

***BIZTONSÁG VS. TÖRVÉNYES
ELLENŐRZÉS AZ INTERNET
ALAPÚ KOMMUNIKÁCIÓBAN
- ELLENTÉTES VAGY EGYMÁSSAL MEGFÉRŐ
KÖVETELMÉNYEK?***



Dr. Kovács Zoltán

HÍRKÖZLÉS VS. ELEKTRONIKUS ÚTON FOLYTATOTT KOMMUNIKÁCIÓ

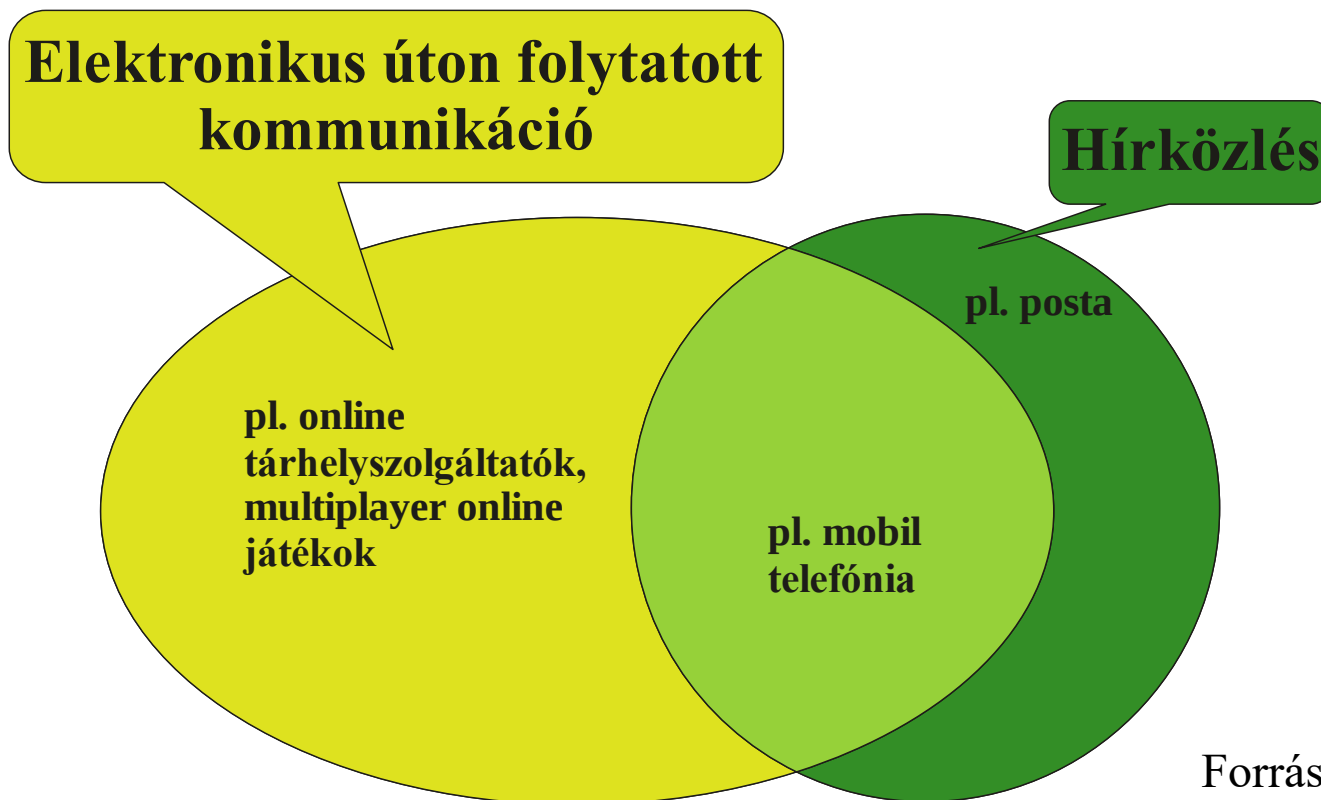
Kommunikáció ellenőrzés:

- Mi is a kommunikáció? „A” személytől „B” személyig eljut az információ?
- Email? És a pizkozatok?
- Posztok, blogok?
- Hírközlés vs. Fájlcseré
- Tárolt adatok?
- Online játékok?
- *[Biztos csak ezt kell ellenőrizni? (pl. Google Maps, kereskedelmi-, banki szolgáltatási alternatívák)]*



AZ ELEKTRONIKUS ÚTON FOLYTATOTT KOMMUNIKÁCIÓ VÁLTOZÁSA

Az elektronikus úton folytatott kommunikáció és a hírközlés viszonya



Forrás: saját



A RÉGI SZABÁLYOZÁS PROBLÉMÁI

Az elektronikus hírközlésről szóló 2003. évi C. törvény (Eht.) –
hagyományos hírközlés

Skype: első béta verziója 2003. augusztusában

2011-re átlagban 20 millió felhasználó használta egyidejűleg

Facebook: 2004. február 4-én debütált

2012. október 4-én havi szinten több, mint 1 milliárd ember használta
aktívan



AZ ELEKTRONIKUS ÚTON FOLYTATOTT KOMMUNIKÁCIÓ VÁLTOZÁSA

Törvényes ellenőrzés:

Az új technológiákat ellenőrizni kell!

Hagyományos technológiák „értéke” csökken a felhasználóknál, így az ellenőrzést végzőknél is.



