סמינר באבטחת מחשבים

טרור צדק וחופש – Terror, Justice and Freedom

מרצה:פרופסור אור דונקלמן

מוגש ע"י: שרון עבוד

Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety.

Benjamin Franklin.

טרור

Bathtub falls and police officers kill more Americans than terrorism, yet we've been asked to sacrifice our most sacred rights for fear of falling victim to it.

Edward Snowden.

התמודדות עם הטרור

- הפן הכלכלי – המחיר של התמודדות עם טרור.
- ההשפעה של הטרור על התעשייה.
- השימוש בטרור כדי להצדיק בצורה לא הוגנת כשלים מנהלתיים.
- ההשפעה של טרור על החופש שלנו.

מקרי בוחן-עלות תועלת

FEDERAL APPROPRIATIONS AND OBLIGATIONS	$BILLIONS TOTAL FY2001-2014
Iraq (DOD and State)	823.8
Afghanistan (DOD and State)	718.6
Pakistan (DOD and State) War Related Aid and Reimbursement	19.4
Operation Noble Eagle	29.0
War Related Increases to Pentagon Base[1]	836.1
War Related Veterans Care and Disability[2]	160.4
Estimated Homeland Security War Related Increase	471.6
Interest Payments for Direct War[3]	315.7
TOTAL SPENT FY2001-FY2014	**3,374.5**
Estimate of Obligations Incurred for Veterans Care, NPV 2015-2053[4]	1,000
TOTAL SPENT AND OBLIGATED THROUGH FY2014	**4,374.5**

- 350,000 הרוגים ישירים.
- 6,800 חיילים אמריקים הרוגים.
- 970,000 דרישות נכות חדשות של חיילים.
- 6.7 מיליון פליטים.
- אובדן עצום של זכויות וחופש אזרחי בכול המדינות המעורבות.
- 14 מיליארד דולר על סינון נוסעי מטוסים ללא תפיסה של טרוריסט אחד.
- עלות של מעל 4 טריליון דולר.

SECURE 1000 X-RAY HARDWARE

FIREARMS

- Subject is carrying a .380 ACP pistol

מקרי בוחן-עלות תועלת

	Locked office (burglary)	Open office	Restricted location	Public location	No details	Total
Stolen laptops	18	11	2	27	1	59
Cut Kensington locks	1	5	0	1	0	7
Other physical damage	16	0	0	0	0	16

Figure 1. Information from the logs. The logs from both universities are merged to anonymize the data.

Figure 3. During three of the laptop thefts the students produced a fake e-mail giving them permission to take a laptop and went to the janitor. When the third team approached the janitor, he just gave them the keys and let the students go alone in the office.

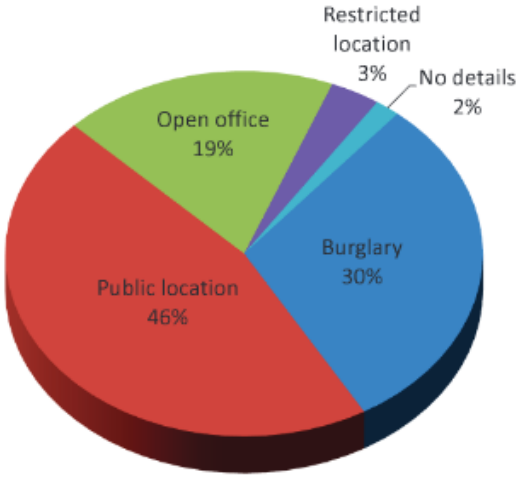


Figure 4. In nine of the tests the custodians willingly gave the laptop, either believing that the teams were from the help desk or that they were sent by the coordinator.

עלות תועלת

סיכון ארגוני זה הסבירות שאיום עקב קימות של נקודות תורפה מתאימים, יתגשם לתקרית אבטחה אשר תגרום נזק לארגון או לשרותי הארגון. המשמעות של הנזק תלויה בערך משאבי הארגון הנפגעים וההשפעה של תקרית האבטחה.

- חוסר באיומים (איומים=0) רומז על חוסר בסיכון ארגוני.
- חוסר בנקודות תרופה (נקודות תרופה=0) רומז על חוסר בסיכון ארגוני.

נובע מכך:

- אמצעי אבטחה צריכים להתמקד במיתון נקודות תורפה ואיומים.
- הסיכון הגבוה ביותר נובע מערך ארגוני גבוה וחשיפה גבוהה לסיכונים.

צ ד ק

Injustice anywhere is a threat to justice everywhere.

Martin Luther King, Jr..

