (Sullivan 2013).

7 ZÁVĚR

Tajné služby už od nepaměti tvoří, dalo by se říci, základ každého moderního státu. Státy, jako aktéři, žijí v neustálé nejistotě a v dnešní době moderních technologií je stále těžší zajistit bezpečnost národa. Díky dokumentům Edwarda Snowdena, zveřejněných britským deníkem *The Guardian a* americkým *The Washington Post*, se mohl celý svět dozvědět o tom, co vlastně všichni vědí, a sice to, že vláda sleduje. Nedochází ovšem jenom ke sledování cizích hrozeb ze strany ať už státních, či nestátních aktérů, ale i ke sledování běžného obyvatelstva. Přitom zákony jako např. Vlastenecký zákon, byly vytvořeny právě pro to, aby stát naplnil jednu ze svých nejdůležitějších povinností, a to zajistit národní bezpečnost a ochránit tak své obyvatelstvo. Snowdenovy dokumenty však ukázaly, že informace o běžných Američanech jsou stejně důležité jako informace o představitelích teroristických organizací.

V dnešní době, kdy se v našich životech objevují technologie, nejen ty komunikační, prakticky na každém kroku, je čím dál tím těžší udržet si své soukromí. Jistě, technologie nám náš život velmi usnadňují. Dnes není problém se téměř kdekoliv připojit na internet pomocí chytrých zařízení, ať už tabletů či telefonů, a najít si informace, které hledáme, sdílet s přáteli své fotografie, pracovat z domova apod. Cenou za to je naše soukromí.

Cílem mé práce bylo zjistit, jaké byly dopady kauzy PRISM na veřejnost a zdali došlo po odhalení kauzy PRISM k nějakým reformám, které by zabránily dalšímu shromažďování dat.

Reformy, které provedl prezident Barack Obama, by se daly definovat jako kosmetické. Situace se může změnit po hlasování o červnovém prodloužení Vlasteneckého zákona, které pokud neprojde, udělalo by sledování o něco složitější. Nicméně sledování, odposlechy atd. tu byly, jsou a budou. V případě ukončení jednoho sledovacího programu dojde k nahrazení programem jiným, který bude zase o něco

komplexnější. Záleží pouze na tom, na kolik o tom bude informována veřejnost.

Z průzkumů, které jsem ve své práci uvedl, vyplývá, že po Snowdenových odhaleních vzrostla obava uživatelů o jejich soukromí a snaží se, i když někdy jen o trochu více, své soukromí v digitálním světě zabezpečit. Mezi uživateli vzrostla obliba šifrovaného připojení, klesl zájem o *cloudové* služby nabízené americkými společnostmi, uživatelé si častěji mění svá hesla nebo využívají jiných vyhledávačů, než je nejznámější Google. Nicméně i nadále existuje velká skupina uživatelů, kteří svůj přístup k soukromí na internetu nezměnili - především z neznalosti dostupných nástrojů. Dále průzkum mezi americkým obyvatelstvem ukázal, že více než polovina dotázaných si nemyslí, že by vládní sledovací programy sloužily veřejným zájmům. Navzdory tomu ovšem většina Američanů podporuje sledovací programy, které slouží ke sledování konkrétních jedinců, kteří např. na internetu hledají návody na výrobu bomb apod.

Další průzkum, který srovnával přístup Evropanů a Američanů ke sledování, ukázal, že i když si obě veřejnosti cení soukromí, jsou oproti Evropanům Američané ochotni obětovat své soukromí ve jménu národní bezpečnosti. Naproti tomu Evropané si myslí, že vláda není oprávněna zasahovat do soukromí svých obyvatel, a to ani v případě, jedná-li se o národní bezpečnost.

Co se týče cloudových služeb, zde bude zajímavé sledovat budoucí vývoj. Ztráty týkající se *cloudových* služeb mohou Američany kvůli kauze PRISM a dalším sledovacím programům stát až desítky miliard dolarů. Zajímavá tedy bude reakce např. Evropy, kde nejsou c*loudové* služby zas tolik populární, a to především právě kvůli bezpečnosti dat. To bude chtít Evropa změnit a zajistit, aby si evropské společnosti vybíraly právě evropské poskytovatele. Některé evropské státy (např. Německo) se snaží urychlit plány, které by v budoucnu zajistily udržení německých dat uvnitř německých hranic.

8 SEZNAM POUŽITÉ LITERATURY A PRAMENŮ

Knihy a odborné články

Acquisti, Alessandro – Gross, Ralph (2006). Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook. *Heinz College.* (http://www.heinz.cmu.edu/~acquisti/papers/acquisti-gross-facebook-privacy-PET-final.pdf, 20. 3. 2015), s. 1 – 16.

Bamford, James (2009). *The shadow factory: the ultra-secret NSA from 9/11 to the eavesdropping on America* (New York: Anchor Books).

Greenwald, Glenn (2014). *No place to hide: Edward Snowden, the NSA and the surveillance state* (London: Hamish Hamilton).