AZ ELEKTRONIKUS ÚTON FOLYTATOTT KOMMUNIKÁCIÓ VÁLTOZÁSA

Hírközlési szolgáltató

helyett

Infrastruktúra szolgáltató

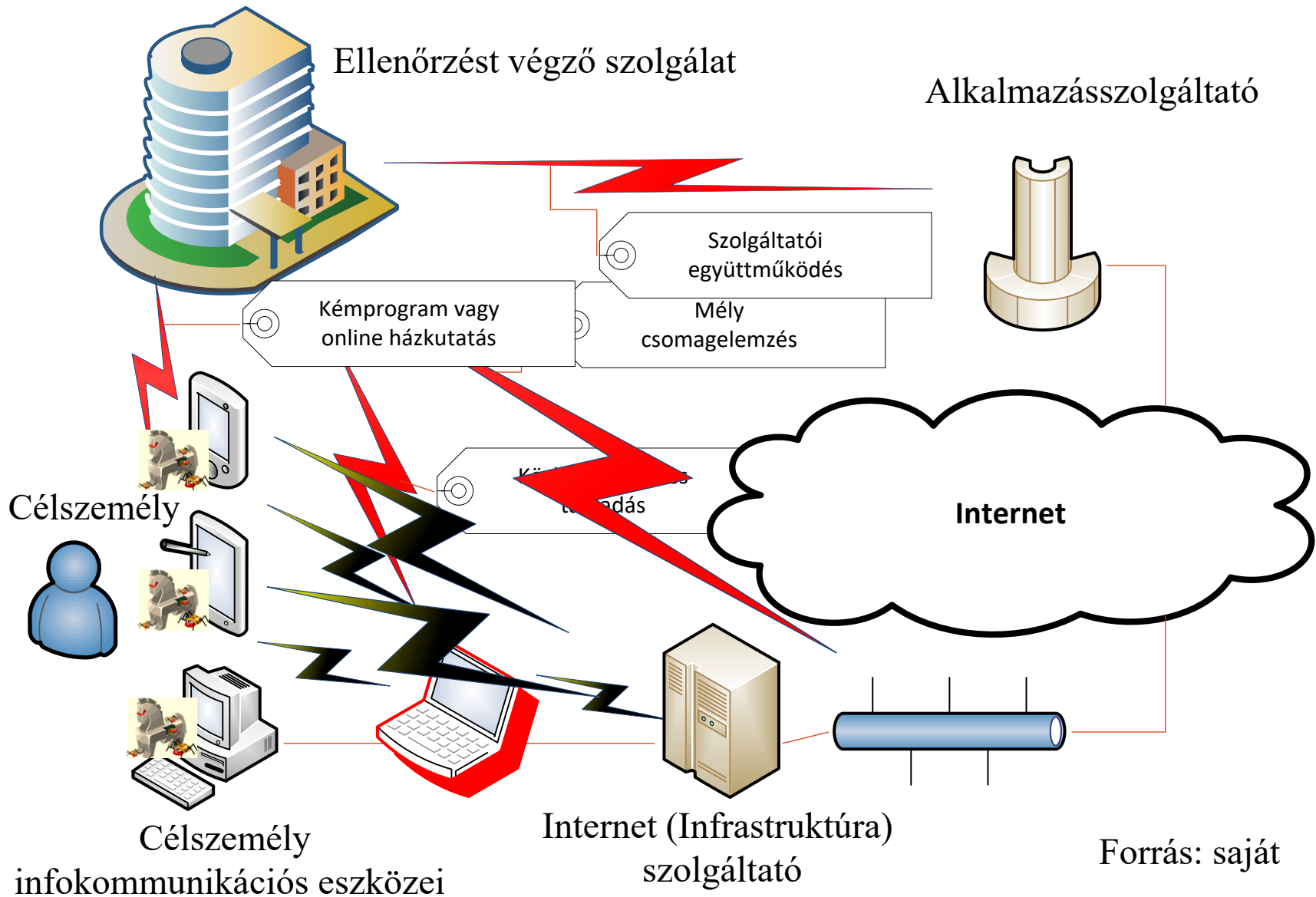
Alkalmazás szolgáltató

Tartalom szolgáltató

Orange vs. Google esete



TECHNIKAI LEHETŐSÉGEK



Forrás: saját



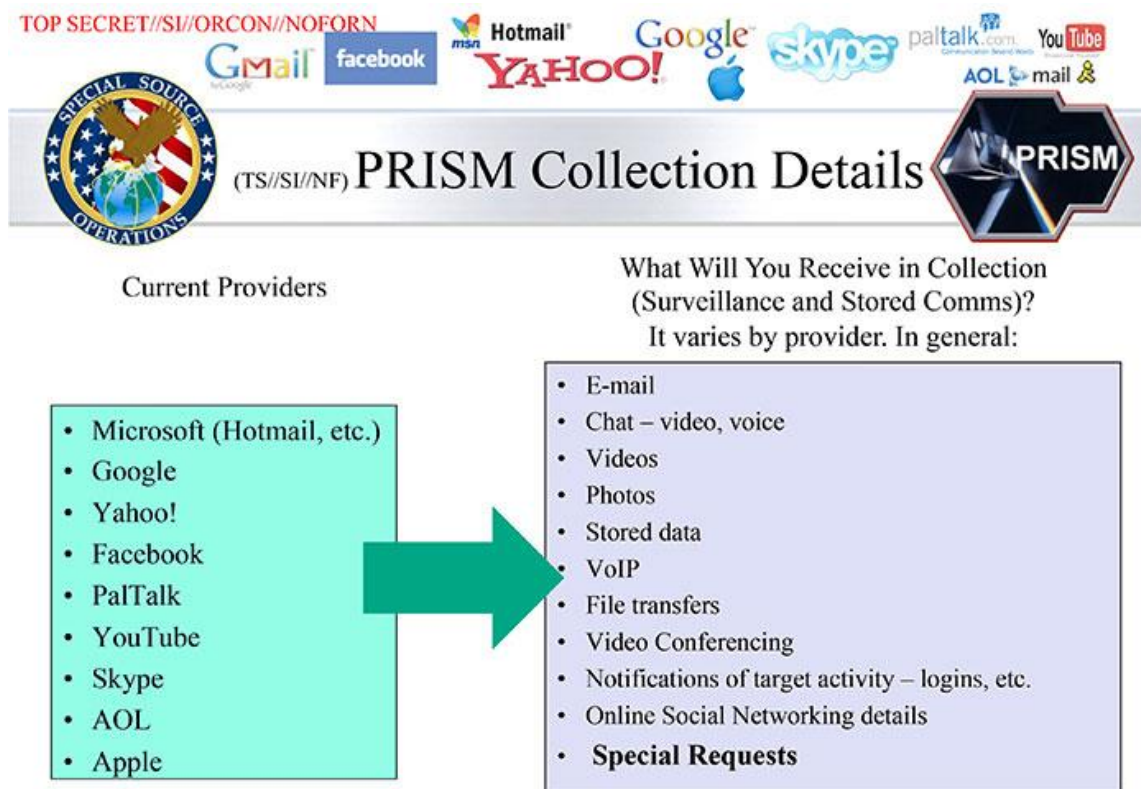
NEMZETKÖZI PÉLDÁK

- Németország és az online házkutatás
„Bundestrojaner” – DigiTask,
majd Gamma Group,
végül saját fejlesztés
- Egyesült Államok és az MitM
Snowden - BADDECISION projekt
- Egyesült Királyság és a mély csomagelemzés
Snowden - TEMPORA projekt



NEMZETKÖZI PÉLDÁK

- USA és a legnagyobb szolgáltatók együttműködése



Complete list and details on PRISM web page:
Go PRISMFAA

TOP SECRET//SI//ORCON//NOFORN



KÖVETKEZTETÉSEK

- minden ország számára kihívás,
- több technikai megoldás is létezik,
- jogi megítélés időnként kétséges,
- nincs általánosan elfogadott jogi szabályozás,
- egyik módszer sem nyújt teljes körű megoldást,
- több (esetleg minden) ellenőrzési módra fel kell készülni,
- **az alkalmazásslavalkóval való együttműködés kikerülhetetlen.**



AZ ÚJ HAZAI SZABÁLYOZÁS

- 2016. évi LXIX. törvény a terrorizmus elleni fellépéssel összefüggő egyes törvények módosításáról