האזנות סתר וטכנולגיה

- 2400 לפני הספירה- שירות הדואר הראשון (מצרים).
- 1792 מערכת הטלגרף אופטי אורך מרחק הראשונה (צרפת -556 תחנות ,4,800 קילומטר).
- 1837 מערכת הטלגרף החשמלית המסחרית הראשונה.
- 1840 המצאת הבול.
- 1876 המצאת הטלפון.
- שנות ה 90 מהפכת האינטרנט.

ההיסטוריה של האזנות הסתר

1860 | 1870 | 1890 | 1920 | 1960 | 1970 | 1990 | 2000 | 2010

1861 מלחמת האזרחים האמריקאית נחשבת כמלחמת המידע הראשונה.

1876 המצאת הטלפון

1890 רשויות אכיפת החוק בארה"ב מתחילות להשתמש בהאזנות סתר

1928 בית המשפט העליון של ארה"ב קובע האזנות סתר חוקיות תחת החוקה

1963 מרטין לותר קינג הבן מואזן על ידי רשויות אכיפת החוק (FBI)

1972 פרשת ווטרגייט

1978 ארה"ב:חוק המעקב המודיעני הפדרלי FISA(Foreign Intelligence Surveillance Act)

1979 ישראל:חוק האזנת סתר

1994 ארה"ב:חוק עזר לרשויות אכיפת החוק בתקשורת CALEA(Communications Assistance for Law Enforcement Act)

1994 פרשת נמרודי

1997 Carnivore(FBI)

1999 ארה"ב :מעל 2,450,000 שיחות טלפון מואזנות בצורה חוקית על יד הרשויות(1350 צווי משפט)

2001 U.S. Patriot act

2005 רשות השידור בארה"ב מאשרת האזנות סתר על VOIP בעזרת CALEA

2013 פרשת סנודן

2014 מכתב הסירוב 8200

האזנות הסתר

http://www.youtube.com/watch?v=xyQluTfyO7g

האזנות סתר בישראל

בישראל, מקובלת ההבחנה בין האזנת סתר למטרת ביטחון המדינה, ובין האזנת סתר למטרת מניעת עבירות פליליות וגילוי עבריינים.

האזנה למטרת ביטחון המדינה מבוצעת על ידי השב"כ או על ידי אגף המודיעין בצה"ל. מי שמתיר בחתימתו האזנת סתר למטרה זו הוא שר הביטחון או ראש הממשלה בלבד, וההיתר תקף עד שלושה חודשים מיום הוצאתו, אך ניתן להאריכו. במקרים דחופים, ראש רשות הביטחון הרלוונטית (ראש השב"כ או ראש אגף המודיעין) רשאים להתיר האזנה גם ללא אישור הדרג המדיני הבכיר, וזאת ל-48 שעות בלבד. בצה"ל, מותרת האזנה למרבית הטלפונים הצה"ליים באישור קשר"ר.

האזנה למטרת גילוי ומניעת עבירות, מבוצעת על ידי המשטרה או על ידי גופי חקירה אחרים (כמו רשות ניירות ערך או הרשות להגבלים עסקיים). היתר להאזנה כזו מתקבל על ידי שופט בבית המשפט המחוזי, לאחר שהוצגו בפניו נימוקים לפגיעה בפרטיות למטרת מניעה מראש או גילוי בדיעבד של פשע (עבירה שעונש המקסימום לגביה הוא מאסר 3 שנים ומעלה). במקרים דחופים רשאי המפקח הכללי של משטרת ישראל להתיר האזנה ל-48 שעות

החוק בישראל אף מתיר לבצע האזנות סתר מסוימות, ללא צורך בהיתר כלשהו, למשל האזנה לתדרים אלחוטיים של חובבי רדיו או של שידורים לציבור. גם האזנה באקראי ובתום לב לשיחה המתקיימת ברשות הרבים - היא מותרת. כמו כן, החוק בישראל מאפשר להאזין לשיחות בינלאומיות ללא צורך בהיתר, וזאת למטרת צנזורה צבאית. גם הקלטה עצמית של שיחות טלפון, או האזנת סתר תוך קבלת הסכמה של אחד הצדדים לשיחה, היא חוקית.

האזנות סתר בישראל נתונים

נתונים שמסרה משטרת ישראל על ההאזנות בשנים 2004-2008

שנה	מספר הבקשות שהוגשו	מספר הבקשות שנדחו	מספר המואזנים	מספר ההיתרים שלא בוצעו	מספר ההיתרים שבוצעו
2004	962	3	632	246	713
2005	996	14	614	101	881
2006	1,255	7	778	127	1,128
2007	1,484	11	958	98	1,375
2008	1,797	16	1,022	83	1,698

מספר הבקשות שאושרו

שנה	ישראל	ארצות הברית
2004	959	1710
2005	982	1773
2006	1248	1839
2007	1473	2208
2008	1781	1891

*ב 2012 מתוך 3395 האזנות סתר בארצות הברית רק 18.19% הביאו להרשעה.