Chiru, Claudiu (2014). Privacy on the internet in the digital era. *Economics, Management, and Financial Markets* 9(4), 141 – 149.

Krieger, Wolfgang (2011). *Dějiny tajných služeb: od faraonů k CIA* (Praha: Vyšehrad).

O'Harrow, Robert Jr. – Nakashima, Ellen (2013). *President's surveillance program worked with private sector to collect data after Sept. 11, 2001*. In: The Washington Post, *NSA Secrets: Government Spying in the Internet Age* (Kindle Edition: Diversion Books), 705 – 771.

Ridge, Tom (2004). Using the Patriot Act to fight terrorism. *Congressional Digest*, 266 – 268).

Risen, James (2006). State *of war: the secret history of the CIA and the Bush administration* (New York: Free Press).

Internetové zdroje

Abramson, Larry (2005). The Patriot Act: Alleged Abuses of the Law. *NPR.* 20. 7. 2005 (http://www.npr.org/templates/story/story.php?storyId=4756403, 15. 4. 2015).

Ackerman, Spencer (2013). Lavabit email service abruptly shut down citing government interference. *The Guardian.* 9. 8. 2013 (http://www.theguardian.com/technology/2013/aug/08/lavabit-email-shut-down-edward-snowden, 20. 3. 2015).

Angwin, Julia – Valentino – DeVries, Jennifer (2011). Apple, Google Collect User Data. *The Wall Street Journal.* 22. 4. 2011 (http://www.wsj.com/articles/SB10001424052748703983704576277101723453610, 23. 3. 2015).

Beal, Vangie. cloud computing (the cloud). *Webopedia.* (http://www.webopedia.com/TERM/C/cloud_computing.html, 18. 4. 2015).

Beuth, Patrick (2013). Bundesbehörden sehen Risiken beim Einsatz von Windows 8. *Zeit Online.* 29. 8. 2013 (http://www.zeit.de/digital/datenschutz/2013-08/trusted-computing-microsoft-windows-8-nsa, 15. 4. 2015).

Bio. (2015). *Edward Snowden Biography* (http://www.biography.com/people/edwardsnowden-21262897, 19. 3. 2015).

Brown, Andrew (2010). Facebook is not your friend. *The Guardian*. 14. 5. 2010 (http://www.theguardian.com/commentisfree/andrewbrown/2010/may/14/facebook-not-your-friend, 25. 2. 2015).

Campbell, Duncan (1999). How NSA access was built into Windows. *Telepolis*. 4. 9. 1999 (http://www.heise.de/tp/artikel/5/5263/1.html, 25. 3. 2015).

CIGI. *CIGI-Ipsos Global Survey on Internet Security and Trust* (https://www.cigionline.org/internet-survey, 18. 4. 2015).

Clapper, James R. (2013). DNI Statement on Activities Authorized Under Section 702 of FISA. *Office of the Director of National Intelligence.* 6. 6. 2013 (http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa, 22. 3. 2015).

Coats, Kenneth (2014). One Nation Under Surveillance. 5 Ways You Give The Government Control. *The Huffington Post.* 28. 4. 2014 (http://www.huffingtonpost.com/kenneth-coats/one-nation-under-surveill_b_4861289.html, 20. 3. 2015).

Electronic Frontier Foundation. *National Security Letters: FAQ* (https://www.eff.org/issues/national-security-letters/faq, 20. 3. 2015).

Electronic Privacy Information Center (2005). *USA PATRIOT ACT SUNSET* (https://epic.org/privacy/terrorism/usapatriot/sunset.html, 18. 4. 2015).

European Commission (2013). *What does the Commission mean by secure Cloud computing services in Europe?* (http://europa.eu/rapid/press-release_MEMO-13-898_en.htm, 18. 4. 2015).

ExpressVPN (2015). *Edward Snowden's Biography in a Nutshell!* (https://www.expressvpn.com/internet-privacy/guides/edward-snowden-biography/, 19. 3. 2015).

Gellman, Barton - Poitras, Laura (2013). U.S., British intelligence mining data from nine U.S. Internet companies in broad secret program. *The Washington Post.* 7. 6. 2013 (http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html, 20. 3. 2015).

Gil, Paul. What Is 'Cloud Computing'? *AbouTech.* (http://netforbeginners.about.com/od/c/f/cloudcomputing.htm, 18. 4. 2015).

Grabianowski, Ed (2007a). How the Patriot Act Works. *How stuff works*. 6. 7. 2007 (http://people.howstuffworks.com/patriot-act.htm, 20. 3. 2015).

Grabianowski, Ed (2007b) . How the Patriot Act Works. *How stuff works*. 6. 7. 2007 (http://people.howstuffworks.com/patriot-act1.htm, 20. 3. 2015).

Grabianowski, Ed (2007c) . How the Patriot Act Works. *How stuff works*. 6. 7. 2007 (http://people.howstuffworks.com/patriot-act2.htm, 20. 3. 2015).

Grabianowski, Ed (2007d) . How the Patriot Act Works. *How stuff works*. 6. 7. 2007 (http://people.howstuffworks.com/patriot-act4.htm, 20. 3. 2015).