 - 5. 2001. évi CVIII. tv.(Ekertv.) módosítása
- 185/2016. (VII. 13.) Korm. rendelet a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről



A SZABÁLYOZÁS KERETEI

- Felhasználót nem érinti
- Gyártót/fejlesztőt/eladót nem érinti

Végpont-végpont titkosítás

- Szolgáltatót érinti

Előírás, mint a hírközlési szolgáltatónál:

Törvényes ellenőrzés kötelező – meg kell teremtenie a feltételeket



HATÁSA A KOMMUNIKÁCIÓ BIZTONSÁGÁRA

- Példa: NMT 450 vs. GSM
- Szolgáltatói hozzáférés: eddig is kiemelt kockázat volt (pl. Skype, Gmail, Snowden anyagok)
- Nem kell átviteli utat gyengíteni
- Nem kell felhasználó eszközt gyengíteni



HATÁSA A KOMMUNIKÁCIÓ BIZTONSÁGÁRA

- Szolgáltatónak érdeke az audit – versenyelőny
- Ismert lesz a felhasználónak kinek adhatják ki az adatait
- Eddig sem volt garancia, hogy nem építenek-e be valamilyen hátsó kaput



EGYEBEK

- Kikényszeríthetőség
 - Példa: szerencsejátékok, adózás
 - Szankció most: ismételhető pénzbírság
 - Kiforratlan terület még
- Jogi garanciák:
 - Erős meglévő jogi keretek
 - Nincs szűrő-kutató hozzáférés
 - Szolgáltató meggyőződhet törvényességről.



***KÖSZÖNÖM A
FIGYELMET!***