ב 2013 ביצעה ארצות הברית 3576 האזנות סתר , מחיר ממוצע להאזנת סתר *43,361$.עלות שנתית 155 מיליון $*

ב 1993 עלות שנתית של 51 מיליון $.

מעקב וריגול

http://www.youtube.com/watch?v=ljTmnOy8FB0

חוק נתוני תקשורת

חוק סדר הדין הפלילי (סמכויות אכיפה - נתוני תקשורת) -2007 -"חוק האח הגדול"

החוק מאפשר לרשויות חקירה (משטרה , מצ"ח, המחלקה לחקירת שוטרים, רשות ניירות ערך, רשות ההגבלים העסקיים, רשות המסים) לקבל נתוני תקשורת (שכוללים נתוני מיקום , נתוני מנוי, נתוני תעבורה)

נתוני מיקום - שמוגדרים בחוק כנתוני איכון של ציוד קצה שנמצא ברשות מנוי. הכוונה היא לאפשרות לזהות את המקום הגאוגרפי שממנו בוצעה שיחת טלפון, למשל היכן נמצא קו הטלפון הנייח או היכן היה המשוחח בעת שיחה בטלפון נייד (בעיקר טלפון סלולרי).

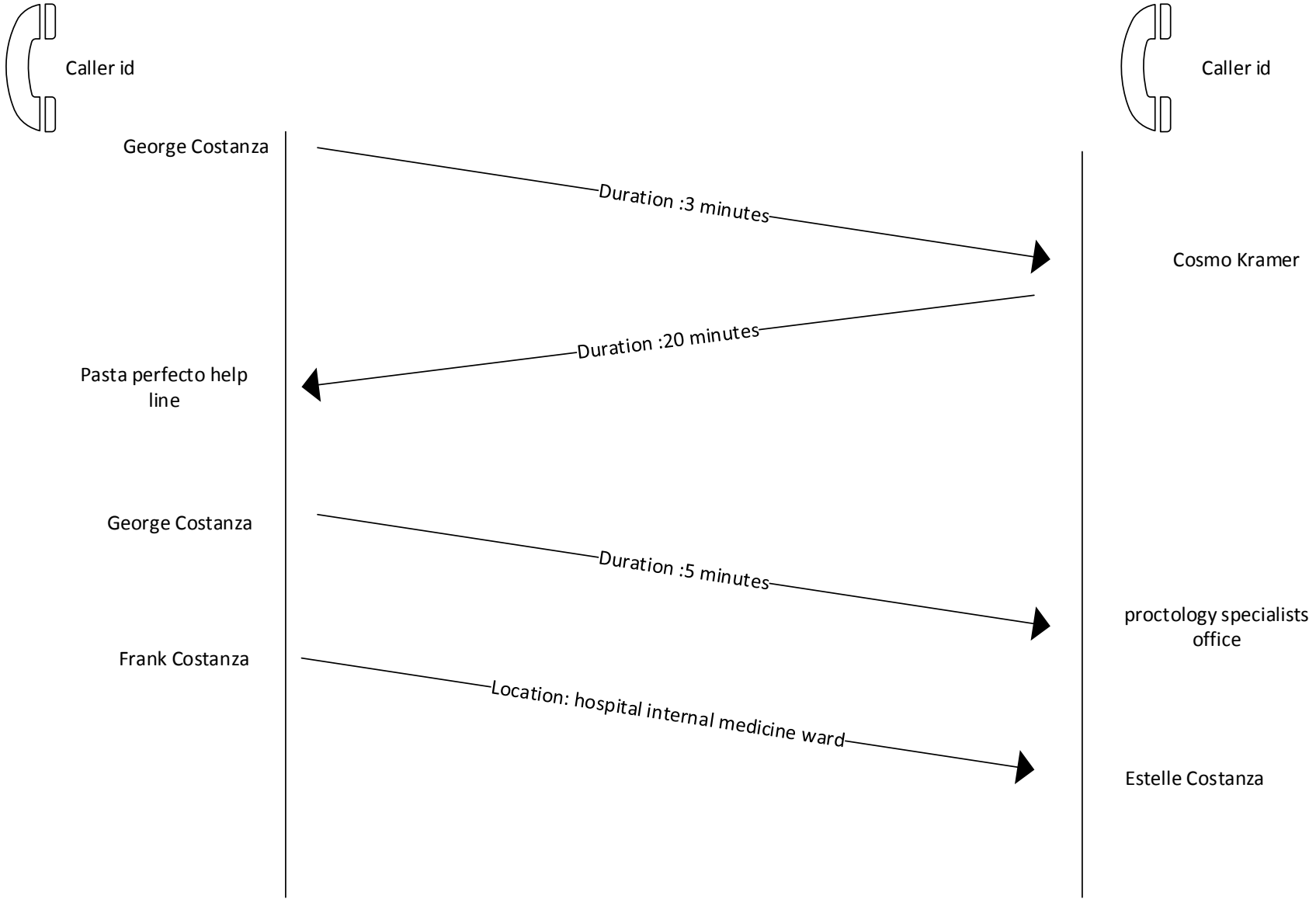
נתוני מנוי - שכוללים את סוג שירות התקשורת (הנקרא בחקיקה שירות בזק, אבל איננו מוגבל לשירותים של חברת בזק), כלומר אם מדובר בשיחת טלפון נייח או נייד, גלישה באינטרנט, משלוח דואר אלקטרוני וכדומה; שם, כתובת ומספר זהות של המנוי; פרטי אמצעי התשלום של המנוי; הכתובת שבה הותקן הציוד שמשמש את המנוי; נתונים מזהים של הציוד.