Greenwald, Glenn – MacAskill, Ewen – Poitras, Laura – Ackerman, Spencer – Rushe, Dominic (2013). Microsoft handed the NSA access to

encrypted messages. *The Guardian*. 12. 7. 2013 (http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data, 22. 3. 2015).

Greenwald, Glenn – MacAskill, Ewen – Poitras, Laura (2013). Edward Snowden: the whistleblower behind the NSA surveillance revelations. *The Guardian*. 11. 6. 2013 (http://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblowersurveillance, 19. 3. 2015).

Greenwald, Glenn (2013). NSA collecting phone records of millions of Verizon customers daily. *The Guardian.* 6. 6. 2013 (http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-courtorder, 23. 3. 2015).

Harding, Luke (2014). How Edward Snowden went from loyal NSA contractor to whistleblower. *The Guardian*. 1. 2. 2014 (http://www.theguardian.com/world/2014/feb/01/edward-snowden-intelligence-leaknsa-contractor-extract, 19. 3. 2015).

Chesbro, Michael. A Brief History of U.S. Intelligence. *American board for certification in Homeland Security.*(http://www.abchs.com/ihs/SUMMER2014/ihs_articles_1.php, 18. 4. 2015).

Christensson, Per (2010). What is the difference between upstream and downstream traffic? *PC.net.* 28. 5. 2010 (http://pc.net/helpcenter/answers/upstream_vs_downstream_traffic, 19. 4. 2015).

Infoplease. *National Security Agency* (http://www.infoplease.com/encyclopedia/history/national-security-agency.html, 20. 3. 2015).

Internet live stats. *Internet users* (http://www.internetlivestats.com/internet-users/, 25. 2. 2015).

Investopedia. *USA Patriot Act* (http://www.investopedia.com/terms/p/patriotact.asp, 15. 3. 2015).

Janssen, Cory. Internet Privacy. *Technopedia*. (http://www.techopedia.com/definition/24954/internet-privacy, 23. 2. 2015).

Johnson, Bobbie (2010). Privacy no longer a social norm, says Facebook founder*. The Guardian*. 11. 1. 2010 (http://www.theguardian.com/technology/2010/jan/11/facebook-privacy, 24. 3. 2015).

Kayyali, Nadia (2015). Section 215 of the Patriot Act Expires in June. Is Congress Ready? *Eletronic Frontier Foundation.* 29. 1. 2015 (https://www.eff.org/deeplinks/2015/01/section-215-patriot-act-expires-june-congress-ready, 19. 4. 2015).

McCormick, Will (2014). 71% of Americans Care Deeply about their Online Privacy Amid Recent Privacy Concerns. *Business Wire*. 29. 7. 2014 (http://www.businesswire.com/news/home/20140729006077/en/71-Americans-Care-Deeply-Online-Privacy-Privacy#.VTq2TpP-i9K, 18. 4. 2015).

Microsoft News Center (2013). *Statement from Microsoft about response to government demands for customer data* (http://news.microsoft.com/2013/07/11/statement-from-microsoft-about-response-to-government-demands-for-customer-data/, 22. 3. 2015).

Murse, Tom (2015). What is the National Security Agency? *About.com.* (http://uspolitics.about.com/od/usgovernment/a/intelligencecom.htm, 19. 3. 2015).

Murse, Tom. What is PRISM in the National Security Agency?*About.com* (http://uspolitics.about.com/od/antiterrorism/a/What-Is-Prism-In-The-National-Security-Agency.htm, 10. 2. 2015).

Neal, Ryan W. (2013a). Edward Snowden Reveals Secret Decryption Programs: 10 Things You Need To Know About Bullrun And Edgehill. *International Business Times.* 6. 9. 2013 (http://www.ibtimes.com/edward-snowden-reveals-secretdecryption-programs-10-things-you-need-know-about-bullrun-edgehill, 23. 3. 2015).

Neal, Ryan W. (2013b). NSA PRISM Leaks Boost Private Search Engines: StartPage And Ixquick Pass 4 Million Daily Searches. *International Business Times.* 15. 7. 2013 (http://www.ibtimes.com/nsa-prism-leaks-boost-private-search-engines-startpage-ixquick-pass-4-million-daily-searches-1346457, 17. 4. 2015).

Neuman, Scott (2015). Snowden: Asylum In Switzerland A 'Great Political Option'. *NPR*. 6. 3. 2015 (http://www.npr.org/blogs/thetwo-way/2015/03/06/391279409/snowden-asylum-in-switzerland-a-great-political-option, 16. 3. 2015).

Nichols – Vaughan, Steven J. (2015). The most popular US end-user operating systems, according to the federal government. *ZDnet*. 27. 3. 2015 (http://www.zdnet.com/article/the-federal-government-on-what-are-the-most-popular-us-end-user-operating-systems/, 25. 3. 2015).

Null, Christopher (2013). PRISM could ruin businesses that rely on the cloud. *PCWorld.* 14. 8. 2013 (http://www.pcworld.com/article/2046652/prism-could-ruin-businesses-that-rely-on-the-cloud.html, 17. 4. 2015).

Office of the Director of National Intelligence (2013). *Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (http://www.dni.gov/files/documents/Facts%20on%20the%20Collection%20of%20Intelligence%20Pursuant%20to%20Section%20702.pdf 23. 3. 2015).

OpenCongress. *Protect America Act of 2007* (https://www.opencongress.org/wiki/Protect_America_Act_of_2007#note-Lichtblau_et_al, 23. 3. 2015).

Padilla, Len (2014). How the PRISM fallout impacts cloud adoption. *DatacenterDynamics.* 14. 1. 2014 (http://www.datacenterdynamics.com/security/how-the-prism-fallout-impacts-cloud-adoption/84561.fullarticle, 17. 4. 2015).

Paganini, Pierluigi (2015). Encryption Increases Its Popularity and US Is in a Dilemma. *Security Affairs.* 13. 4. 2015 (http://securityaffairs.co/wordpress/35936/digital-id/encryption-us-problem.html, 16. 4. 2015).

Paganini, Pierluigi. NSA Surveillance Is Changing Users' Internet Experience. *Infosec Institute.* (http://resources.infosecinstitute.com/nsa-surveillance-changing-users-internet-exp***l***, 17. 4. 2015).

PC.net (2015). *Spyware* (http://pc.net/glossary/definition/spyware, 23. 2. 2015).

Privacy International. *The Five Eyes* (https://www.privacyinternational.org/?q=node/51, 21. 3. 2015).

Rainie, Lee – Madden, Mary (2015). Americans‘ Privacy Strategies Post – Snowden. *Pew Research Center.* 16. 3. 2015 (http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/, 16. 4. 2015).

Ray, Michael (2014). Edward Snowden American intelligence contractor. *Encyclopædia Britannica*. 23. 10. 2014 (http://www.britannica.com/EBchecked/topic/1934662/Edward-Snowden, 19. 3. 2015).

Reardon, Marguerite (2011). Lawmakers demand answers from Apple on iPhone tracking. *CNET.* 21. 4. 2011 (http://www.cnet.com/news/lawmakers-demand-answers-from-apple-on-iphone-tracking/, 24. 3. 2015).

Risen, James – Lichtblau, Eric (2005). Bush Secretly Lifted Some Limits on Spying in U.S. After 9/11, Ofiicials Say. *The New York Times*. 15. 12. 2005 (http://www.nytimes.com/2005/12/15/politics/15cndprogram.html?pagewanted=all&_r=2&, 23. 3. 2015).

Risen, Tom (2015). Would NSA Data Surveillance End With Patriot Act? *U.S. News.* 25. 3. 2015 (http://www.usnews.com/news/articles/2015/03/25/would-nsa-data-surveillance-end-with-patriot-act, 19. 4. 2015).

Rosen, Jeffrey (2011). The Patriot Act Gives Too Much Power to Law Enforcement. *The New York Times.* 8. 9. 2011 (http://www.nytimes.com/roomfordebate/2011/09/07/do-we-still-need-the-patriot-act/the-patriot-act-gives-too-much-power-to-law-enforcement, 18. 4. 2015).

RT (2013). *Canadian spy agency 'dissected' Brazilian Energy Ministry* (http://rt.com/news/canada-spying-brazilian-ministry-819/, 21. 3. 2015).

Rybka, Michal (2014). Kdo a proč zabil TrueCrypt? *PCTuning.* 6. 6. 2014 (http://pctuning.tyden.cz/software/ochrana-soukromi/30086-kdo-a-proc-zabil-truecrypt?start=7, 20. 3. 2015).

Skype / Microsoft (2014). *Skype Terms of Use* (http://www.skype.com/en/legal/tou/, 23. 3. 2015).

Smith, Tom (2013). Apathy to PRISM Represents Changing Attitudes to Privacy. *GlobalWebIndex.* 24. 6. 2013 (http://www.globalwebindex.net/blog/apathy-to-prism-represents-changing-attitudes-to-privacy, 16. 4. 2015).

Solomon, John (2007). FBI Finds It Frequently Overstepped in Collecting Data. *The Washington Post*. 14. 6. 2007 (http://www.washingtonpost.com/wp-dyn/content/article/2007/06/13/AR2007061302453.html, 20. 3. 2015).

Soper, Taylor (2015). ACLU technologist: 'Amazon has escaped the transparency spotlight'. *Geekwire.* 12. 3. 2015 (http://www.geekwire.com/2015/prominent-aclu-technologist-chris-soghoian-amazon-has-escaped-the-transparency-spotlight/, 18. 4. 2015).

Sottek, T. C. – Kopstein, Joshua (2013). Everything you need to know about PRISM. *The Verge*. 17. 7. 2013 (http://www.theverge.com/2013/7/17/4517480/nsa-spying-prism-surveillance-cheat-sheet, 10. 2. 2015).