נתוני תעבורה - שכוללים את סוג התקשורת (שיחה, הודעת דואר אלקטרוני, גלישה באינטרנט, וכדומה); נתונים של הציוד של מי שיזם את השיחה, מי שמקבל אותה וציוד שנמצא בדרך (למשל, אם היה שירות "עקוב אחרי", או במקרים גלישה באינטרנט); נתונים של מקור השיחה ושל היעד; מועד השיחה; משך השיחה או המסר, הסוג שלו (למשל אם צורף קובץ להודעת הדואר האלקטרוני).

באישור בית משפט במקרים רגילים.

או במקרים דחופים על ידי שוטר או שוטר צבאי (ללא ביקורות שיפוטית , קיימת ביקורות של היועץ המשפטי ושל הכנסת אחת לכמה זמן)

חשיבות נתוני תקשורת -דוגמא



ניתוח תעבורה

1998 –ארצות הברית , 1329 האזנות סתר עלי ידי המשטרה , 9507 זימוני איסופי מידע של רשומות שיחות יוצאות (pen registers), 5207 זימוני מכשירי תפוס ועקוב (trap and trace) איסוף מידע של רשומות שיחות נכנסות (גם של שיחות חסומות) .

1992- נתונים מראים שלכחצי מיליון תושבים זומנו נתוני השיחות שלהם.

2006- AT&T העבירה ל NSA את נתוני התעברוה של כול לקוחתיה (בהמשך נאסף המידע של 200 מיליון אמריקים משלושת חברות הטלפון הגדולת).

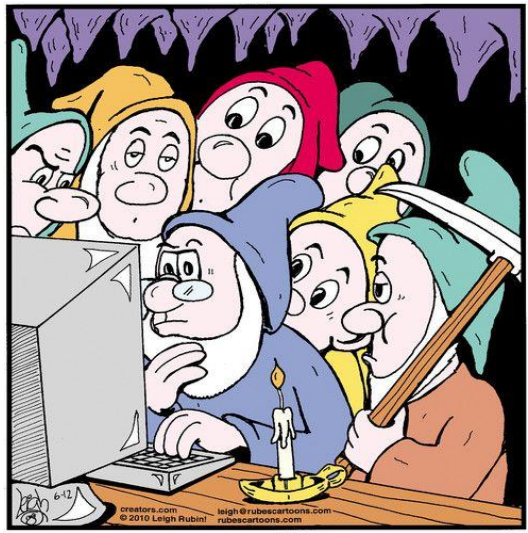
למה להשתמש באמצעי זה:

- זול.
- לא מוגן חוקית כמו האזנות סתר.
- מצריך פחות זמן ופחות משאבים לטיפול.
- מאפשר לקבל נתונים על משתמשים ללא ידעתם.