Statista (2015). *Leading social networks worldwide as of March 2015, ranked by number of active users (in millions)* (http://www.statista.com/sta

tistics/272014/global-social-networks-ranked-by-number-of-users/, 31. 3. 2015).

Stokes, Bruce (2013). NSA Spying: A Threat to US Interests? *YaleGlobal online*. 5. 12. 2013 (http://yaleglobal.yale.edu/content/nsa-spying-threat-us-interests, 24. 3. 2015).

Strohm, Chris (2015). Obama Puts Limited Restraints on NSA Spying After Snowden Leaks. *BloombergBusiness*. 3. 2. 2015 (http://www.bloomberg.com/news/articles/2015-02-03/obama-puts-limited-restraints-on-nsa-spying-after-snowden-leaks-i5pfsf9c, 25. 3. 2015).

Sullivan, Danny (2013). Duck Duck Go's Post-PRISM Growth Actually Proves No One Cares About "Private" Search. *Search Engine Land.* 22. 6. 2013 (http://searchengineland.com/duck-duck-go-prism-private-search-164333, 17. 4. 2015).

TechTerms. *Phishing* (http://techterms.com/definition/phishing, 23. 2. 2015).

The Library of Congress. *H.R.3162Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 (Enrolled Bill [Final as Passed Both House and Senate] - ENR*)(http://thomas.loc.gov/cgi-bin/query/F?c107:1:./temp/~c107nLrHUD:e17182:, 25. 3. 2015).

Tucker, Harry (2015). Snowden leaks: Five Eyes alliance, Australian involvement detailed. *News.com.au*. 21. 1. 2015 (http://www.news.com.au/technology/online/snowden-leaks-five-eyes-allianceaustralian-involvement-detailed/story-fnjwnj25-1227191761395, 23. 3. 2015).

Verge Staff (2014). President Obama's NSA reforms show both promise and peril. *The Verge.* 17. 1. 2014 (http://www.theverge.com/2014/1/17/5316980/president-obama-nsa-signals-intelligence-reform-report-card, 25. 3. 2015).

Washingtons Blog (2013). *NSA Built Back Door In All Windows Software by 1999* (http://www.washingtonsblog.com/2013/06/microsoft-programmed-in-nsa-backdoor-in-windows-by-1999.html, 25. 3. 2015).

Zurcher, Anthony (2013). Roman Empire to the NSA: A world history of government spying. *BBC.* 1. 11. 2013 (http://www.bbc.com/news/magazine-24749166, 20. 3. 2015).

9 RESUMÉ

Although the topic of the PRISM cause is only two years old, surveillance in many various forms has been there since time immemorial. PRISM was launched from the ashes of President George W. and since then the National Security Agency (NSA) launched the program for secret data collection. The aim of the program PRISM is to gather information from the Internet and telephone communications from users both in the United States and around the world. The existence of this program was revealed by whistle – blower Edward Snowden, former CIA employee and contractor for NSA. His action divides society into halves. Some people consider him as a hero and some as a traitor to his own country. Snowden pointed out that the NSA does not gather data only about criminals and potential threats to the US, but also about ordinary users or even high – level politicians.

The aim of this work was to find out what are the impacts of PRISM cause on public a whether there have been any reforms that could prevent from further data collection.

The reforms carried out by President Barack Obama, could be defined as cosmetic. The situation may change after the June vote on the extension of the Patriot Act. If the Patriot Act is not extended, it will make surveillance more difficult. However, surveillance, wiretapping etc were there, are there and will be there. In case of termination of a surveillance program, it will be replaced by another one, which will be a little more complex. It just depends on how much, will the public be informed.

The surveys included in the work say that Snowden’s revelations, has increased concerns about users privacy. Now users are trying to make their privacy more secured. The popularity of encryption services and connection has increased among users, less users are interested in cloud services provided by US companies and more users started to use alternative search engines. However, the surveys also showed that even after Snowden’s relevation there is a large group of users, who did not

change their attitude to their privacy – mainly because they do not know the available tools. Another survey, which compared the attitude of European citizens and American citizens about surveillance, has shown that American citizens are more willing to sacrifice their privacy in the name of national security. In contrast, Europeans think that the government is not entitled to interfere the privacy of its citizens and even in the case of national security. As for cloud services, there will be interesting to monitor future developments. Losses, related to cloud services, can cost up Americans, because of the PRISM cause and other surveillance programs, to tens of billions of dollars. Thus the reaction i.e. of Europe will be interesting. In Europe cloud services are not so much popular, mainly because of data security. Some European countries (eg. Germany) make an effort to accelerate plans, which could ensure that the maintenance of their data will stay inside their countries.

10 PŘÍLOHY

Příloha č. 1: PRISM *Upstream*

Příloha č. 2: Data zapojení jednotlivých firem do programu PRISM

Příloha č. 3: Počet hovorů a e-mailů, které prošly americkým komunikačním systémem

Příloha č. 4: Nejpoužívanější sociální sítě dle počtu uživatelů z března 2015

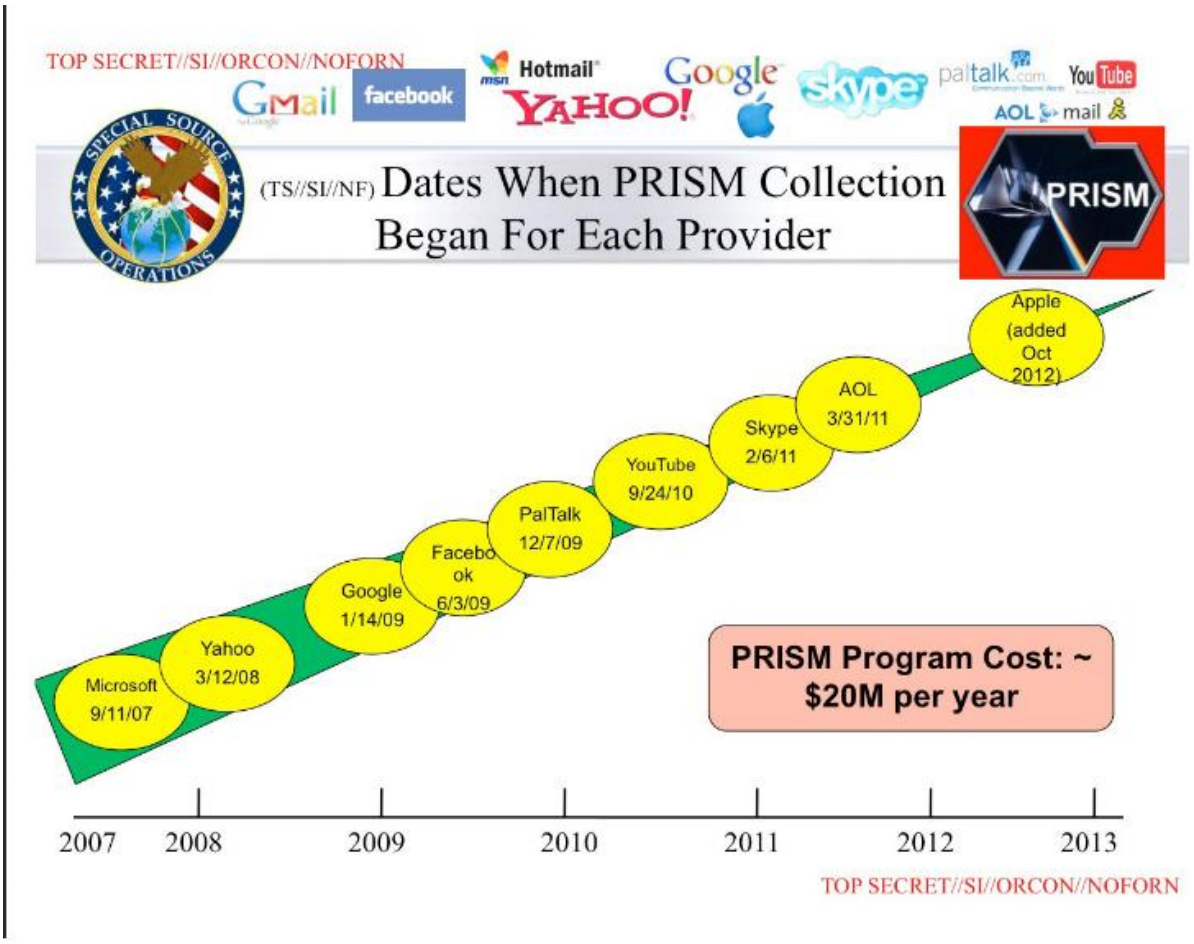
Příloha č. 5: Graf ukazuje rozdílný přístup dvou věkových skupin ke sdílení informací