כריית מידע

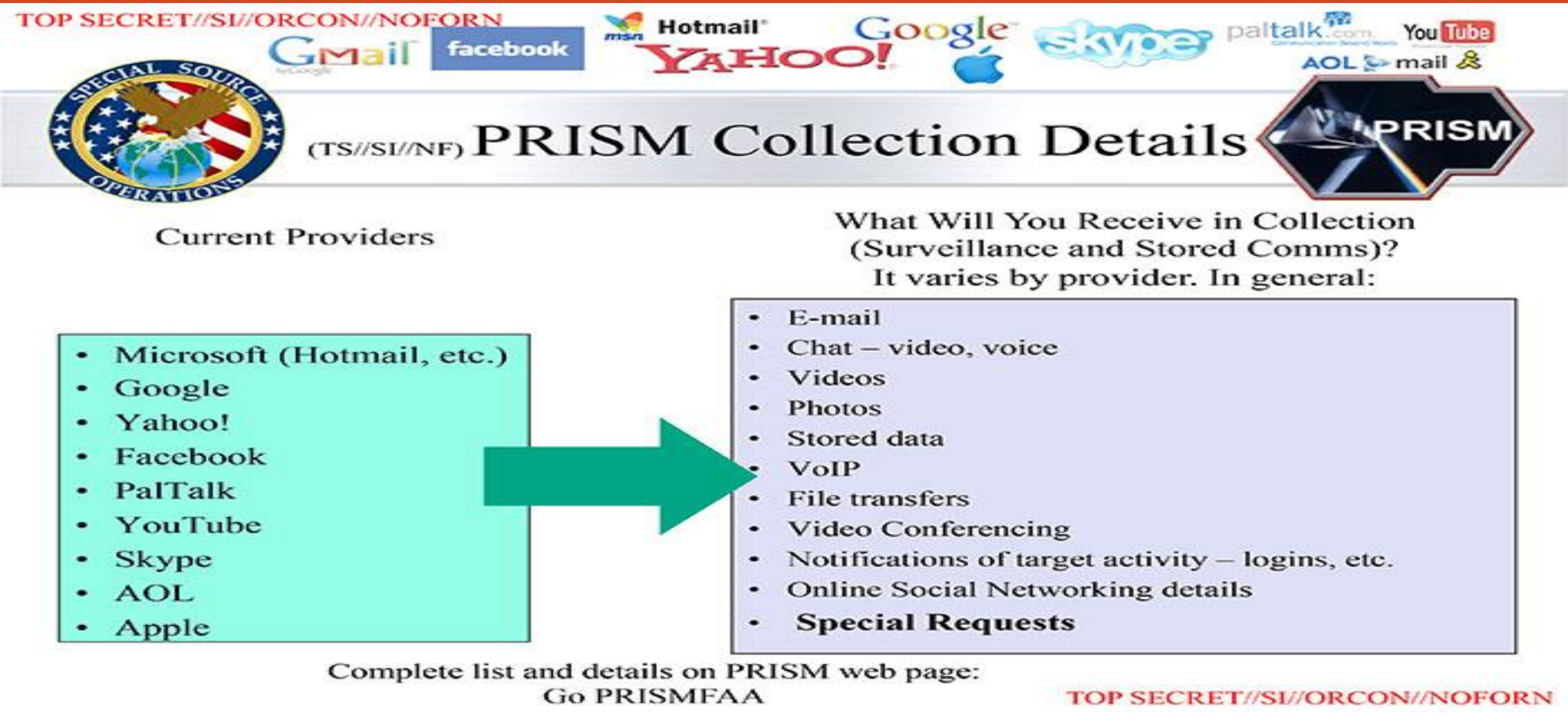
כריית מידע או **כריית נתונים** (באנגלית: **Data mining**) היא הפעלת אלגוריתם או תוכנית מחשב לצורך גילוי מידע הטמון בבסיסי נתונים קיימים, והסקת מסקנות מהצלבתו. גילוי ידע בבסיסי נתונים הוא תהליך שנועד לחקור ולנתח כמות גדולה של מידע באמצעים אוטומטיים ככל שניתן כדי לגלות דפוסים .

- **Total Information Awareness** (**TIA**)-information collected :
    - credit card purchases, magazine subscriptions, web browsing histories, academic grades, bank deposits, passport applications, driver's licenses, toll records, judicial records, divorce records, etc.
    - Health information collected by TIA include drug prescriptions ,medical records, and individual DNA.
- **Multistate Anti-Terrorism Information Exchange Program(MATRIX)**
- **Prism**
- **Muscular**



Data mining

PRISM


TOP SECRET//SI//ORCON//NOFORN
Gmail
facebook
Hotmail
YAHOO!
Google
skype
paltalk.com
YouTube
AOL mail
SPECIAL SOURCE OPERATIONS
(TS//SI//NF) PRISM Collection Details
PRISM
Current Providers
What Will You Receive in Collection (Surveillance and Stored Comms)? It varies by provider. In general:
• Microsoft (Hotmail, etc.)
• Google
• Yahoo!
• Facebook
• PalTalk
• YouTube
• Skype
• AOL
• Apple
• E-mail
• Chat – video, voice
• Videos
• Photos
• Stored data
• VoIP
• File transfers
• Video Conferencing
• Notifications of target activity – logins, etc.
• Online Social Networking details
• Special Requests
Complete list and details on PRISM web page:
Go PRISMFAA
TOP SECRET//SI//ORCON//NOFORN

Muscular

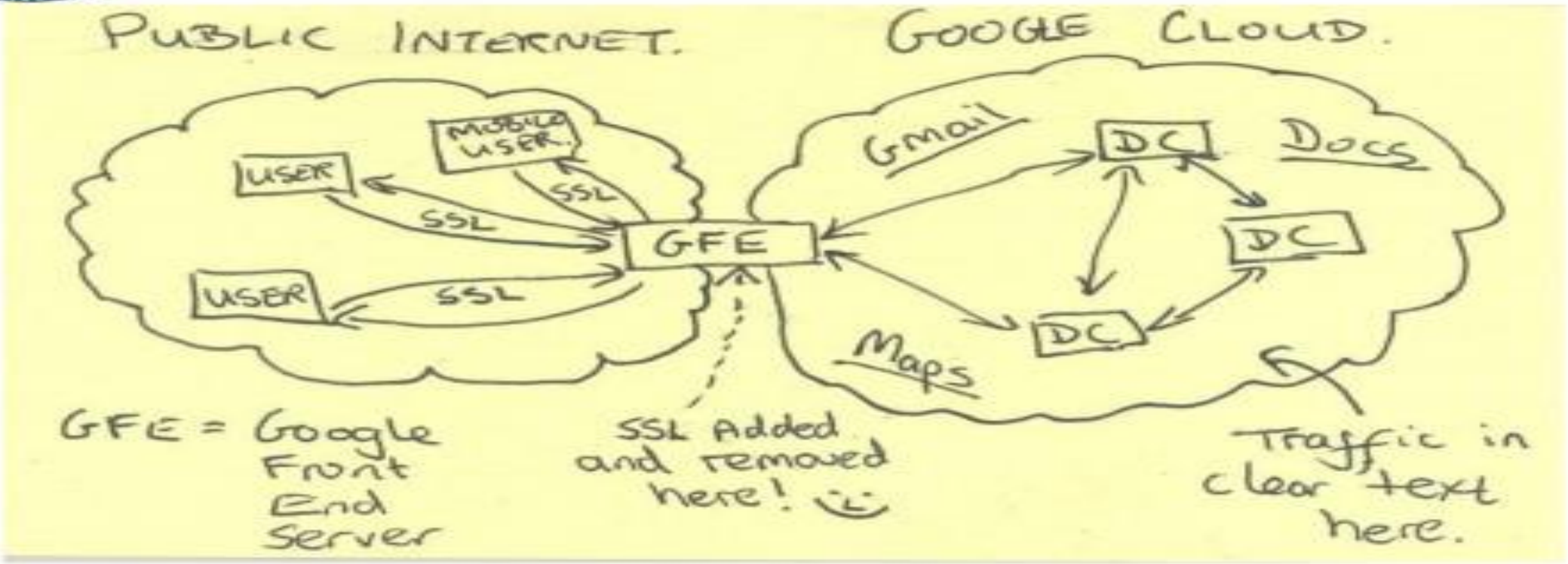
MUSCULAR (DS-200B)

- Operational July 2009
- (S//REL USA,GBR) Large international access located in United Kingdom
- Four TURMOIL T16s at 2.5Gb each - total ingest 10Gb
- LPTs installed May 2010 increase ingest to 20Gb
- Tasking worked cooperatively with GCHQ counterparts
- Partner to assume total control/responsibility for systems
- IP Subnet promotion in place, VoIP in the works

Muscular

TOP SECRET//SI//NOFORN

Current Efforts - Google



TOP SECRET//SI//NOFORN

איך ממשלות עוקפות את החוק

- ברוב ממשלות העולם האזנה לאזרחים זרים אינה מוגנת בחוק(החלפת טובות).
- פרצות בחוק המאפשרות לקבל נתונים בקלות (זימון מידע לעומת צו חיפוש).
- קשרים קרובים של חברות התקשרות לממשלות מקלים על השגת המידע.
- אם אחד מהצדדים מסכים להאזנה האזנה חוקית (טלפונים ציבורים ,מחשבים במרחב הציבורי).
- מידע שהועבר לצד שלישי אינו מוגן בחוק (Facebook) או cloud computing and storage.

מודעין תקשורתי על מטרות זרות

- רוב המודעין התקשורתי הנאסף מתבצע בתחום הבטחוני.