Příloha č. 6: Kdy se Američané bojí o online soukromí

Příloha č. 1: PRISM *Upstream*

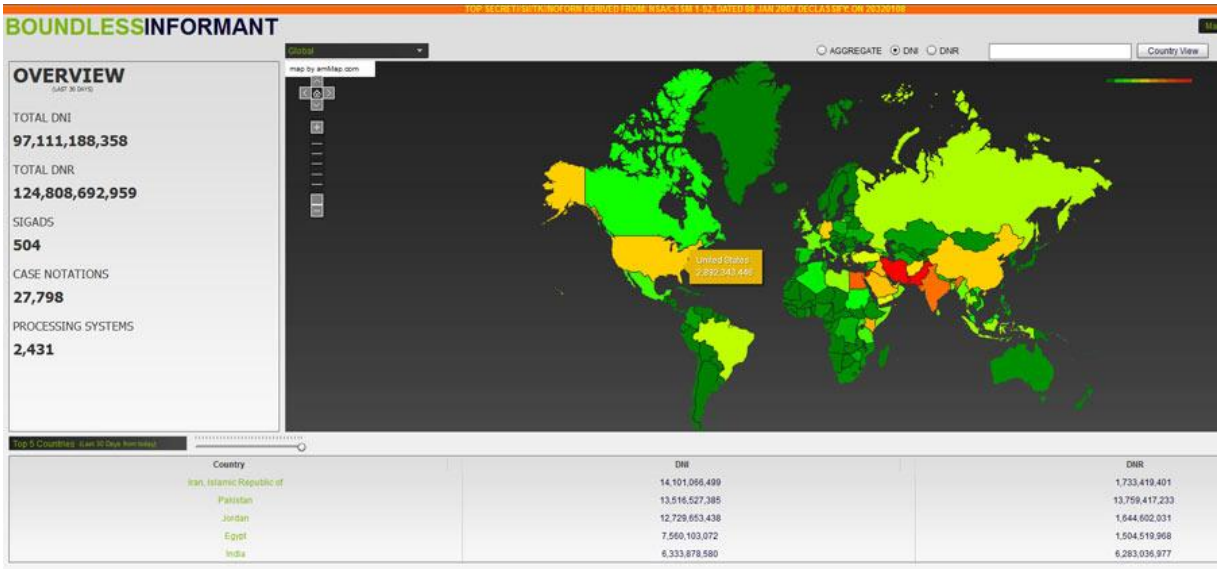
Zdroj: http://www.webpronews.com/leaked-nsa-slide-reveals-prisms-brother-upstream-2013-07, (20. 3. 2015).

Příloha č. 2: Data zapojení jednotlivých firem do programu PRISM



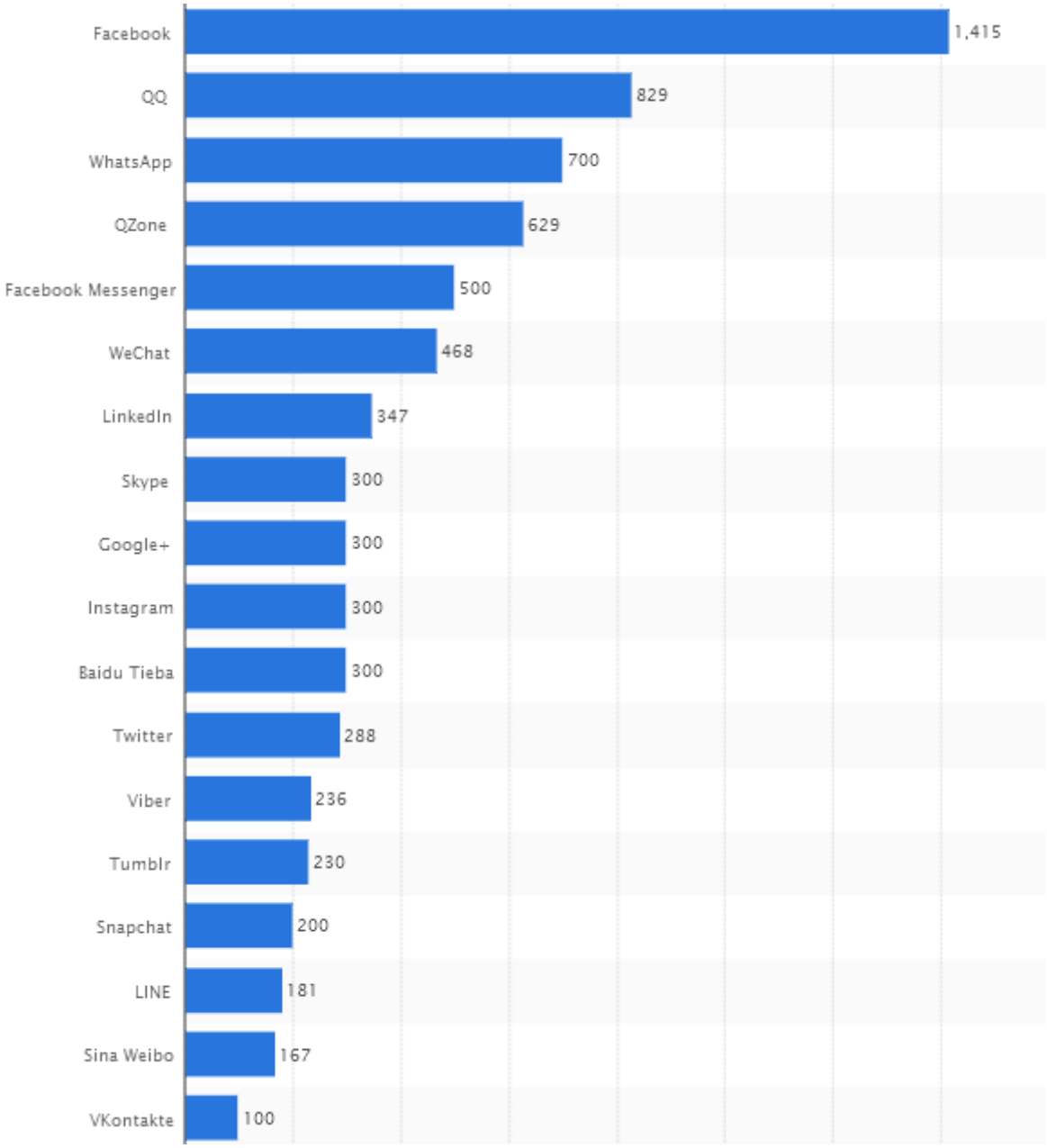
Zdroj: http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, (4. 4. 2015).