אשלון (Echelon) היא מערכת של מודיעין אותות המהווה את מערכת הריגול האלקטרונית הגדולה ביותר בהיסטוריה. אשלון הינה ברית של המדינות דוברות האנגלית: ארצות הברית, הממלכה המאוחדת, קנדה, אוסטרליה וניו זילנד. מטבעה הסודי של המערכת, מרבית הידע עליה אינו מגיע ממקור ראשון, אלא משמועות, עדויות וספקולציות של מביני דבר. מקובל להאמין שאשלון מיירטת שיחות טלפון, פקסים, שידורי לוויין והודעות דואר אלקטרוני ברחבי העולם. מעריכים כי אשלון מיירטת למעלה מ־3 מיליארד התקשרויות מדי יום.

- פרשת הציתותים בארצות הברית היא פרשת ריגול של הסוכנות לביטחון לאומי, ה- NSA, המאזינה למיליוני לקוחות של חברת התקשורת ורייזון ועוקבת אחר חשבונות האינטרנט של מיליוני אזרחים אמריקאים וזרים, כאמצעי נוסף להגן על תושבי ארצות הברית מפני טרור.

- באוקטובר 2013 פורסם שבמסגרת תוכנית שכונתה Us-985d, תוך חודש אחד הקליטה ה- NSA בצרפת כשבעים מיליון שיחות טלפון ומסרונים, לצורך חיפוש אחר חשודים בטרור, אך גם לצרכים שאינם ביטחוניים

- prism("מנסרה"), שבאמצעותה יכול הארגון לעקוב אחר כתובות דואר אלקטרוני, היסטוריית חיפוש, העברת קבצים בין מחשבים, ושיחות המתנהלות בין המשתמשים באתרים רבים, בהם גוגל, פייסבוק, ואפל. בינואר 2014 פורסם כי גם אפליקציות שירות מבוסס מיקום כגון גוגל מפות ואף משחקים כגון אנגרי בירדס שימשו למעקב בידי סוכנויות הביון של בריטניה וארצות הברית.

- ב-1 ביולי 2013 פרסם ה"גארדיאן" כי המודיעין האמריקאי מרגל אחרי שגרירות האיחוד האירופי במשרדיו בוושינגטון ובניו יורק ו"אחרי שגרירויות ונציגויות של 38 מדינות על אדמת ארצות הברית המכונות כולן מטרות", תוך שימוש במכשירי ציתות, ציוד אלקטרוני והתחברות לכבלי אנטנות.

Clipper Chip

בשנת 1993 פרסמה ממשלת ארצות הברית תקן הצפנה בשבב Clipper שהשתמש במספר אלגוריתמים סודיים, ביניהם צופן סימטרי בשם Skipjack. השבב בין היתר נועד לאפשר לרשויות גישה לתוכן המוצפן באמצעות דלת אחורית - מפתח נוסף אותו קיבלו בעת ייצור השבב.

מערכת מבוססת החלפת מפתחות על ידי דיפי הלמן והצפנת תעבורה על ידי skipjack.

לאחר כישלון המערכות במדיונות שונות , קודמו תקנים חדשים של מערכות Key escrow בברטיניה וארצות הברית .

מנגנוני העידוד שממשלות העולם השתמשו הם:

- לחץ כלכלי (בעזרת פרויקטים משותפים)
- מניעת יצוא (ולכן הגבלת מכירה מקומית)

אמינות? שלמות?

שליטה על יצוא

אחד מהמנגנונים שמשלות העולם ביצוע על מנת להבטיח את גישתם למידע הם:

- מניעת יצוא.
- עידוד תקנים נחותים ("קלים לפריצה") של הצפנה.
- בירוקרטיה.
- יצירת מצג שווא של יצוא למניעת פיתוח מקומי.

- Hans Buhler(1992)
- Netscape

חופש

Freedom is never more than one generation away from extinction. We didn't pass it to our children in the bloodstream. It must be fought for, protected, and handed on for them to do the same.

Ronald Reagan.

נייטרליות הרשת

נייטרליות הרשת הוא עיקרון ביישום רשתות התקשורות, הקובע כי לא תתבצע העדפה או אפליה בין מכשירים, שירותים או מחירים. רשת נייטרלית היא רשת תקשורת שאפשר לחבר אליה כל סוג של ציוד מתאים, שיפעל בכל תקן מתאים, ולקבל בה שירות ללא הבדל בין הפלטפורמות בהן בנויות האתרים או שירותים אחרים, והיא אינה מגבילה בשום אופן את התוכן המותר, ואינה מפלה לרעה את סוג תוכן אחד על חשבון סוג תוכן אחר על ידי הגבלת מהירות או כל הגבלה אחרת.

https://www.youtube.com/watch?v=0782P6m5cX0

בעקבות אישור חוק ההסדרים ביולי 2010, נקבע כי חברות הסלולר לא יכולו להפלות שירותים שונים באינטרנט הסלולרי, בעיקר יישומי שיחות VoIP. החוק קובע כי אסורה פגיעה בנייטרליות הרשת, אם באמצעים טכנולוגיים או באמצעים תמחיריים.