Příloha č. 3: Počet hovorů a e-mailů, které prošly americkým komunikačním systémem



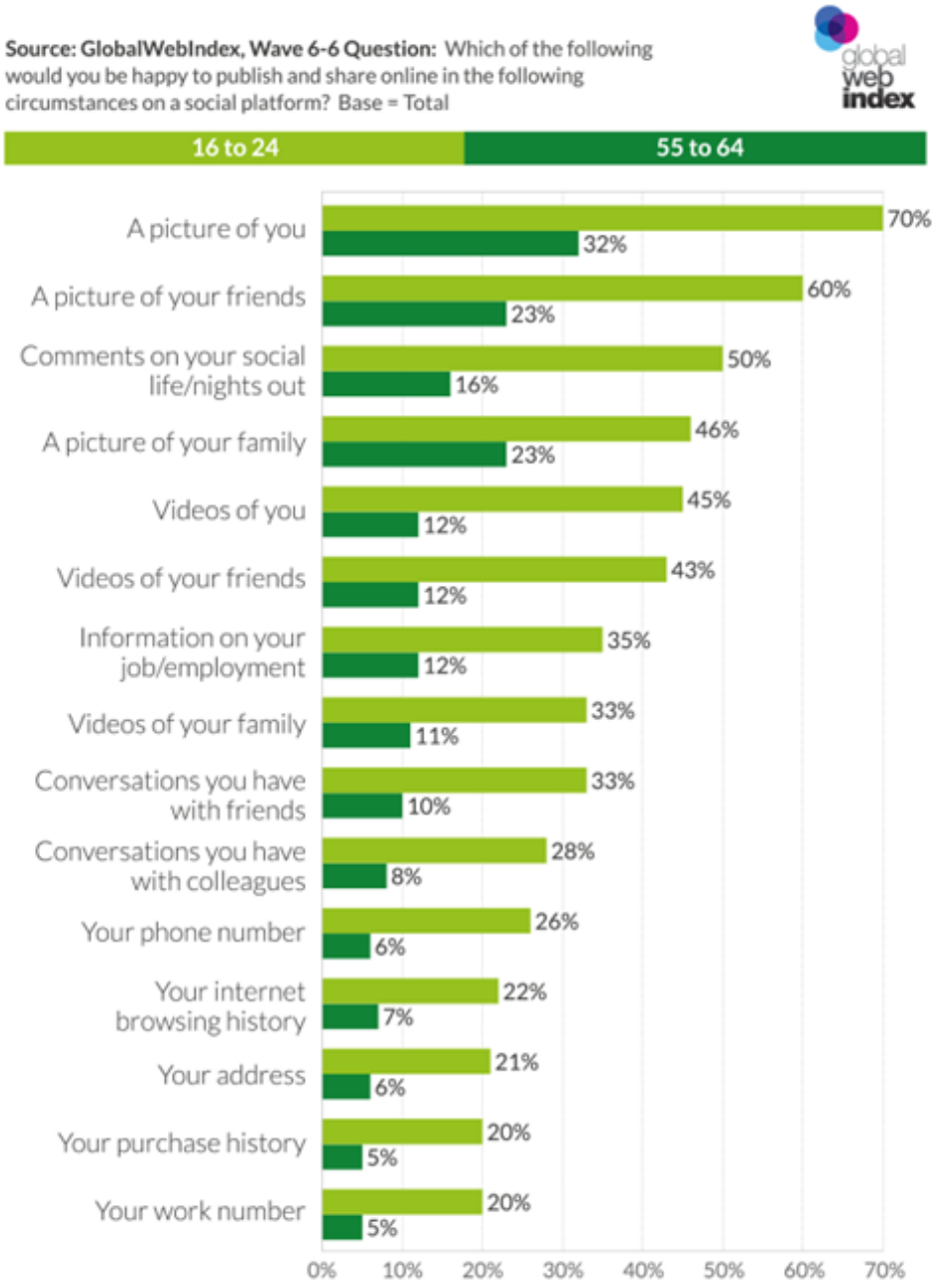
Zdroj: http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining, (5. 4. 2015).

Příloha č. 4: Nejpoužívanější sociální sítě dle počtu uživatelů z března 2015



Zdroj: http://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/, (8. 4. 2015).

Příloha č. 5: Graf ukazuje rozdílný přístup dvou věkových skupin ke sdílení informací



Zdroj: http://www.globalwebindex.net/blog/apathy-to-prism-represents-changing-attitudes-to-privacy, (15. 4. 2015).

Příloha č. 6: Kdy se Američané bojí o online soukromí

Zdroj: http://www.statista.com/chart/2663/when-americans-worry-about-online-privacy/, (15. 4. 2015).