נייטרליות הרשת

Google Search I'm Feeling Lucky

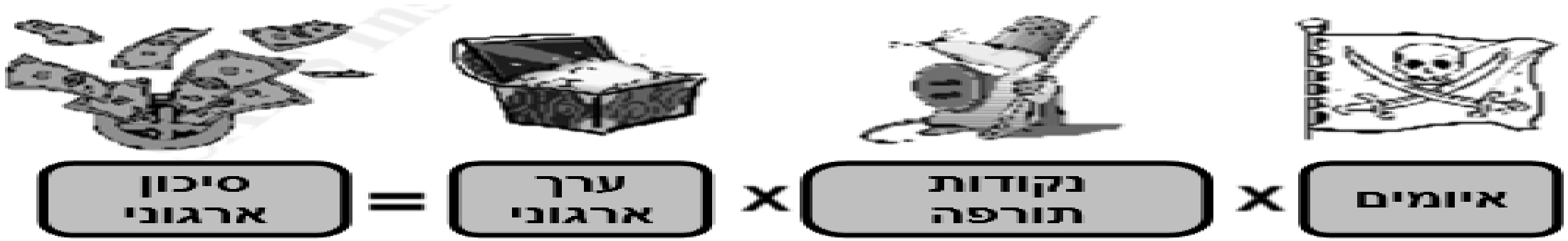
Tell Congress: Please don't censor the web!

נייטרליות הרשת

סיכום

שומר השער הראשון בשמירה על הצדק, הפרטיות והחירות האזרחית שלנו הוא מהנדס אבטחת המידע.

לא כול הנוצץ זהב , המניעים של ממשלות, ארגונים לאומים וחברות אינם תמיד ברורים , ולכן תמיד צריך להסתכל על התמונה מכול צדדיה.



Terror and freedom

https://www.youtube.com/watch?v=GnZnbk_2wSI

https://www.youtube.com/watch?v=aS1HKfbXLp4

https://www.youtube.com/watch?v=KAev9ZS5kas

wiretapping

http://www.youtube.com/watch?v=xyQluTfyO7g

http://www.youtube.com/watch?v=o3wfZhM9ibI

http://www.youtube.com/watch?v=NDYE_HRrSt4

http://www.youtube.com/watch?v=IjTmnOy8FB0

www.youtube.com/watch?v=ZmQYcq1VWxw

NSA and data mining

http://www.youtube.com/watch?v=2y-mpO0JB_U

http://www.youtube.com/watch?v=pjYoT3sZIWA

http://www.youtube.com/watch?v=ntT3CUhV9eA

http://www.youtube.com/watch?v=0JR7tBTuH8I

http://www.youtube.com/watch?v=m3ZDMCUz2Xs

נייטרליות הרשת-קישורים להמשך העשרה

http://www.youtube.com/watch?v=Pp1MAMkIa6A

http://www.youtube.com/watch?v=xjOxNiHUsZw

http://www.youtube.com/watch?v=9sogCXsvp9w

http://www.youtube.com/watch?v=0782P6m5cX0

מקורות מידע

מקורות מידע
http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2006/2006WT.pdf
http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2007/Table22007.pdf
http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2008/Table2.pdf
http://en.wikipedia.org/
http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2013/Table2.pdf
http://www.cl.cam.ac.uk/~rja14/Papers/SEv2-c24.pdf
http://www.the7eye.org.il/topic/%D7%A4%D7%A8%D7%A9%D7%AA-%D7%A0%D7%9E%D7%A8%D7%95%D7%93%D7%99-%D7%92%D7%99%D7%9C%D7%99%D7%95%D7%9F-%D7%9E%D7%99%D7%95%D7%97%D7%93/
http://cryptome.org/2014/
http://mlk-kpp01.stanford.edu/index.php/encyclopedia/encyclopedia/enc_federal_bureau_of_investigation_fbi/
http://doc.utwente.nl/69903/1/Stolen_laptop_case_study.pdf
https://www.usenix.org/sites/default/files/conference/protected-files/sec14_slides_mowery.pdf

If you want total security, go to prison. There you're fed, clothed, given medical care and so on. The only thing lacking... is freedom. Dwight D. Eisenhower